# Dépannage de l'authentification Web sur un contrôleur de réseau local sans fil

## Contenu



## Introduction

Ce document fournit des conseils afin de dépanner des questions d'authentification Web dans un environnement Sans fil du contrôleur LAN (WLC).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance du point d'accès léger Protocol (LWAPP) /Control et ravitaillement des points d'accès sans fil (CAPWAP)
- La connaissance de configurer le point d'accès léger (LAP) et le WLC pour le fonctionnement de base.
- Connaissance de base de l'authentification Web et de l'authentification Web de configurer sur WLCs. Pour les informations sur configurer l'authentification Web sur WLCs, référez-vous à l'exemple Sans fil de configuration d'authentification Web de contrôleur LAN.

### Composants utilisés

Les informations dans ce document sont basées sur un WLC 5500 qui exécute la version 7.0.98.0 de micrologiciels.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-

vous que vous comprenez l'effet potentiel de toute commande.

### Produits connexes

Ce document peut également être utilisé avec ces matériels :

- Contrôleurs sans fil de la gamme Cisco 5500
- Contrôleurs de réseau LAN fil de la gamme Cisco 4400
- Contrôleurs de LAN sans fil de la gamme Cisco 4100
- Contrôleurs sans-fil de la gamme Cisco 2500
- Contrôleurs de réseau local sans fil de la gamme Cisco 2100
- Contrôleurs de LAN sans fil de la gamme Cisco 2000
- Contrôleur de réseau local sans fil de la gamme Cisco Airespace 3500
- Contrôleur de réseau local sans fil de la gamme Cisco Airespace 4000
- Module contrôleur de réseau local sans fil Cisco
- Module de services sans fil (WiSM) des gammes Cisco Catalyst 6500/7600
- Contrôleurs sans-fil de la gamme Cisco Flex 7500
- Cisco Wireless Services Module 2 (WiSM2)
- Contrôleurs de réseau local sans fil intégrés Cisco Catalyst 3750

### Conventions

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

## Authentification Web sur WLCs

L'authentification Web est une fonctionnalité de sécurité de la couche 3 qui fait ne pas permettre le contrôleur le trafic IP, excepté les paquets liés aux dn de paquets liés au DHCP, d'un client particulier jusqu'à ce que ce client ait correctement fourni un nom d'utilisateur valide et un mot de passe à une exception du trafic permise par l'ACL de Pre-Auth. L'authentification Web est la seule stratégie de sécurité qui permet au client d'obtenir une adresse IP avant l'authentification. Il s'agit d'une méthode d'authentification simple qui ne requiert aucun utilitaire demandeur ou client. L'authentification Web peut être faite localement sur un WLC ou via un serveur RADIUS. L'authentification Web est généralement utilisée par les clients qui veulent déployer un réseau d'accès invité.

