Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant CatOS

Contenu

Introduction

Ce document explique comment configurer le 802.1x d'IEEE sur un Catalyst 6500/6000 que cela exécute en mode hybride (CatOS sur l'engine de superviseur et logiciel de Cisco IOS® sur le MSFC) et serveur de Service RADIUS (Remote Authentication Dial-In User Service) pour l'authentification et l'affectation VLAN.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Guide d'installation pour le Cisco Secure ACS pour Windows 4.1
- Guide utilisateur pour le Cisco Secure Access Control Server 4.1
- Fonctionnement de RADIUS
- Commutation de Catalyst et guide de déploiement ACS

Composants utilisés

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

- Catalyst 6500 qui exécute la version de logiciel 8.5(6) de CatOS sur l'engine de superviseur et le Logiciel Cisco IOS version 12.2(18)SXF sur le MSFC**Remarque:** Vous avez besoin prendre en charge de la version 6.2 de CatOS ou plus tard l'authentification basée sur port de 802.1x.**Remarque:** Avant que la version de logiciel 7.2(2), une fois que le serveur de 802.1x est authentifié, il joigne un VLAN NVRAM-configuré. Avec des versions de version de logiciel 7.2(2) et ultérieures, après authentification, un serveur de 802.1x peut recevoir son affectation VLAN du serveur de RAYON.
- Cet exemple utilise le Cisco Secure Access Control Server (ACS) 4.1 en tant que serveur de RAYON.**Remarque:** Un serveur de RAYON doit être spécifié avant d'activer le 802.1x sur le commutateur.
- Clients PC qui prend en charge l'authentification de 802.1x.**Remarque:** Cet exemple utilise des clients de Microsoft Windows XP.

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

La norme de 802.1x d'IEEE définit un client-serveur - le protocole basé de contrôle d'accès et d'authentification qui limite les périphériques non autorisés de se connecter à un RÉSEAU LOCAL par les ports publiquement accessibles. le 802.1x contrôle l'accès au réseau en créant deux Points d'accès virtuels distincts à chaque port. Un Point d'accès est un port incontrôlé ; l'autre est un port commandé. Tout le trafic par le port unique est disponible aux deux Points d'accès. le 802.1x authentifie chaque périphérique d'utilisateur qui est connecté à un port de commutateur et assigne le port à un VLAN avant de faire disponible tous les services qui sont offerts par le commutateur ou le RÉSEAU LOCAL. Jusqu'à ce que le périphérique soit authentifié, le contrôle d'accès de 802.1x permet seulement le Protocole EAP (Extensible Authentication Protocol) au-dessus du trafic du RÉSEAU LOCAL (EAPOL) par le port auquel le périphérique est connecté. Après l'authentification est réussie, le trafic normal peut traverser le port.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer la fonction décrite de 802.1x dans ce document.

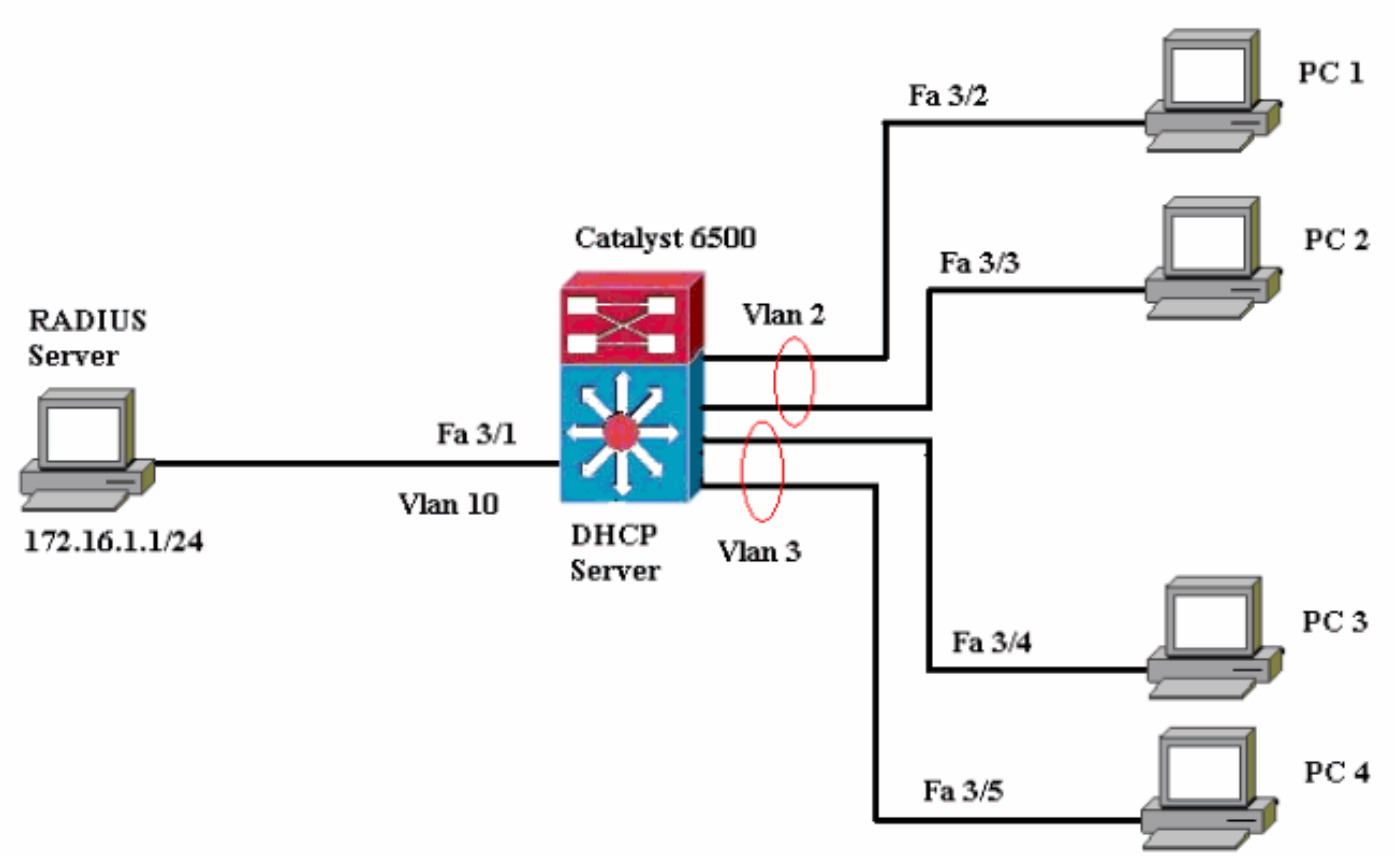
Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Cette configuration requiert les étapes suivantes :

- Configurez le commutateur de Catalyst pour l'authentification de 802.1x
- Configurez le serveur de RAYON
- Configurez les clients PC pour utiliser l'authentification de 802.1x

