Configurer un point d'accès léger en tant que demandeur 802.1x

Contenu

Introduction

Ce document décrit comment configurer un point d'accès léger en tant que suppliant de 802.1x pour authentifier contre un serveur de RAYON.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Cisco Aironet 1130, 1240, ou Point d'accès de gamme 1250
- WLC qui exécute la version 5.1 de ® IOS
- Commutateurs de la gamme Cisco Catalyst 3560 avec la Cisco IOS version 12.2(35)SE5
- Commutateurs de la gamme Cisco Catalyst 3750 avec la Cisco IOS version 12.2(40)SE
- Commutateurs de la gamme Cisco Catalyst 4500 avec la Cisco IOS version 12.2(40)SG
- Commutateurs de la gamme Cisco Catalyst 6500 avec l'engine 32 de superviseur qui exécute la Cisco IOS version 12.2(33)SXH

Composants utilisés

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.

Conventions

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

Informations générales

Les recouvrements ont installé les Certificats en usine X.509, signés par une clé privée, qui sont gravés dans le périphérique au moment de la fabrication. Les recouvrements emploient ce certificat pour authentifier avec le WLC au processus de jonction. Le pour en savoir plus, se rapportent à sécuriser le plan de contrôle LWAPP du document déployant des contrôleurs LAN de radio de gamme de Cisco 440X. Cette méthode décrit une autre manière d'authentifier des recouvrements. Avec la version 5.1 WLC, vous pouvez configurer l'authentification de 802.1x entre un Point d'accès de Cisco Aironet et un commutateur de Cisco. Le Point d'accès agit en tant que suppliant de 802.1x et est authentifié par le commutateur contre un serveur de RAYON (ACS) cet EAP-FAST d'utilisations avec le ravitaillement anonyme PAC. Une fois qu'il est configuré pour l'authentification de 802.1x, le commutateur ne permet à aucun trafic autre que le trafic de 802.1x pour traverser le port jusqu'à ce que le périphérique connecté au port authentifie avec succès. Un Point d'accès peut être authentifié ou avant qu'il joigne un WLC ou après qu'il a joint un WLC, dans ce cas vous configurent le 802.1x sur le commutateur après que le RECOUVREMENT joigne le WLC.

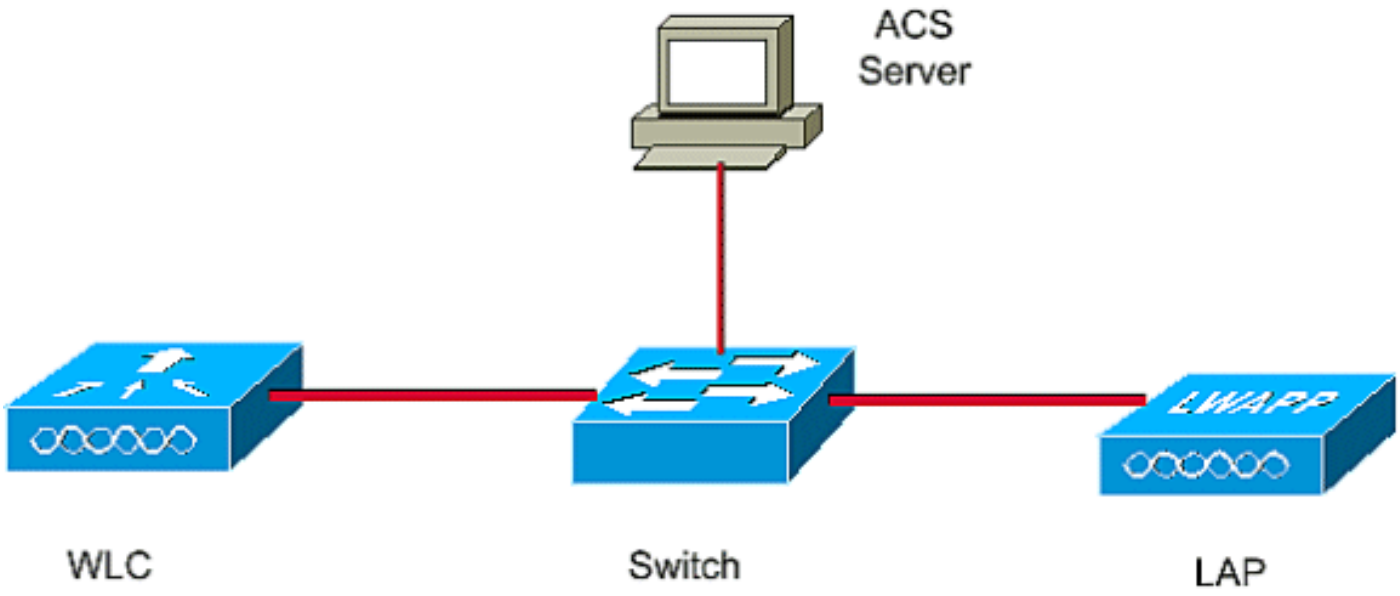
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise ces adresses IP :