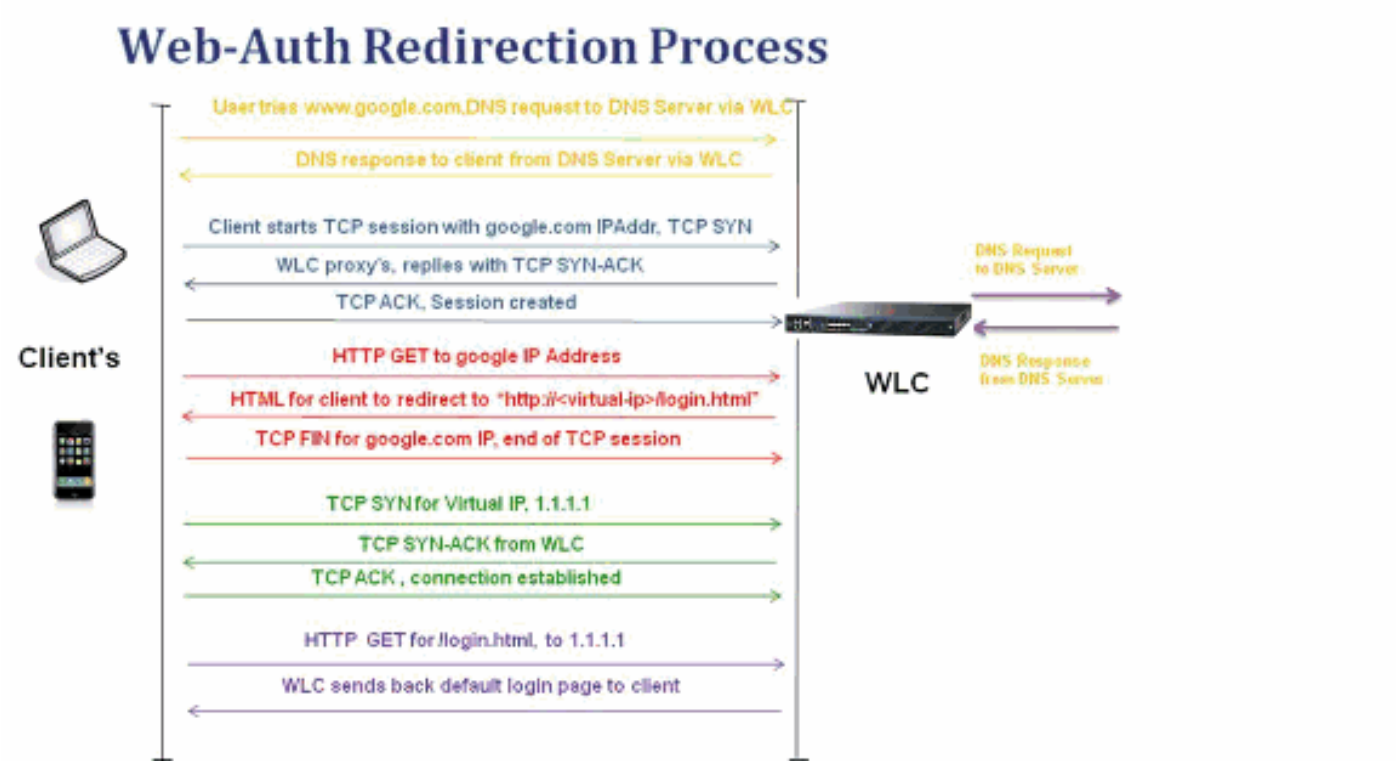
Les débuts d'authentification Web quand le contrôleur intercepte le premier HTTP de TCP (port 80) OBTIENNENT le paquet du client. Pour que le navigateur Web du client obtienne ceci loin, le client doit d'abord obtenir une adresse IP, et fait une traduction de l'URL à l'adresse IP (résolution de DN) pour le navigateur Web. Ceci fait le navigateur Web connaître quelle adresse IP pour envoyer le HTTP OBTENEZ.

Quand l'authentification Web est configurée sur le WLAN, le contrôleur bloque tout le trafic (jusqu'à ce que la procédure d'authentification est terminée) du client, excepté le DHCP et le trafic DNS. Quand le client envoie le premier HTTP ARRIVEZ au port TCP 80, le contrôleur réoriente le client à https:1.1.1.1/login.html pour le traitement. Ce processus évoque par la suite la page Web de procédure de connexion.

**Remarque:** Quand vous utilisez un web server externe pour l'authentification Web, certaines des Plateformes WLC ont besoin d'un ACL de pré-authentification pour le web server externe, qui inclut le contrôleur de gamme Cisco 5500, une gamme Cisco 2100 contrôleur, la gamme Cisco 2000 et le module réseau de contrôleur. Pour les autres Plateformes WLC l'ACL de pré-authentification n'est pas obligatoire.

**Remarque:** Mais, l'il est conseillé de configurent un ACL de Préauthentification pour le web server externe quand vous utilisez une authentification de Web externe.

Cette section explique le procédé de redirection d'authentification Web en détail.




- Vous ouvrez le navigateur Web et saisissez un URL, par exemple, `http://www.google.com`. Le client envoie une demande de DN de cet URL d'obtenir l'IP pour la destination. WLC saute la demande de DN au serveur DNS et le serveur DNS répond de retour avec des DN répondent, qui contient l'adresse IP de la destination `www.google.com`, qui consécutivement est expédiée aux clients sans fil
- Les essais de client puis pour ouvrir une connexion TCP avec l'adresse IP de destination. Il envoie un paquet de synchronisation de TCP destiné à l'adresse IP de `www.google.com`.
- Le WLC a des règles configurées pour le client et par conséquent peut agir en tant que proxy pour `www.google.com`. Il renvoie un paquet du TCP SYN-ACK au client avec la source comme adresse IP de `www.google.com`. Le client renvoie un paquet du TCP ACK afin de se terminer la prise de contact à trois voies de TCP et la connexion TCP est entièrement établie.
- Le client envoie un HTTP OBTIENNENT le paquet destiné à `www.google.com`. Le WLC intercepte ce paquet, l'envoie pour la manipulation de redirection. La passerelle d'application de HTTP prépare un corps HTML et le renvoie comme réponse au HTTP GET demandé par le client. Ce HTML incite le client pour aller à l'URL par défaut de page Web du WLC, par exemple, `http:// <Virtual-Server-IP>/login.html`.
- Le client ferme la connexion TCP avec l'adresse IP, par exemple `www.google.com`.
- Maintenant le client veut aller à `http://1.1.1.1/login.html` et ainsi il essaye d'ouvrir une connexion TCP avec l'adresse IP virtuelle du WLC. Il envoie un paquet de synchronisation de