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



- Serveur de RAYON — Exécute l'authentification réelle du client. Le serveur de RAYON valide l'identité du client et informe le commutateur si le client est autorisé à accéder au RÉSEAU LOCAL et à commuter des services. Ici, le serveur de RAYON est configuré pour l'authentification et l'affectation VLAN.
- Commutateur — Contrôle l'accès physique au réseau basé sur l'état d'authentification du client. Le commutateur agit en tant qu'intermédiaire (proxy) entre le client et le serveur de RAYON, demandant les informations d'identité du client, vérifiant ces informations avec le serveur de RAYON, et transmettant par relais une réponse au client. Ici, le commutateur de Catalyst 6500 est également configuré comme serveur DHCP. Le soutien d'authentification de 802.1x du protocole DHCP (DHCP) permet au serveur DHCP pour assigner les adresses IP aux classes différentes d'utilisateurs finaux en ajoutant l'identité de l'utilisateur authentifiée dans le processus de découverte DHCP.
- Clients — Les périphériques (postes de travail) cet accès de demande au RÉSEAU LOCAL et aux services de commutateur et répondent aux demandes du commutateur. Ici, PC 1 4 sont les clients qui demandent un accès au réseau authentifié. PC 1 et 2 emploieront le même laisser-passer de connexion pour être dans le VLAN 2. De même, PC 3 et 4 utiliseront un laisser-passer de connexion pour des clients PC VLAN 3. sont configurés pour atteindre

l'adresse IP d'un serveur DHCP.**Remarque:** Dans cette configuration, n'importe quel client qui échoue l'authentification ou n'importe quel client capable non-802.1x se connectant au commutateur est refusé l'accès au réseau en les déplaçant à un VLAN inutilisé (VLAN 4 ou 5) utilisant les caractéristiques d'échec d'authentification et de VLAN invité.

Configurez le commutateur de Catalyst pour l'authentification de 802.1x

Cette configuration de commutateur témoin inclut :

- Activez l'authentification de 802.1x et les caractéristiques associées sur des ports FastEthernets.
- Connectez le serveur de RAYON au VLAN 10 derrière le port FastEthernet 3/1.
- Configuration du serveur DHCP pour deux groupes IP, un pour des clients dans le VLAN 2 et autre pour des clients dans le VLAN 3.
- Routage inter-VLAN pour avoir la Connectivité entre les clients après authentification.

Référez-vous aux instructions de configuration d'authentification pour les instructions sur la façon dont configurer l'authentification de 802.1x.

Remarque: Assurez-vous que le serveur de RAYON se connecte toujours derrière un port autorisé.

Catalyst 6500

```
Console (enable) set system name Cat6K System name set.
!--- Sets the hostname for the switch. Cat6K> (enable)
set localuser user admin password cisco Added local user
admin. Cat6K> (enable) set localuser authentication
enable LocalUser authentication enabled !--- Uses local
user authentication to access the switch. Cat6K>
(enable) set vtp domain cisco VTP domain cisco modified
!--- Domain name must be configured for VLAN
configuration. Cat6K> (enable) set vlan 2 name VLAN2 VTP
advertisements transmitting temporarily stopped, and
will resume after the command finishes. Vlan 2
configuration successful !--- VLAN should be existing in
the switch !--- for a successsful authentication. Cat6K>
(enable) set vlan 3 name VLAN3 VTP advertisements
transmitting temporarily stopped, and will resume after
the command finishes. Vlan 3 configuration successful !-
-- VLAN names will be used in RADIUS server for VLAN
assignment. Cat6K> (enable) set vlan 4 name
AUTHFAIL_VLAN VTP advertisements transmitting
temporarily stopped, and will resume after the command
finishes. Vlan 4 configuration successful !--- A VLAN
for non-802.1x capable hosts. Cat6K> (enable) set vlan 5
name GUEST_VLAN VTP advertisements transmitting
temporarily stopped, and will resume after the command
finishes. Vlan 4 configuration successful !--- A VLAN
for failed authentication hosts. Cat6K> (enable) set
vlan 10 name RADIUS_SERVER VTP advertisements
transmitting temporarily stopped, and will resume after
the command finishes. Vlan 10 configuration successful
!--- This is a dedicated VLAN for the RADIUS Server.
Cat6K> (enable) set interface sc0 10 172.16.1.2
255.255.255.0 Interface sc0 vlan set, IP address and
netmask set. !--- Note: 802.1x authentication always
uses the !--- sc0 interface as the identifier for the
authenticator !--- when communicating with the RADIUS
```