- L'adresse IP du commutateur est 10.77.244.210
- L'adresse IP du serveur ACS est 10.77.244.196
- L'adresse IP du WLC est 10.77.244.204

Configurez le RECOUVREMENT

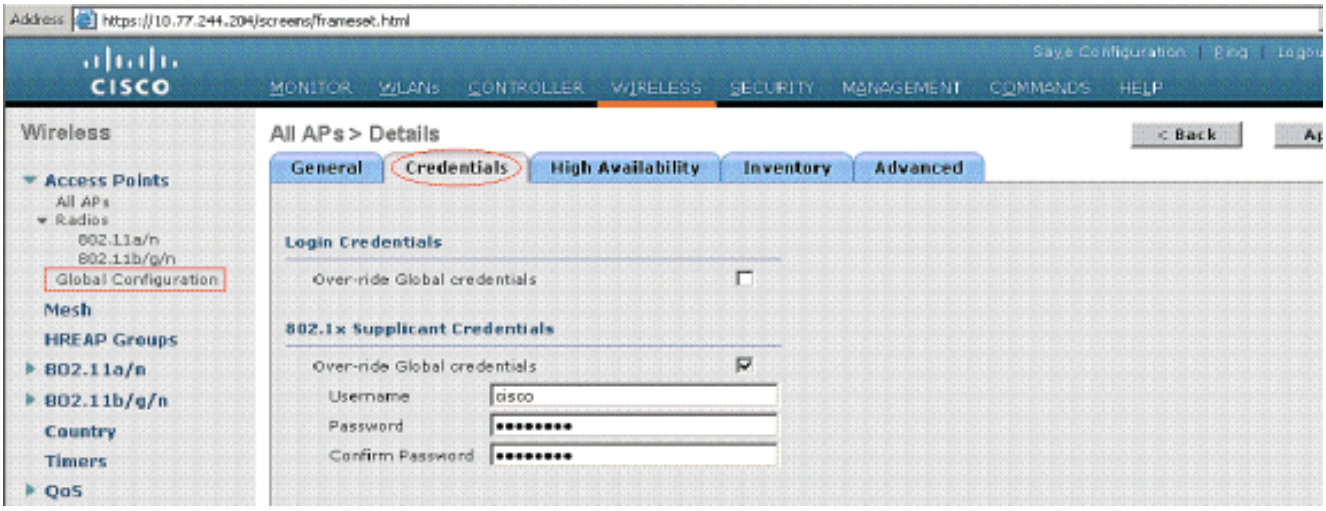
Dans cette section, vous êtes présenté avec les informations pour configurer le RECOUVREMENT en tant que suppliant de 802.1x.