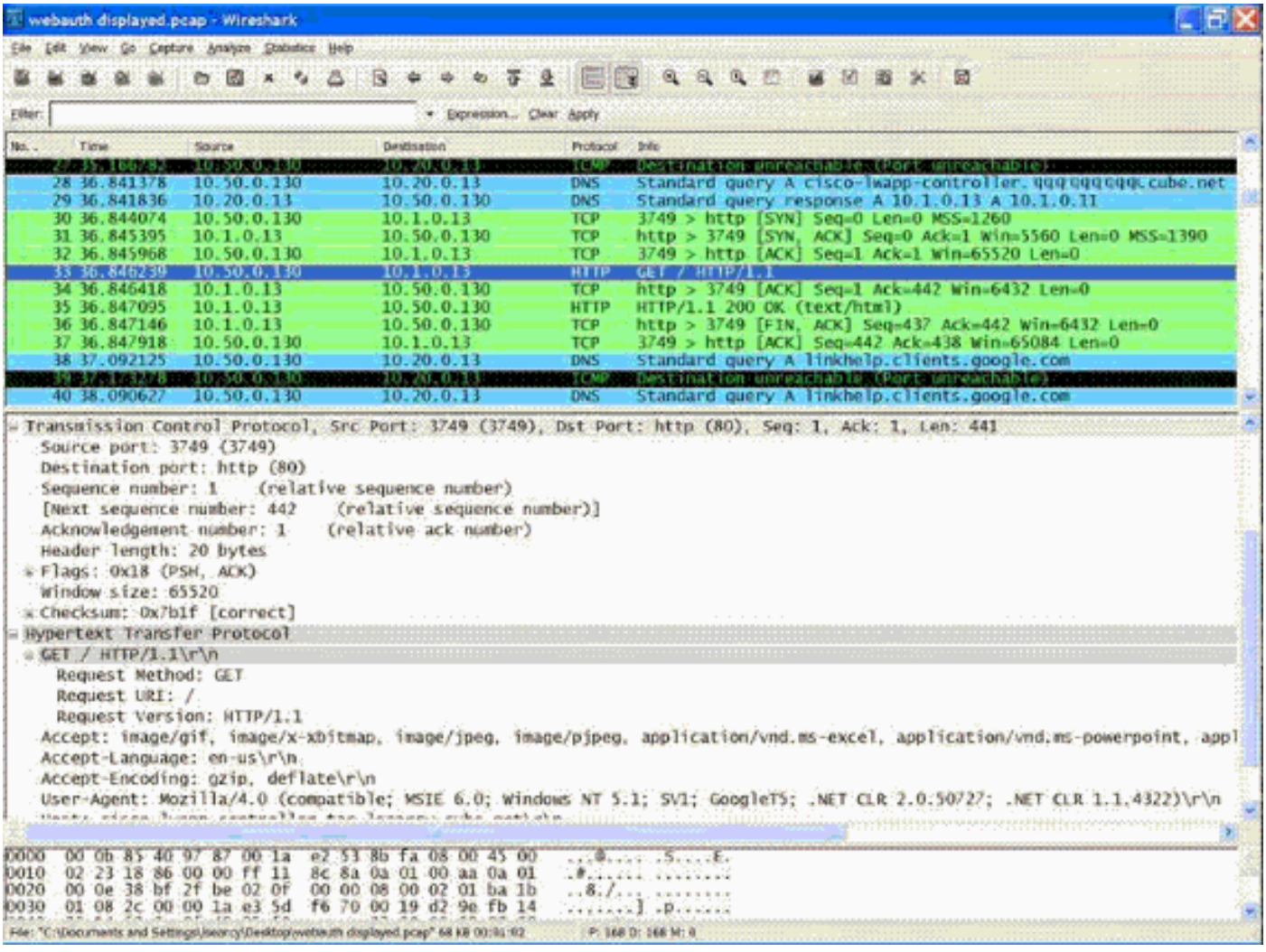
TCP pour 1.1.1.1 au WLC.