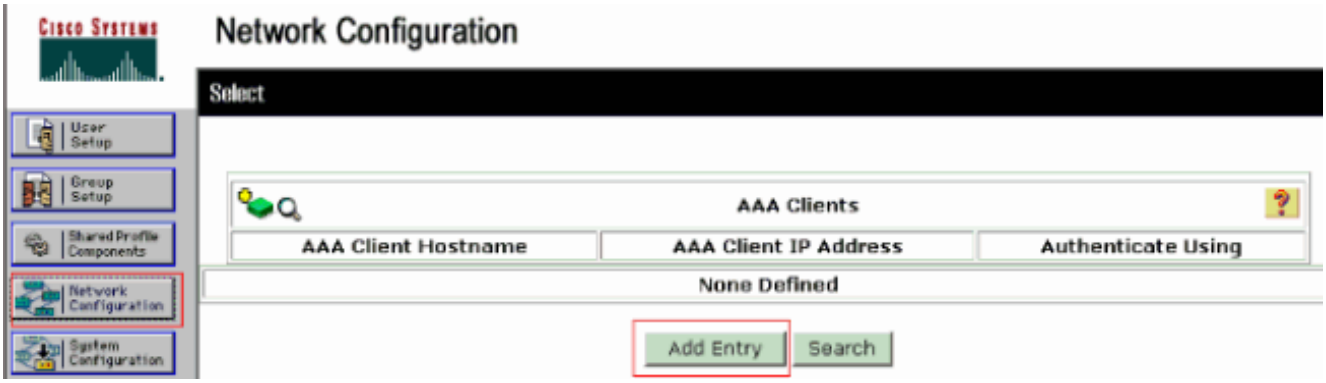
server. Cat6K> (enable) **set vlan 10 3/1** VLAN 10 modified. VLAN 1 modified. VLAN Mod/Ports ---- ---------- 10 3/1 *!--- Assigns port connecting to RADIUS server to VLAN 10.* Cat6K> (enable) **set radius server 172.16.1.1 primary** 172.16.1.1 with auth-port 1812 acct-port 1813 added to radius server table as primary server. *!--- Sets the IP address of the RADIUS server.* Cat6K> (enable) **set radius key cisco** Radius key set to cisco *!--- The key must match the key used on the RADIUS server.* Cat6K> (enable) **set dot1x system-auth-control enable** dot1x system-auth-control enabled. Configured RADIUS servers will be used for dot1x authentication. *!--- Globally enables 802.1x. !--- You must specify at least one RADIUS server before !--- you can enable 802.1x authentication on the switch.* Cat6K> (enable) **set port dot1x 3/2-48 port-control auto** Port 3/2-48 dot1x port-control is set to auto. Trunking disabled for port 3/2-48 due to Dot1x feature. Spantree port fast start option enabled for port 3/2-48. *!--- Enables 802.1x on all FastEthernet ports. !--- This disables trunking and enables portfast automatically.* Cat6K> (enable) **set port dot1x 3/2-48 auth-fail-vlan 4** Port 3/2-48 Auth Fail Vlan is set to 4 *!--- Ports will be put in VLAN 4 after three !--- failed authentication attempts.* Cat6K> (enable) **set port dot1x 3/2-48 guest-vlan 5** Ports 3/2-48 Guest Vlan is set to 5 *!--- Any non-802.1x capable host connecting or 802.1x !--- capable host failing to respond to the username and password !--- authentication requests from the Authenticator is placed in the !--- guest VLAN after 60 seconds. !--- **Note:** An authentication failure VLAN is independent !--- of the guest VLAN. However, the guest VLAN can be the same !--- VLAN as the authentication failure VLAN. If you do not want to !--- differentiate between the non-802.1x capable hosts and the !--- authentication failed hosts, you can configure both hosts to !--- the same VLAN (either a guest VLAN or an authentication failure VLAN). !--- For more information, refer to !--- Understanding How 802.1x Authentication for the Guest VLAN Works.* Cat6K> (enable) **switch console** Trying Router-16... Connected to Router-16. Type ^C^C^C to switch back... *!--- Transfers control to the routing module (MSFC).* Router>**enable** Router#**conf t** Enter configuration commands, one per line. End with CNTL/Z. Router(config)#**interface vlan 10** Router(config-if)#**ip address 172.16.1.3 255.255.255.0** *!--- This is used as the gateway address in RADIUS server.* Router(config-if)#**no shut** Router(config-if)#**interface vlan 2** Router(config-if)#**ip address 172.16.2.1 255.255.255.0** Router(config-if)#**no shut** *!--- This is the gateway address for clients in VLAN 2.* Router(config-if)#**interface vlan 3** Router(config-if)#**ip address 172.16.3.1 255.255.255.0** Router(config-if)#**no shut** *!--- This is the gateway address for clients in VLAN 3.* Router(config-if)#**exit** Router(config)#**ip dhcp pool vlan2_clients** Router(dhcp-config)#**network 172.16.2.0 255.255.255.0** Router(dhcp-config)#**default-router 172.16.2.1** *!--- This pool assigns ip address for clients in VLAN 2.* Router(dhcp-config)#**ip dhcp pool vlan3_clients** Router(dhcp-config)#**network 172.16.3.0 255.255.255.0** Router(dhcp-config)#**default-router 172.16.3.1** *!--- This pool assigns ip address for clients in VLAN 3.* Router(dhcp-config)#**exit** Router(config)#**ip dhcp excluded-address 172.16.2.1** Router(config)#**ip dhcp excluded-address 172.16.3.1** *!--- In order to go back to*

```
the Switching module, !--- enter Ctrl-C three times.
Router# Router#^C Cat6K> (enable) Cat6K> (enable) show
vlan VLAN Name Status IfIndex Mod/Ports, Vlans ---- ----
-------------- --------- ------- ----------------------
- 1 default active 6 2/1-2 3/2-48 2 VLAN2 active 83 3
VLAN3 active 84 4 AUTHFAIL_VLAN active 85 5 GUEST_VLAN
active 86 10 RADIUS_SERVER active 87 3/1 1002 fddi-
default active 78 1003 token-ring-default active 81 1004
fddinet-default active 79 1005 trnet-default active 80
!--- Output suppressed. !--- All active ports will be in
VLAN 1 (except 3/1) before authentication. Cat6K>
(enable) show dot1x PAE Capability Authenticator Only
Protocol Version 1 system-auth-control enabled max-req 2
quiet-period 60 seconds re-authperiod 3600 seconds
server-timeout 30 seconds shutdown-timeout 300 seconds
supp-timeout 30 seconds tx-period 30 seconds !---
Verifies dot1x status before authentication. Cat6K>
(enable)
```

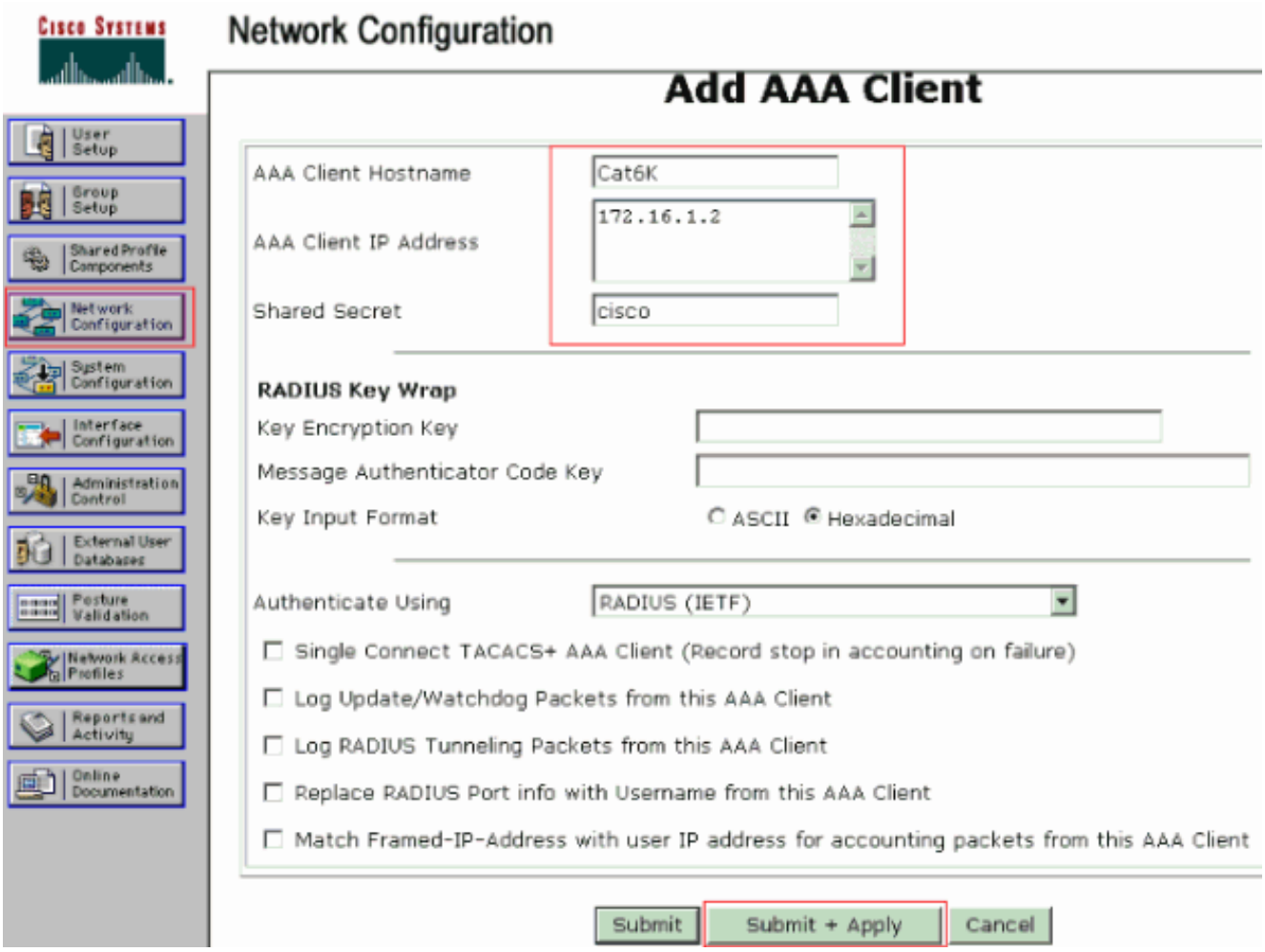
Configurez le serveur de RAYON

Le serveur de RAYON est configuré avec une adresse IP statique de 172.16.1.1/24. Terminez-vous ces étapes afin de configurer le serveur de RAYON pour un client d'AAA :