Procédez comme suit :

1. Assurez-vous que le Point d'accès est chargé avec une image légère de reprise.
2. Connectez le RECOUVREMENT au commutateur.
3. Le RECOUVREMENT passe par le processus de jonction et s'inscrit au WLC. Ceci peut être vérifié du menu Sans fil du WLC suivant les indications de la figure 1.**Figure 1**

4. Cliquez sur le **Point d'accès**, et cliquez sur l'onglet de **qualifications**.
5. Sous les qualifications de suppliant de 802.1x se dirigeant, cochez la case **globale de qualifications de priorité** pour placer le nom d'utilisateur et mot de passe de 802.1x pour ce Point d'accès. Vous pouvez également placer le nom d'utilisateur et mot de passe en commun à tous les Points d'accès qui joignent un WLC avec le menu de configuration

globale. La figure 2 affiche comment placer les qualifications de 802.1x pour un Point d'accès.**Figure 2**



Remarque: Vous pouvez également placer le nom d'utilisateur et mot de passe de 802.1x pour un Point d'accès avec le **config ap dot1xuser de** commande WLC CLI **ajoutez le <password> Cisco_AP (nom de mot de passe de <user> de nom d'utilisateur AP)**.

6. Cliquez sur **Apply** pour valider les modifications.
7. **Save configuration de** clic pour sauvegarder les qualifications.**Remarque:** Une fois qu'enregistrées, ces qualifications sont retenues à travers des réinitialisations WLC et AP. Ils changent seulement quand le RECOUVREMENT joint un nouveau WLC. Le RECOUVREMENT assume le nom d'utilisateur et mot de passe qui ont été configurés sur le nouveau WLC.
8. Si le Point d'accès n'a pas joint un WLC encore, vous devez consoler dans le RECOUVREMENT pour placer les qualifications et pour utiliser cette commande CLI dans le mode enable :`LAP#lwapp ap dot1x username <username> password <password>` **Remarque:** Cette commande est disponible seulement pour les Points d'accès qui exécutent l'image de 5.1 reprises.