- Le WLC répond de retour avec un TCP SYN-ACK et le client renvoie un TCP ACK au WLC afin de se terminer la prise de contact.
- Le client envoie un HTTP OBTIENNENT pour /login.html a destiné à 1.1.1.1 afin de demander pour la page de connexion.
- Cette demande est permise jusqu'au serveur Web du WLC, et le serveur répond de retour avec la page de connexion par défaut. Le client reçoit la page de connexion sur la fenêtre du navigateur où l'utilisateur peut avancer et procédure de connexion.

Voici un exemple. Dans cet exemple, l'adresse IP du client est 10.50.0.130. Le client a résolu l'URL au web server qu'il accédait à 10.1.0.13. Comme vous pouvez voir, le client a fait la prise de contact à trois voies pour commencer la connexion TCP et a puis envoyé un HTTP OBTIENNENT le paquet commençant par le paquet 30. Le contrôleur intercepte les paquets et répond avec le code 200. Le paquet du code 200 a un URL de réorientation dans lui :

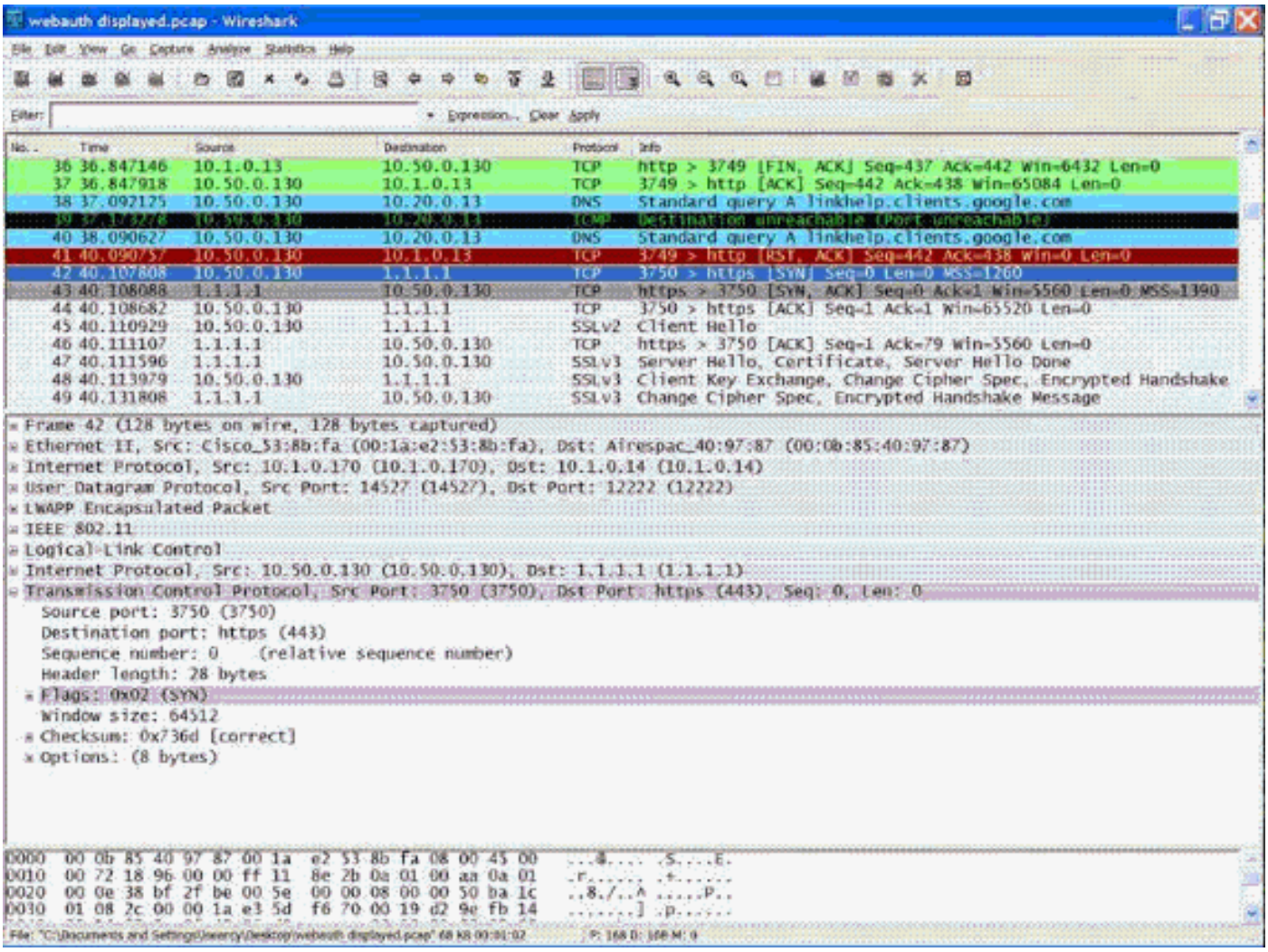
```
<HTML><HEAD><TITLE>Cisco Systems Inc. Web Authentication Redirect</TITLE><META
http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma"
content="no-cache"><META http-equiv="Expires" content="-1"><META http-equiv="refresh"
content="1; URL=https://1.1.1.1/login.html?redirect=cisco-lwapp-controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

Il ferme alors la connexion TCP par la prise de contact à trois voies.




Le client commence alors la connexion HTTPS à l'URL de réorientation qui l'envoie à 1.1.1.1, qui est l'adresse IP virtuelle du contrôleur. Le client doit valider le certificat de serveur ou l'ignorer afin d'apporter le tunnel SSL. Dans ce cas, c'est un certificat auto-signé ainsi le client l'a ignoré. La page Web de procédure de connexion est envoyée par ce tunnel SSL. Le paquet 42 commence

les transactions.




Vous avez une option de configurer le nom de domaine pour l'adresse IP virtuelle du contrôleur LAN Sans fil. Si vous configurez le nom de domaine pour l'adresse IP virtuelle, ce nom de domaine est retourné dans le paquet d'OK de HTTP du contrôleur en réponse au HTTP OBTIENNENT le paquet du client. Vous alors devez exécuter une résolution de DN pour ce nom de domaine et une fois qu'il obtient une adresse IP de la résolution de DN, elle tente d'ouvrir une session TCP avec cette adresse IP, qui est un IP configuré sur une interface virtuelle du contrôleur.

Par la suite, la page Web est traversée le tunnel au client et l'utilisateur renvoie le nom d'utilisateur/mot de passe par le tunnel SSL.

L'authentification Web est exécutée par une de ces trois méthodes :

- Authentification Web utilisant une page Web interne (par défaut). Référez-vous à choisir la page d'authentication login de web par défaut pour plus d'informations sur l'utilisation de la page Web par défaut.