1. Afin de configurer un client d'AAA, cliquez sur Network Configuration sur la fenêtre de gestion ACS.
2. Cliquez sur Add l'**entrée** sous la section de clients d'AAA.



3. Configurez l'adresse Internet de client d'AAA, l'adresse IP, la clé secrète partagée et le type d'authentification en tant que :Adresse Internet de client d'AAA = nom de hôte du commutateur (**Cat6K**).Adresse IP de client d'AAA = interface de gestion (adresse sc0)IP du commutateur (**172.16.1.2**).Secret partagé = rayon clé configuré sur le commutateur (**Cisco**).Authentifiez utilisant = **IETF de RAYON**.**Remarque:** Pour l'exécution correcte, la clé secrète partagée doit être identique sur le client d'AAA et l'ACS. Les clés distinguent les majuscules et minuscules.
4. Cliquez sur Submit **+ appliquez** pour apporter ces modifications efficaces, comme indiqué dans cet exemple
   :

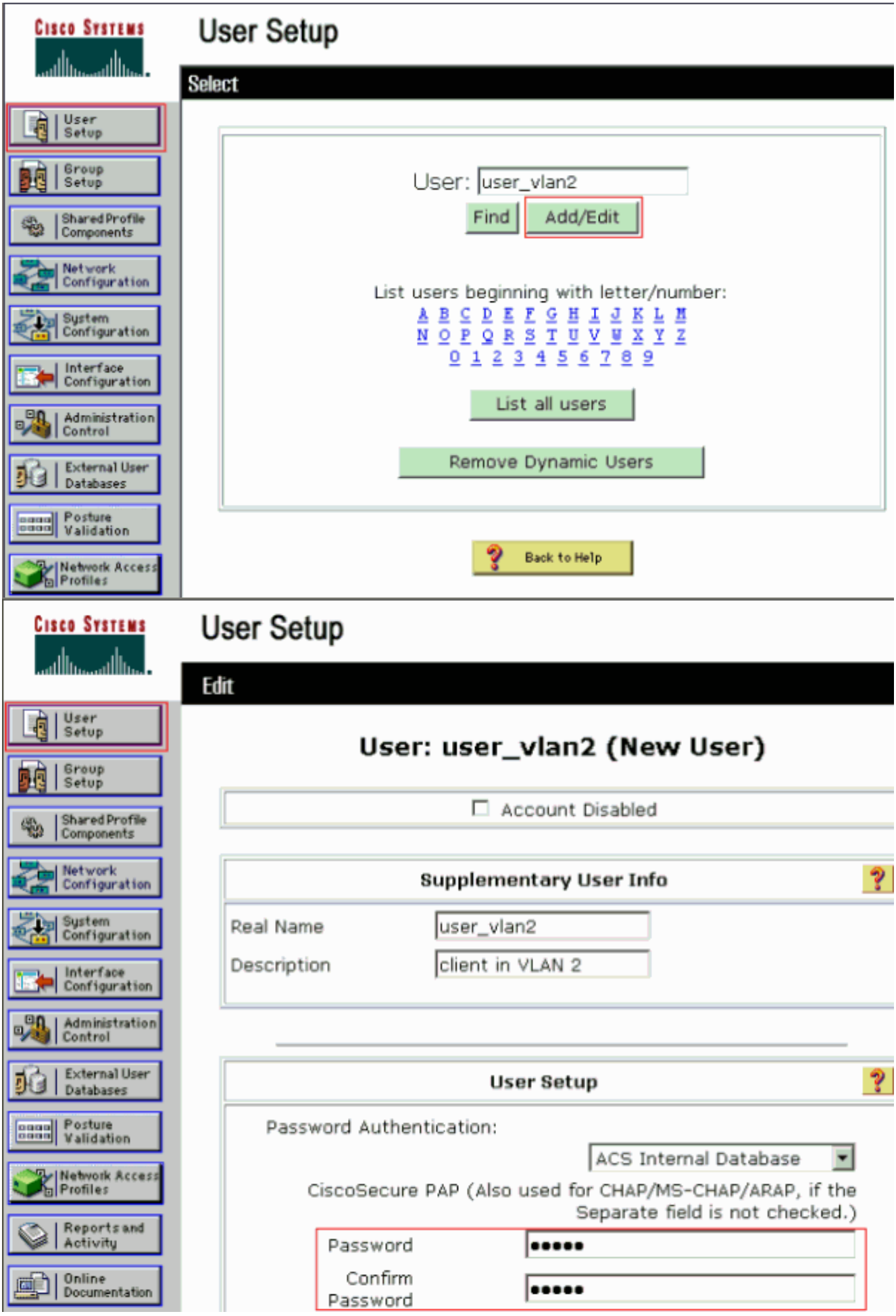


Terminez-vous ces étapes afin de configurer le serveur de RAYON pour l'authentification, le VLAN et l'affectation d'adresse IP :

Deux noms d'utilisateur doivent être créés séparément pour les clients qui se connectent au VLAN 2 aussi bien que pour le VLAN 3. Ici, un utilisateur **user_vlan2** pour des clients se connectant au VLAN 2 et un utilisateur différent **user_vlan3** pour des clients se connectant au VLAN 3 sont créés à cet effet.