Configurez le commutateur

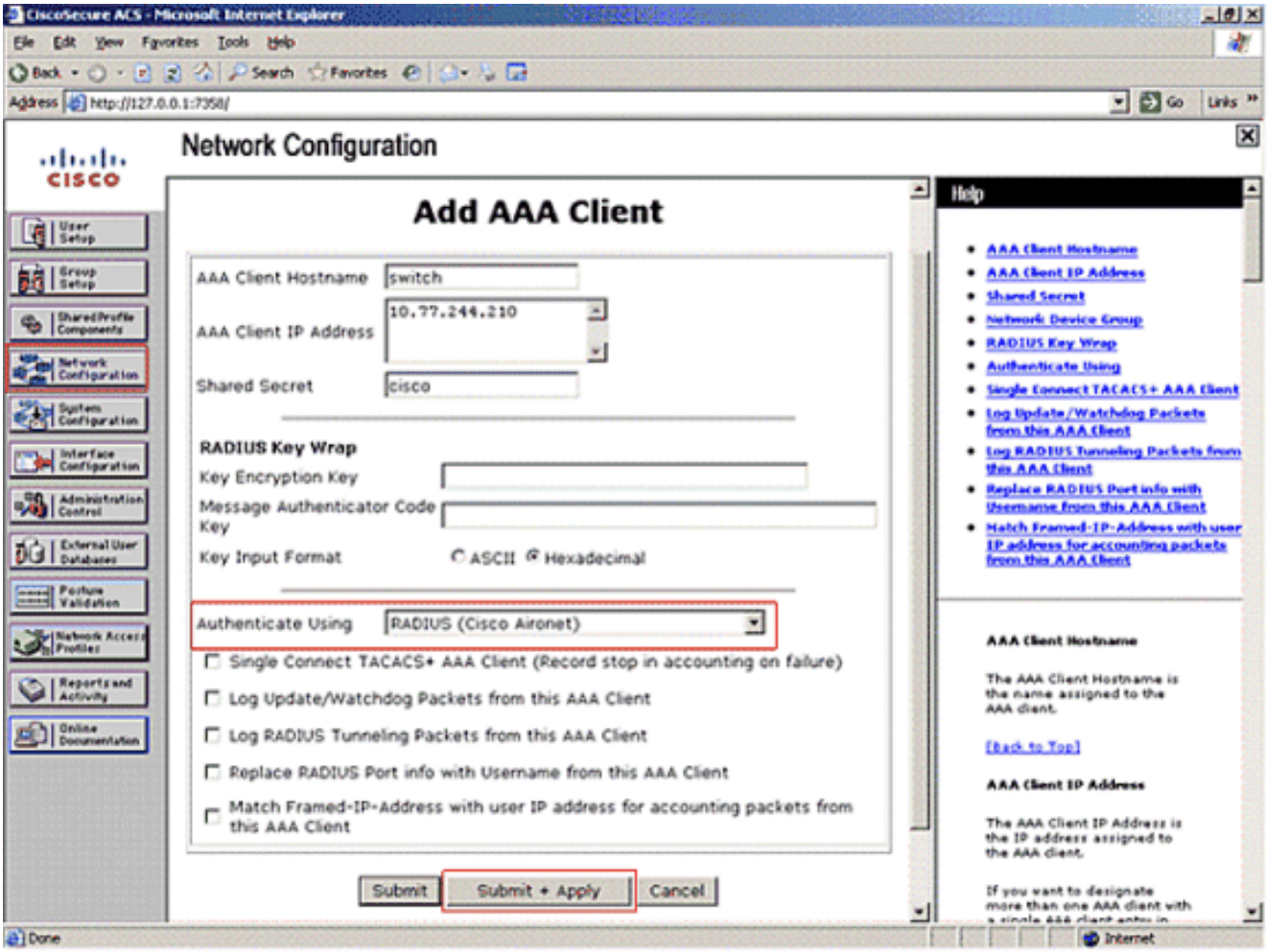
Le commutateur agit en tant qu'authentificateur pour le RECOUVREMENT et authentifie le RECOUVREMENT contre un serveur de RAYON. Si le commutateur n'a pas le logiciel conforme, améliorez le commutateur. Sur le commutateur CLI, sélectionnez ces commandes d'activer l'authentification de 802.1x sur un port de commutateur :

```
switch#configure terminal                    switch(config)dot1x system-auth-control
switch(config)aaa new-model                    switch(config)aaa authentication dot1x default
group radius                    switch(config)radius server host 10.77.244.196 key cisco!---
configures the radius server with shared secret switch(config)interface gigabitEthernet 1/0/43!-
-- 43 is the port number on which the access point is connected. switch(config-if)switchport
mode access switch(config-if)dot1x pae authenticator!--- configures dot1x authentication
switch(config-if)dot1x port-control auto!--- With this command switch initiates the 802.1x
authentication.
```