- Authentification Web utilisant une page de connexion personnalisée. Référez-vous à créer une page de connexion personnalisée d'authentification Web pour plus d'informations sur la façon utiliser la page de connexion personnalisée.
- Authentification Web utilisant une page de connexion d'un web server externe. Référez-vous utilisant une page de connexion personnalisée d'authentification Web d'un serveur Web externe pour plus d'informations sur la façon utiliser une page de connexion d'un web server

externe.

**Remarque:** Le paquet authentique personnalisé de Web a une limite de jusqu'à 30 caractères pour des noms du fichier. Assurez-vous qu'aucun nom du fichier dans le paquet n'est plus grand que 30 caractères.

**Remarque:** De la version 7.0 WLC en avant, si l'authentification Web est activée sur le WLAN et vous avez également des règles d'ACL CPU, les règles d'authentification Web basées par client ont toujours la priorité plus élevée tant que le client est unauthenticated dans l'état de `WebAuth_Reqd`. Une fois que le client va à l'état de `PASSAGE`, les règles d'ACL CPU obtiennent appliqué.

**Remarque:** Par conséquent si CPU ACLs sont activées dans le WLC, une règle d'autoriser pour l'IP d'interface virtuelle est exigée (dans TOUTE direction) en ces conditions :

- Quand l'ACL CPU n'a pas un autoriser TOUTE LA règle pour les deux directions.
- Quand là existe un autoriser TOUTE LA règle, mais existe là également une règle de REFUSER pour le port 443 ou 80 d'une priorité plus élevée.

**Remarque:** La règle d'autoriser pour l'IP virtuel devrait être pour le protocole TCP et le port 80, si le secureweb est désactivé, ou le port 443, si le secureweb est activé. C'est nécessaire afin de permettre l'accès du client à l'authentification réussie de courrier d'adresse IP d'interface virtuelle quand CPU ACLs sont en place.

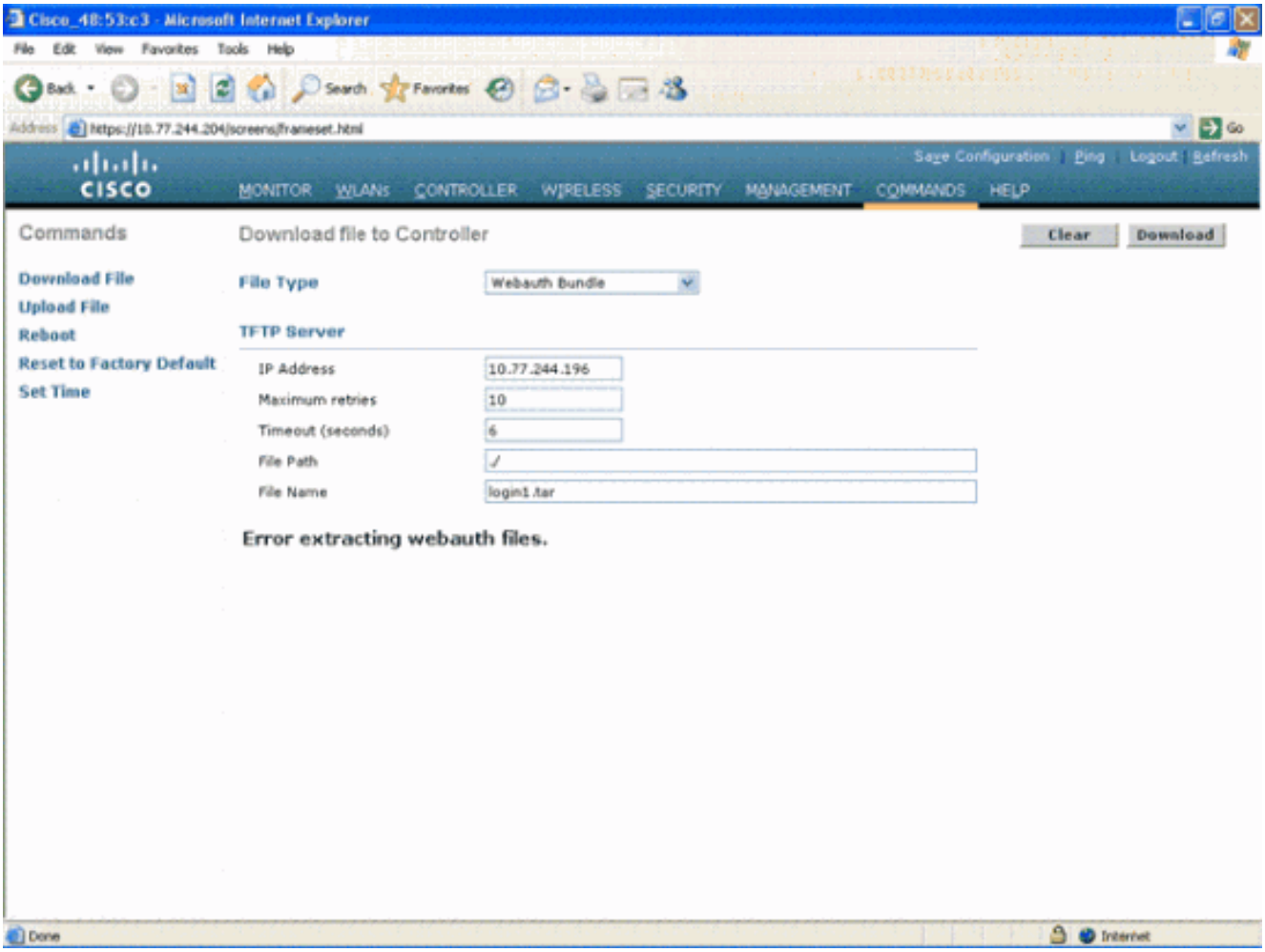
## Dépannage de l'authentification Web

Après que vous configuriez l'authentification Web, si la caractéristique ne fonctionne pas comme prévu, terminez-vous ces étapes de dépannage :

1. Vérifiez si le client obtient une adresse IP. Sinon, les utilisateurs peuvent décocher le **DHCP prié** sur le WLAN et donner au client sans fil une adresse IP statique. Ceci assume l'association avec le Point d'accès. Référez-vous à la section de *questions d'adressage IP de questions de client de dépannage dans le réseau sans fil unifié Cisco pour dépanner des questions connexes DHCP*.