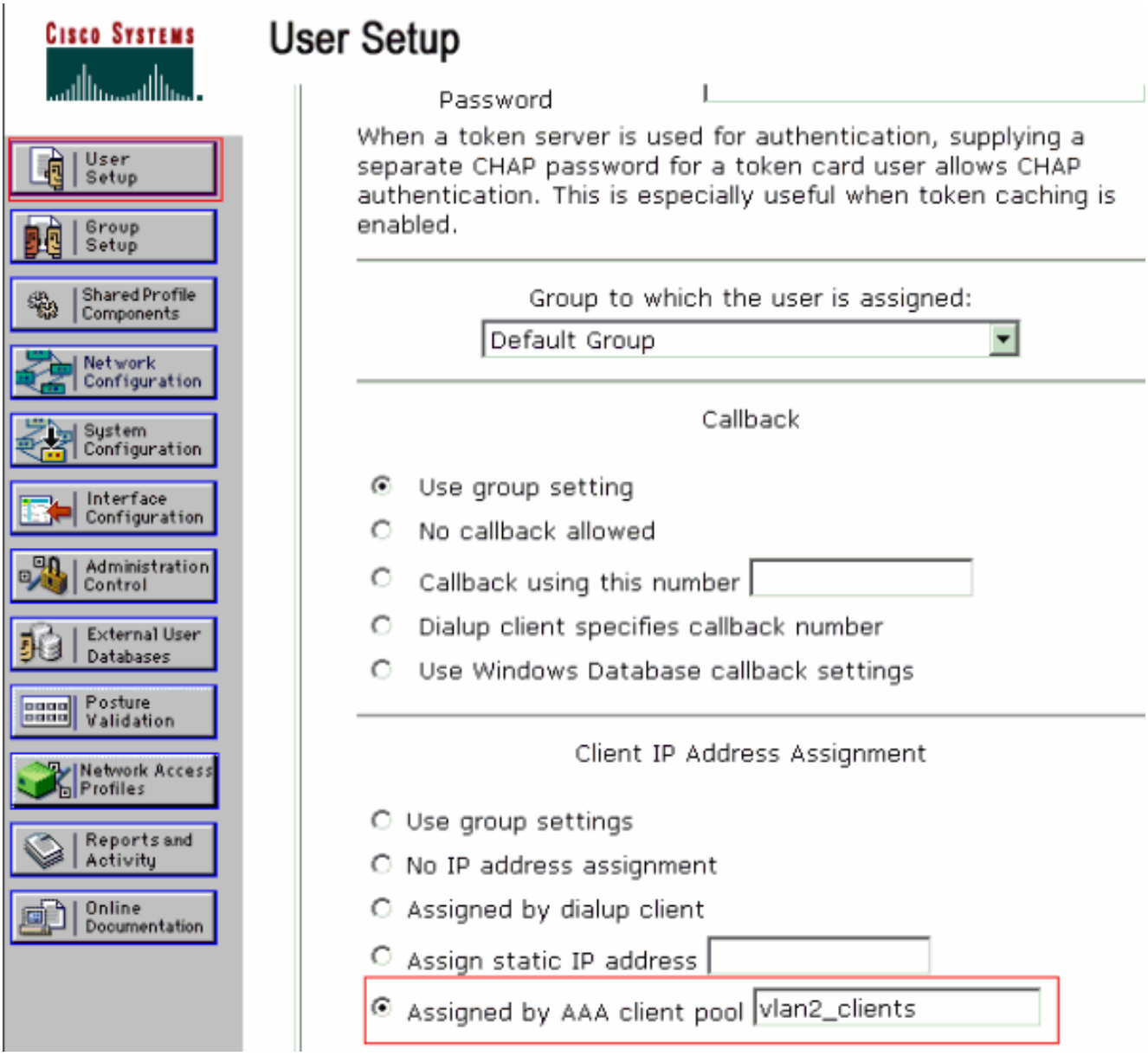
Remarque: Ici, la configuration utilisateur est affichée pour les clients qui se connectent au VLAN 2 seulement. Pour les utilisateurs qui se connectent au VLAN 3, remplissez la même procédure.

1. Afin d'ajouter et configurer des utilisateurs, cliquez sur User Setup et définissez le nom d'utilisateur et mot de
   passe.



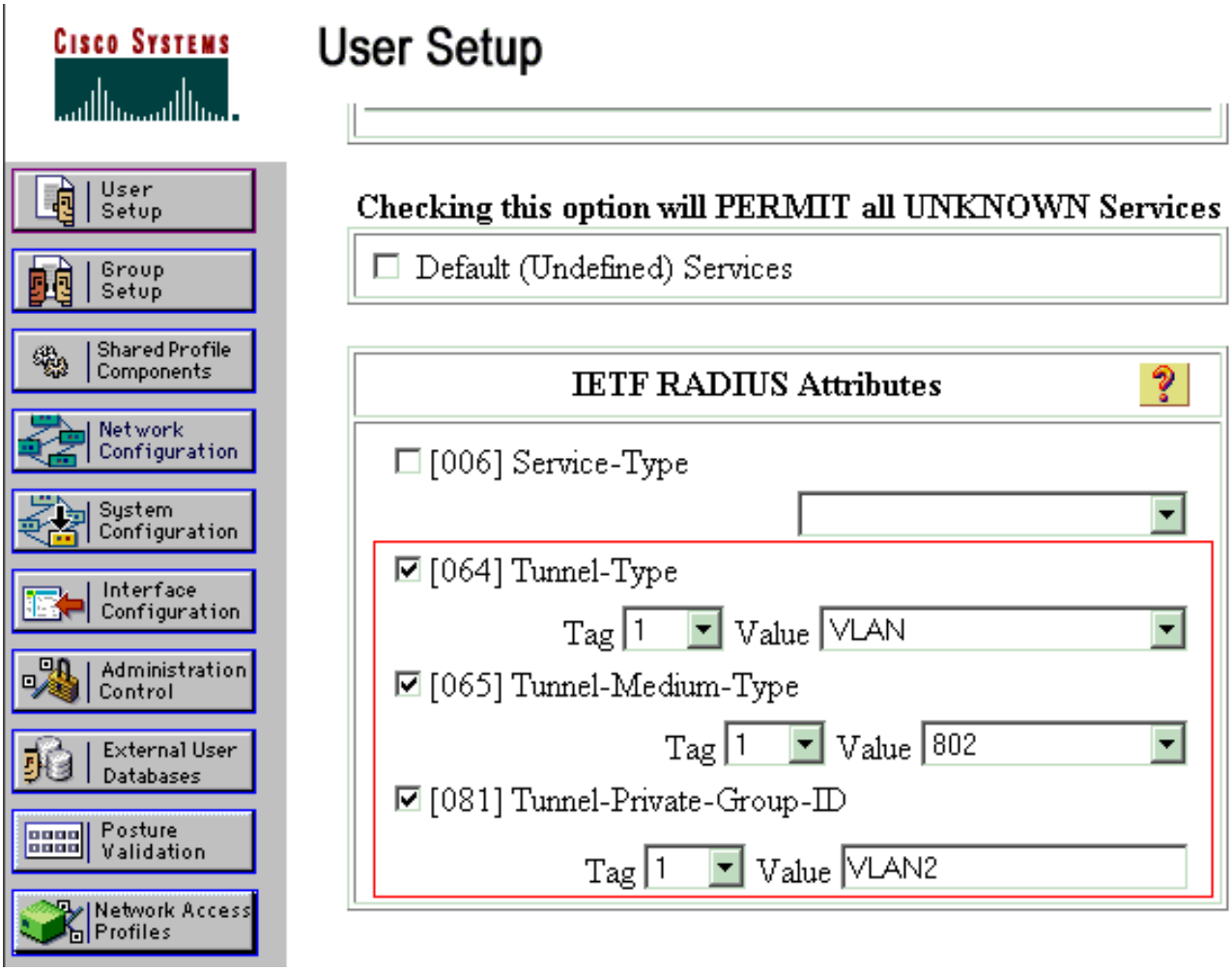
2. Définissez l'affectation d'adresse IP de client comme **assignée par le client pool d'AAA**. Écrivez le nom du groupe d'adresse IP configuré sur le commutateur pour les clients VLAN

2.