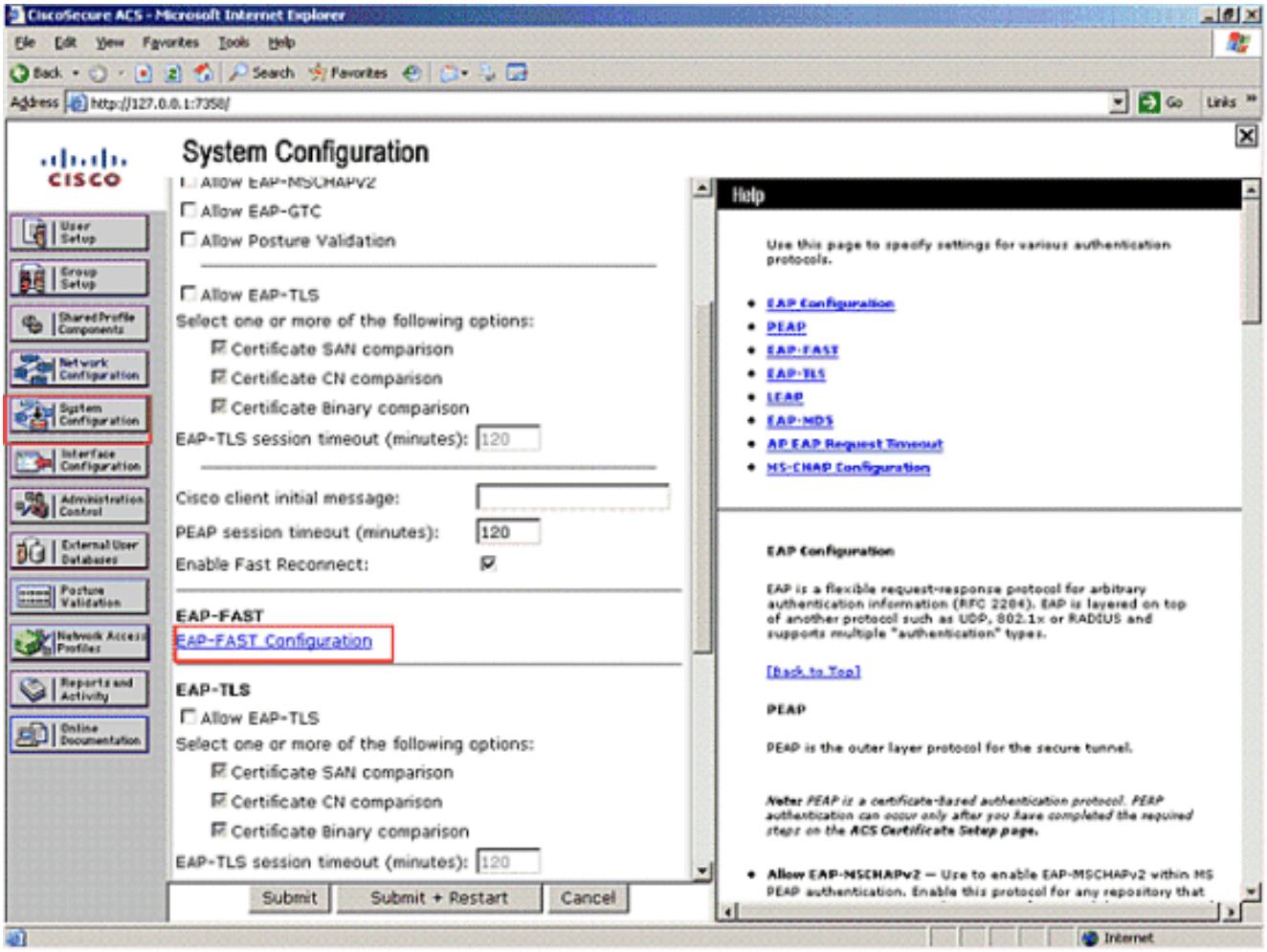
Configurez le serveur de RAYON

Le RECOUVREMENT est authentifié avec l'EAP-FAST. Assurez-vous que le serveur de RAYON vous utilisent des supports cette méthode d'EAP. Dans cet exemple, le serveur ACS est utilisé pour l'authentification. Terminez-vous ces étapes sur le serveur ACS :