2. Sur des versions WLC plus tôt que 3.2.150.10, vous devez manuellement entrer dans **https://1.1.1.1/login.html** afin de naviguer vers la fenêtre d'authentification Web.L'étape suivante dans le processus est résolution de DN de l'URL dans le navigateur Web. Quand un client WLAN se connecte à un WLAN configuré pour l'authentification Web, le client obtient une adresse IP du serveur DHCP. L'utilisateur ouvre un navigateur Web et introduit une adresse de site Web. Le client exécute alors la résolution de DN d'obtenir l'adresse IP du site Web. Maintenant, quand les essais de client pour atteindre le site Web, le WLC intercepte le HTTP obtenez la session du client et réorientez l'utilisateur à la page de connexion d'authentification Web.
3. , Assurez-vous par conséquent que le client peut exécuter la résolution de DN pour que la redirection fonctionne. Sur Windows, choisissez le **Start > Run**, écrivez le **CMD** afin d'ouvrir une fenêtre de commandes, et faites un « nslookup www.cisco.com » et voyez si l'adresse IP revient.Sur des MACs/Linux : ouvrez un terminal window et faites un « nslookup www.cisco.com » et voyez si l'adresse IP revient.Si vous croyez le client n'obtient pas la résolution de DN, vous peut l'un ou l'autre :Écrivez ou l'adresse IP de l'URL (par exemple, http://www.cisco.com est http://198.133.219.25)Essayez d'atteindre directement la page du webauth du contrôleur avec https:// <Virtual_interface_IP_Address>/login.html. Typiquement

c'est http://1.1.1.1/login.html.Écrivant cet URL évoque la page Web ? Si oui, il est le plus susceptible un problème de DN. Ce pourrait également être un problème de certificat. Le contrôleur, par défaut, utilise un certificat auto-signé et la plupart des navigateurs Web mettent en garde contre les utiliser.

4. Pour l'authentification Web utilisant la page Web personnalisée, assurez-vous que code HTML pour la page Web personnalisée est approprié.Vous pouvez télécharger un script d'authentification Web d'échantillon des téléchargements logiciels de Cisco. Par exemple, pour les 4400 contrôleurs, choisissez les **Produits > la radio > contrôleur LAN Sans fil > Contrôleurs autonomes > Contrôleurs de réseau local sans fil de la gamme Cisco 4400 > contrôleur LAN sans fil Cisco 4404 > logiciel sur le châssis > l'authentification Web Sans fil Bundle-1.0.1 de contrôleur réseau local** et téléchargez le **fichier webauth_bundle.zip**.Ces paramètres sont ajoutés à l'URL quand le navigateur Internet de l'utilisateur est réorienté à la page de connexion personnalisée :ap_mac — L'adresse MAC du Point d'accès auquel l'utilisateur de sans fil est associé.switch_url — L'URL du contrôleur auquel les identifiants utilisateurs devraient être signalés.réorientez — L'URL auquel l'utilisateur est réorienté après l'authentification est réussie.code statut — Code d'état est retourné du serveur de l'authentification Web du contrôleur.wlan — Le WLAN SSID auquel l'utilisateur de sans fil est associé.Ce sont codes d'état disponibles :Code d'état 1 : « Vous êtes déjà ouvert une session. Aucune action supplémentaire n'est exigée sur votre cloison »Code d'état 2 : « Vous n'êtes pas configuré pour authentifier contre le portail web. Aucune action supplémentaire n'est exigée sur votre cloison »Code d'état 3 : « Le nom d'utilisateur spécifié ne peut pas être utilisé à ce moment. Peut-être le nom d'utilisateur est déjà connecté dans le système ? »Code d'état 4 : « Vous avez été exclu. »Code d'état 5 : « La combinaison de nom d'utilisateur et de mot de passe que vous avez écrite est non valide. Essayez s'il vous plaît de nouveau. »
5. Tous les fichiers et images qui doivent apparaître sur la page Web personnalisée devraient être empaquetés dans un fichier de .tar avant de télécharger au WLC. Assurez-vous qu'un des fichiers inclus dans le paquet de goudron est login.html. Vous recevez ce message d'erreur si vous n'incluez pas le fichier de login.html
:




Référez-vous aux instructions pour la section d'authentification Web Customized de l'exemple Sans fil de configuration d'authentification Web de contrôleur LAN pour plus d'informations sur la façon créer une fenêtre personnalisée d'authentification Web.**Remarque:** Les fichiers qui sont grands et les fichiers qui ont de longs noms auront comme conséquence une erreur d'extraction. Les images d'il est recommandé que sont dans le format de .jpg.

6. L'Internet Explorer 6.0 est SP1 ou plus tard le navigateur recommandé pour l'usage de l'authentification Web. D'autres navigateurs peuvent ou peuvent ne pas travailler.
7. Assurez-vous que l'option de **script** n'est pas bloquée sur le navigateur de client car la page Web personnalisée sur le WLC est fondamentalement un script HTML. Sur IE 6.0, ceci est désactivé par défaut pour des raisons de sécurité.**Remarque:** Le bloqueur d'afficher doit être désactivé sur le navigateur si vous en avez configuré vous affichez des messages pour l'utilisateur.**Remarque:** Si vous parcourez à un site de **https**, la redirection ne fonctionne pas. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCar04580 (clients enregistrés seulement).
8. Si vous avez un **nom d'hôte** configuré pour l'**interface virtuelle du** WLC, assurez-vous que la résolution de DN est disponible pour le nom d'hôte de l'interface virtuelle.**Remarque:** Naviguez vers le menu de **Controller > Interfaces du** GUI WLC afin d'assigner une **adresse Internet de DN à l'**interface virtuelle.
9. Parfois le Pare-feu installé sur l'ordinateur client bloque la page de connexion d'authentification Web. Désactivez le Pare-feu avant que vous essayiez d'accéder à la page de connexion. Le Pare-feu peut être activé de nouveau une fois que l'authentification Web est terminée.