Remarque: Sélectionnez cette option et introduisez le nom de client ip pool d'AAA dans la case, seulement si cet utilisateur doit faire assigner l'adresse IP par un groupe d'adresse IP configuré sur le client d'AAA.

3. Définissez les attributs 64 et 65 de l'Internet Engineering Task Force (IETF).Assurez-vous que les balises des valeurs sont placés à 1, comme indiqué dans cet exemple. Le Catalyst ignore n'importe quelle balise autre que 1. afin d'affecter un utilisateur à une particularité VLAN, vous doit également définir l'attribut 81 avec un *nom* VLAN qui correspond.**Remarque:** *Le nom* VLAN devrait être exactement même que celui configuré dans le commutateur.**Remarque:** L'affectation VLAN basée sur le *nombre* VLAN n'est pas prise en charge avec
CatOS.

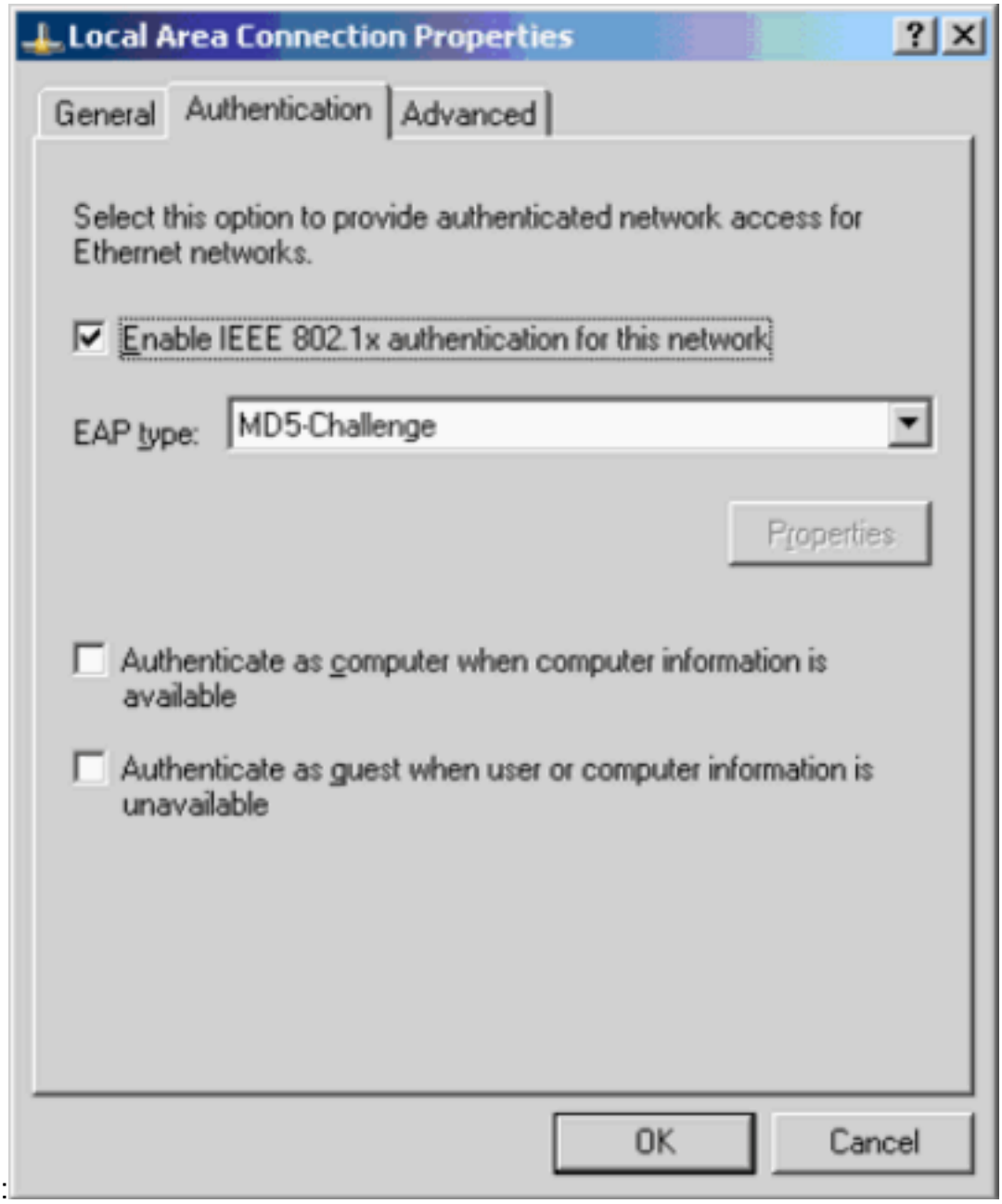


Référez-vous à RFC 2868 : Attributs RADIUS pour le support de Protocol de tunnel pour plus d'informations sur ces attributs IETF.**Remarque:** En configuration initiale du serveur ACS, les attributs RADIUS IETF peuvent pour afficher dans l'**installation utilisateur**. Choisissez la **configuration d'interface > le RAYON (IETF)** afin d'activer des attributs IETF dans l'écran de configuration utilisateur. Puis, le contrôle attribue **64**, **65**, et **81** dans les colonnes d'utilisateur et de groupe.

Configurez les clients PC pour utiliser l'authentification de 802.1x

Cet exemple est spécifique au Protocole EAP (Extensible Authentication Protocol) de Microsoft Windows XP au-dessus du client du RÉSEAU LOCAL (EAPOL). Procédez comme suit :

1. Choisissez le **début > le panneau de configuration > les connexions réseau**, puis cliquez avec le bouton droit sur votre **connexion au réseau local** et choisissez Properties.
2. Vérifiez l'**icône d'exposition dans la zone de notification une fois connecté** sous l'onglet Général.
3. Sous l'onglet d'authentification, **authentification de 802.1x d'IEEE d'enable de** contrôle **pour ce réseau**.
4. Placez le type d'EAP à **MD5-Challenge**, comme indiqué dans cet exemple