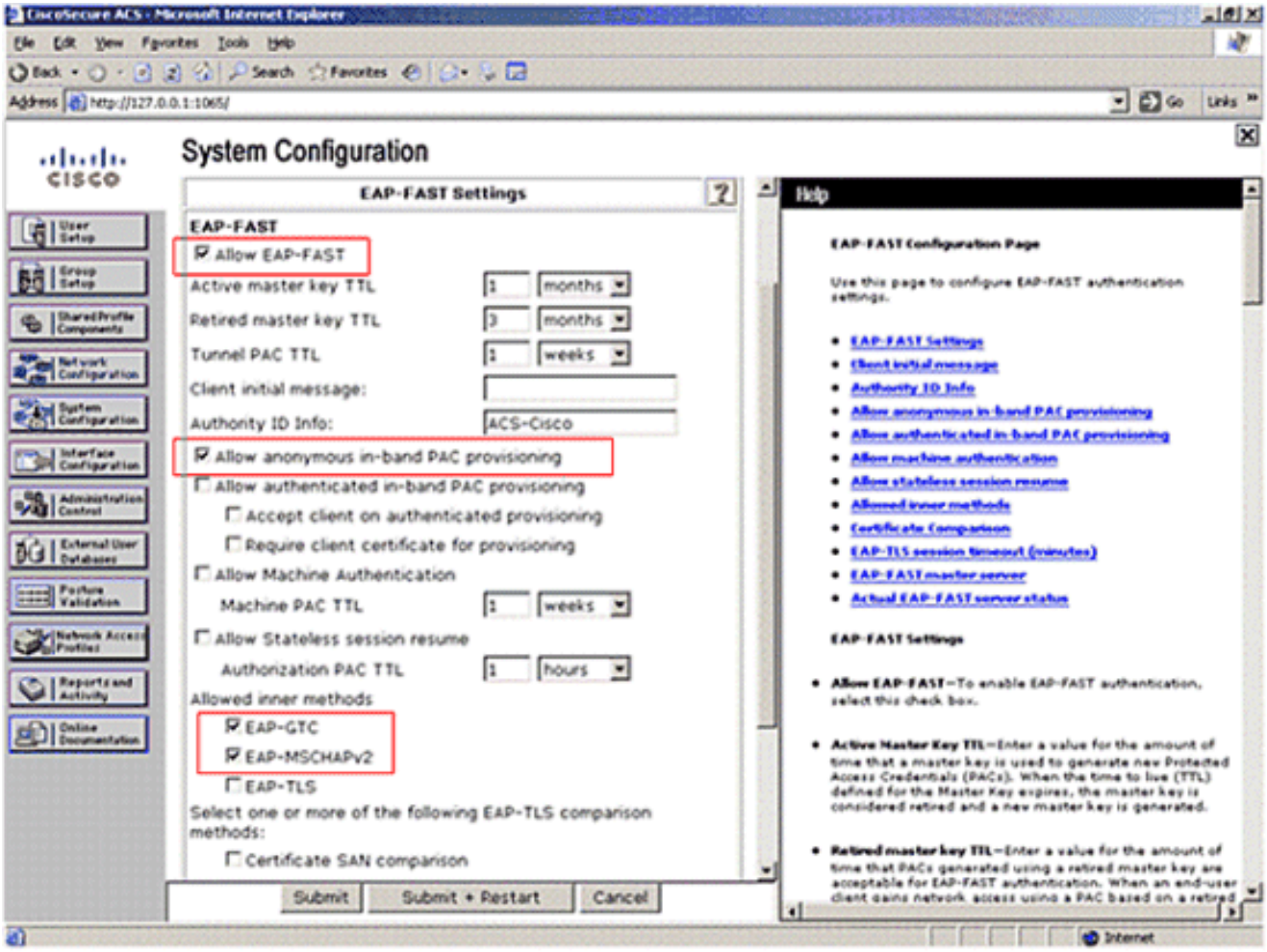
1. Lancez l'écran d'admin ACS.
2. Configurez le nom d'utilisateur et mot de passe du RECOUVREMENT dans la base de données ACS. Afin d'ajouter un compte utilisateur dans l'ACS, référez-vous à la section de gestion des utilisateurs du guide utilisateur de document pour le Cisco Secure Access Control Server 4.2.
3. Configurez le commutateur en tant que client d'AAA au serveur ACS. Sur l'écran d'admin ACS, cliquez sur le **menu Network Configuration**.
4. Sous la section de **client d'AAA**, cliquez sur Add la **nouvelle entrée**. Entrez ces paramètres :Écrivez l'adresse IP du commutateur dans le *champ IP Address de client d'AAA*.Écrivez le secret partagé du commutateur. Ceci doit être exactement identique sur le commutateur et le serveur ACS.Choisissez un **protocole RADIUS** dans l'*authentifier utilisant le* champ. Par défaut, c'est TACACS+.**Remarque:** Vérifiez le serveur ACS pour une description des protocoles RADIUS.Voir la figure 3.**Figure 3**