10. Le Pare-feu de topologie/solution peut être placé entre le client et le serveur de Web-auth,

qui dépend du réseau. Quant à chaque conception de réseaux/solution mises en application, l'utilisateur final devrait s'assurer qu'on permet ces ports sur le pare-feu réseau.

11. Pour que l'authentification Web se produise, le client devrait d'abord s'associer au WLAN approprié sur le WLC. Naviguez vers le menu de **Monitor > Clients** sur le GUI WLC afin de voir si le client est associé au WLC. Vérifiez si le client a une adresse IP valide.
12. Désactivez les paramètres de proxy sur le navigateur de client jusqu'à ce que l'authentification Web soit terminée.
13. La méthode d'authentification de web par défaut est PAP. Assurez-vous qu'on permet à l'authentification PAP sur le serveur de RAYON pour que ceci fonctionne. Afin de vérifier le statut d'authentification client, vérifiez met au point et les messages de log du serveur de RAYON. Vous pouvez utiliser le **debug aaa toute la** commande sur le WLC de visualiser met au point du serveur de RAYON.
14. Mettez à jour le driver du matériel sur l'ordinateur au dernier code du site Internet du constructeur.
15. Vérifiez les configurations dans le suppliant (programme sur l'ordinateur portable).
16. Quand vous utilisez le suppliant de config de Windows Zero construit dans Windows :Vérifiez l'utilisateur fait installer les derniers correctifs.Exécutez-vous met au point sur le suppliant.
17. Sur le client, activez l'EAPOL (WPA+WPA2) et RASTLS se connecte d'une fenêtre de commandes, Start > Run > CMD :`netsh ras set tracing eapol enable`
    `netsh ras set tracing rastls enable`Afin de désactiver les logs, exécutez la même commande mais remplacez l'enable par le débronchement. Pour le XP, tous les logs veulent se trouvent dans C:\Windows\tracing.
18. Si vous n'avez toujours aucune page Web de procédure de connexion, collectez et analysez cette sortie d'un client simple :`debug client <mac_address in format xx:xx:xx:xx:xx:xx>`
    `debug dhcp message enable`
    `debug aaa all enable`
    `debug dot1x aaa enable`
    `debug mobility handoff enable`
19. Si la question n'est pas résolue après que vous vous terminiez ces étapes, collectez ces derniers met au point et utilise l'outil de demande de service TAC (clients enregistrés seulement) afin d'ouvrir une demande de service.`debug pm ssh-appgw enable`
    `debug pm ssh-tcp enable`
    `debug pm rules enable`
    `debug emweb server enable`
    `debug pm ssh-engine enable packet <client ip>`

## Informations connexes

- Exemple de configuration de l'authentification Web sur un contrôleur de réseau local sans fil
- Exemple de configuration d'authentification Web externe avec des contrôleurs de réseau local sans fil
- Support et documentation techniques - Cisco Systems