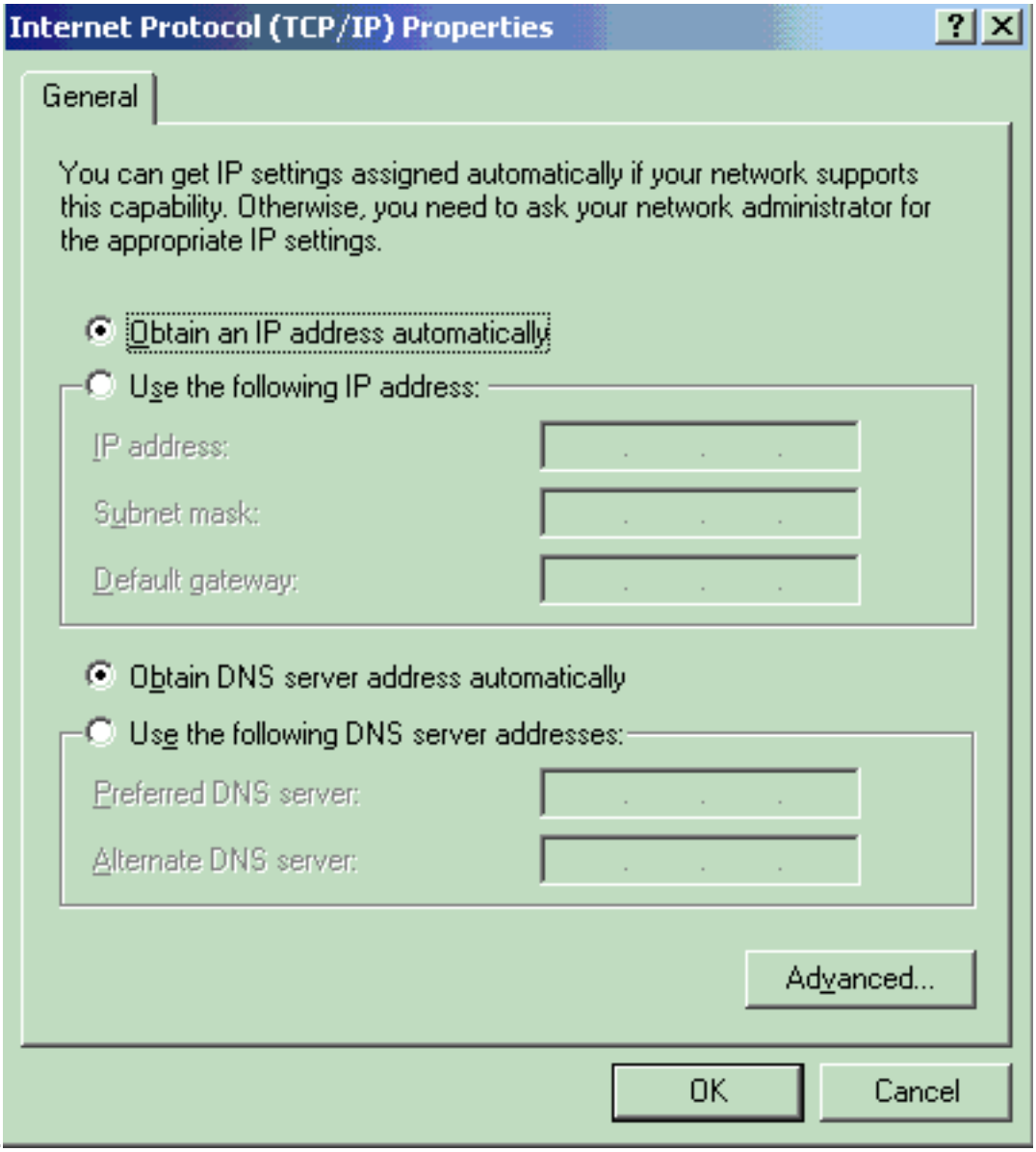


:

Terminez-vous ces étapes afin de configurer les clients pour obtenir une adresse IP d'un serveur DHCP :

1. Choisissez le **début > le panneau de configuration > les connexions réseau**, puis cliquez avec le bouton droit sur votre **connexion au réseau local** et choisissez Properties.
2. Sous l'onglet **General**, cliquez sur **Internet Protocol (TCP/IP)**, puis sur **Properties**.
3. Choisissez **Obtain an IP address**

automatically.



Vérifiez

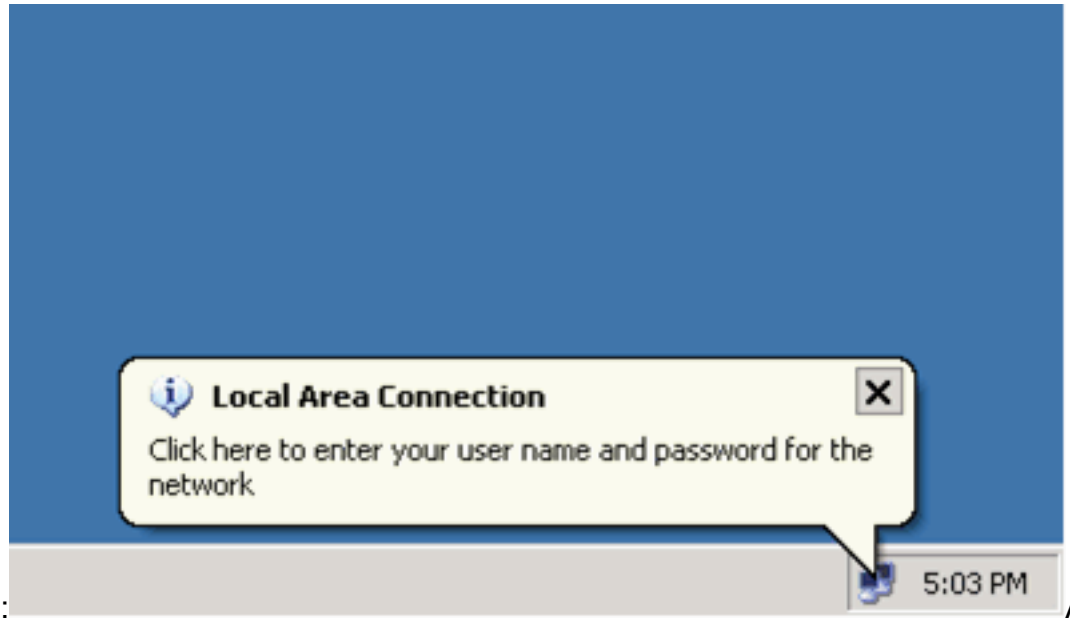
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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** .