5. Cliquez sur Submit **+ appliquez** pour sauvegarder le client d'AAA.
6. L'EAP-FAST doit être activé sur le serveur de RAYON. Cliquez sur le menu de **configuration système** dans le côté gauche. Cliquez sur l'**option de configuration globale d'authentification**.**Figure 4**



7. **Configuration d'EAP-FAST de** clic suivant les indications de figure 4.
8. Sur la page Settings d'EAP-FAST, cochez la case d'**EAP-FAST d'autoriser**. Le RECOUVREMENT utilise l'EAP-FAST avec le ravitaillement anonyme PAC. Cochez la case **anonyme de ravitaillement PAC d'intrabande d'autoriser**. Le pour en savoir plus, se rapportent à l'authentification d'EAP-FAST de document avec l'exemple Sans fil de contrôleurs LAN et de configuration de serveur RADIUS externe.**Figure 5**



9. Assurez-vous qu'**EAP-GTC** et **EAP-MSCHAPv2** sont vérifiés dessous *permettent des méthodes intérieures*. La figure 5 affiche une configuration d'échantillon des étapes 8 et 9.

Vérifiez

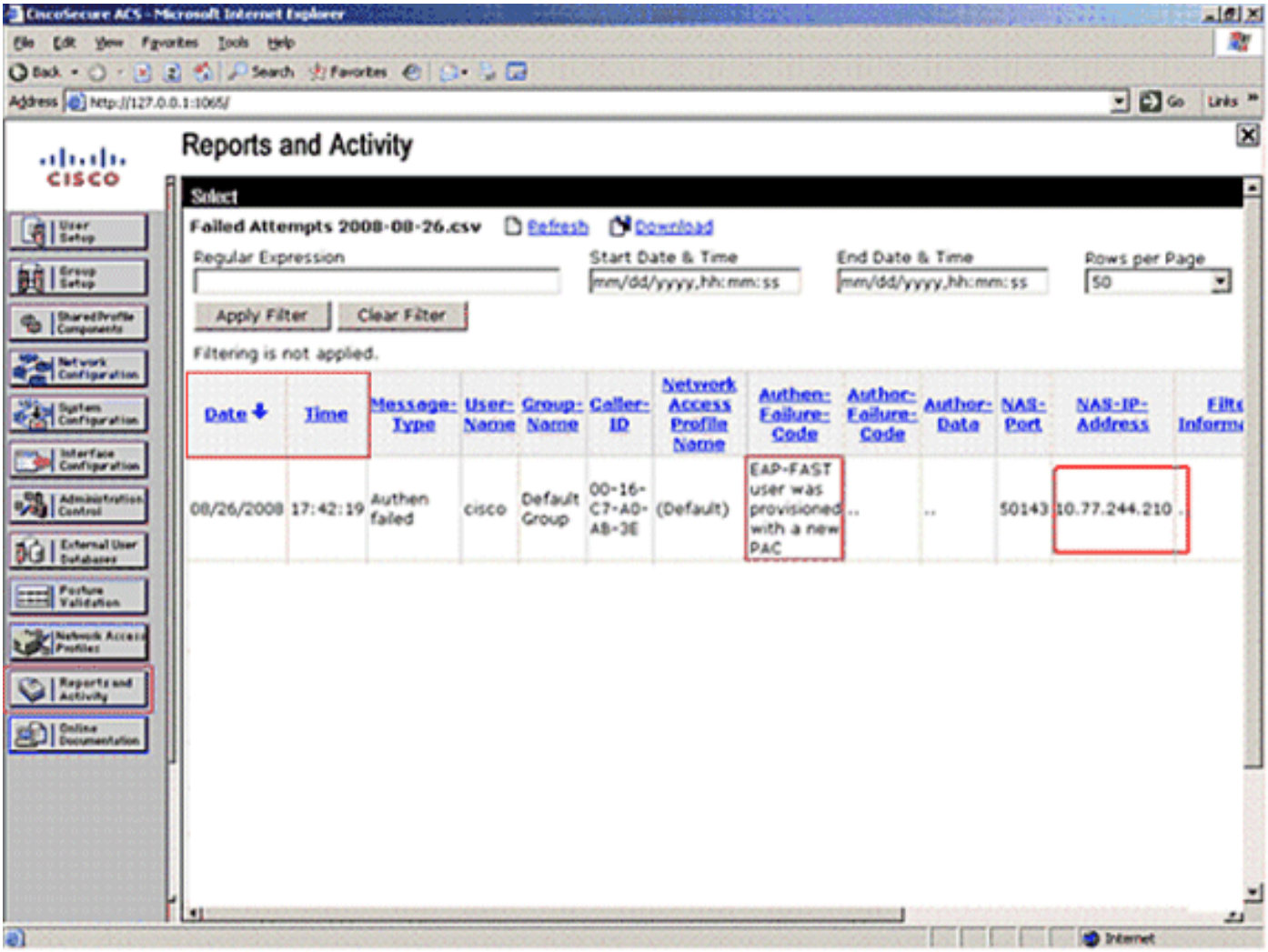
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Une fois que le 802.1x est activé sur le port de commutateur, tout le trafic excepté le trafic de 802.1x est bloqué par le port. Le RECOUVREMENT, qui est déjà enregistré au WLC, obtient dissocié. Seulement après qu'une authentification réussie de 802.1x est l'autre trafic permis pour traverser. L'enregistrement réussi du RECOUVREMENT au WLC après que le 802.1x soit activé sur le commutateur indique que l'authentification de RECOUVREMENT est réussie.

Vous pouvez également vérifier ceci d'ACS. De l'écran principal ACS, cliquez sur le menu d'**états et d'authentification**. Cliquez sur l'option d'**essais ratés**. Si l'authentification est réussie, vous trouvez un message d'*échec de l'authentification* avec l'*utilisateur d'EAP-FAST de* code *provisioned avec un nouveau PAC avec l'IP address du commutateur* dans le domaine de Nas-IP-adresse suivant les indications de la figure 6. Vous pouvez également confirmer avec la date et l'heure de l'authentification.

Figure 6



Dépannez

Utilisez cette section pour dépanner votre configuration.

1. Utilisez la **commande ping** et le contrôle si le serveur ACS est accessible du commutateur.
2. Assurez-vous que le commutateur est configuré en tant que client d'AAA sur le serveur ACS.
3. Assurez-vous que le secret partagé est identique entre le commutateur et le serveur ACS.
4. Vérifiez si l'EAP-FAST est activé sur le serveur ACS.
5. Vérifiez la conformité de logiciel sur les périphériques.
6. Vérifiez si les qualifications de 802.1x sont configurées pour le RECOUVREMENT et sont mêmes sur le serveur ACS.**Remarque:** Le nom d'utilisateur et mot de passe distinguent les majuscules et minuscules.

Dépannage des commandes

Il n'y a actuellement aucune commande de débogage disponible pour cette caractéristique.

Informations connexes

- Contrôle des points d'accès légers
- Configurer l'authentification basée sur port de 802.1x d'IEEE

- Support et documentation techniques - Cisco Systems