Clients PC

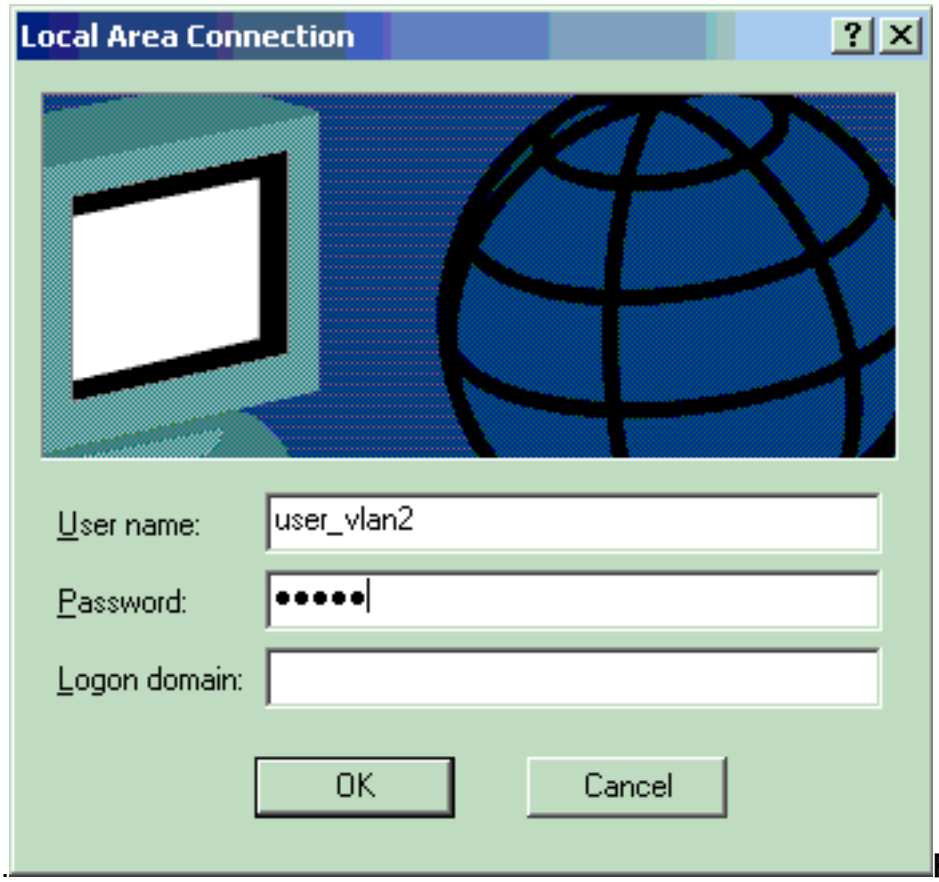
Si vous avez correctement complété la configuration, les clients PC affiche une demande instantanée pour écrire un nom d'utilisateur et mot de passe.

1. Cliquez sur en fonction la demande, que cet exemple affiche



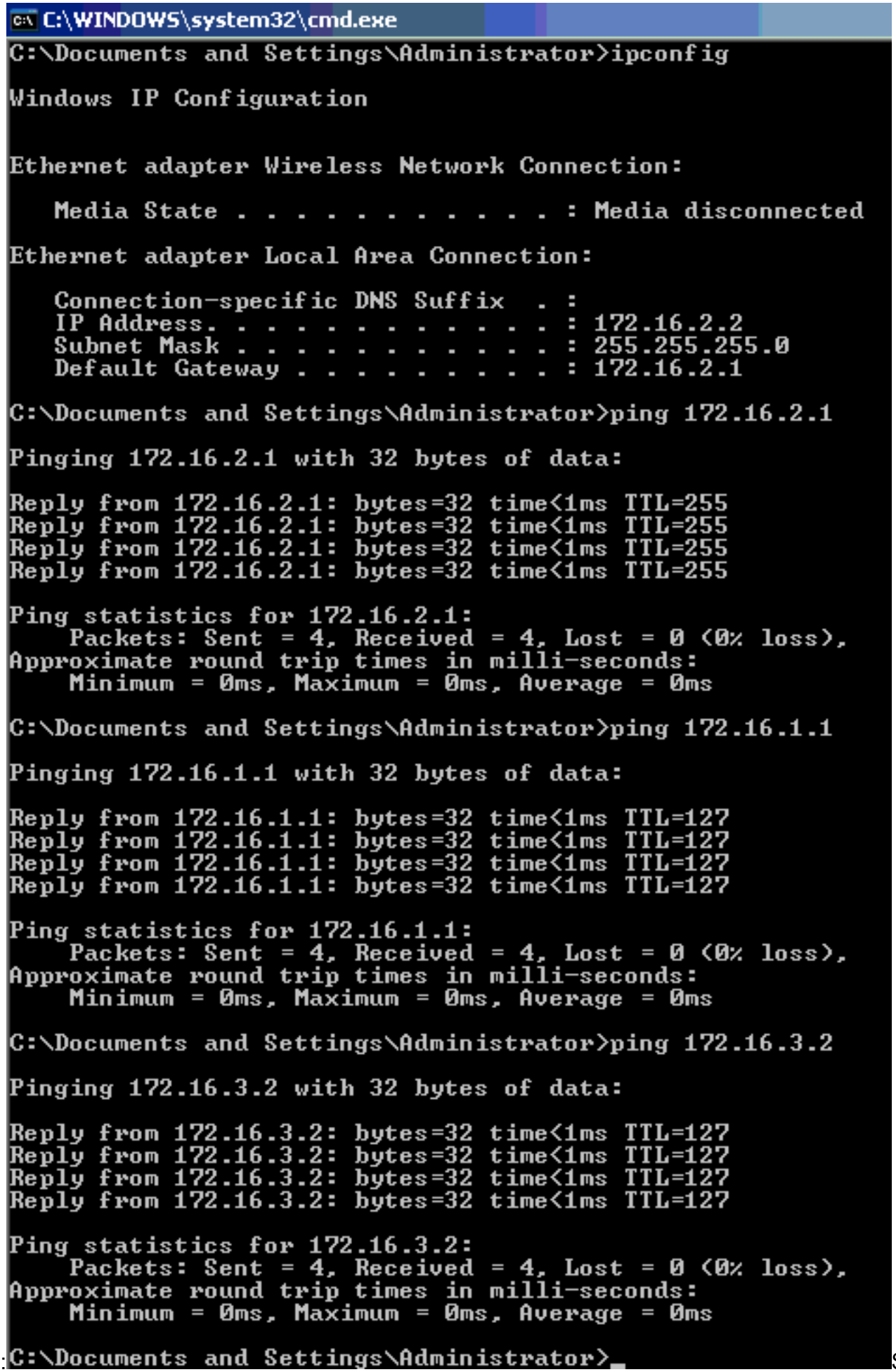
: Affichages d'une fenêtre d'entrée de nom d'utilisateur et mot de passe.

2. Saisissez le nom d'utilisateur et mot de passe.

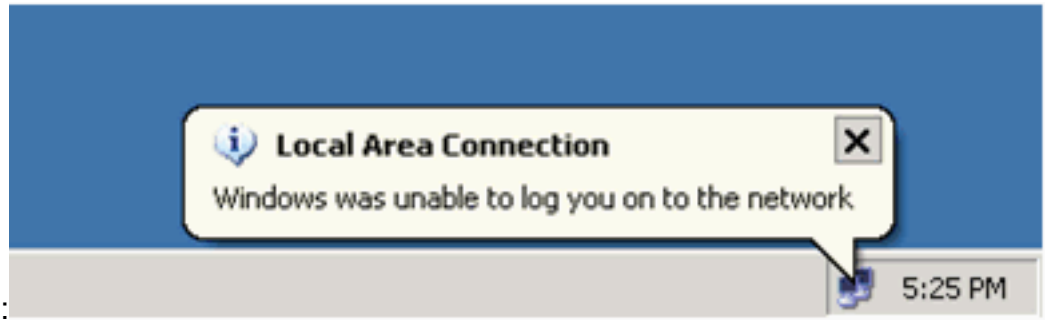


Remarque: Dans PC 1 et 2, écrivez les identifiants utilisateurs VLAN 2. Dans PC 3 et 4, écrivez les identifiants utilisateurs VLAN 3.

3. Si message d'erreur n'apparaît pas, vérifiez la Connectivité avec les méthodes habituelles, telles que l'accès traversant des ressources de réseau et avec la **commande ping**. C'est un résultat de PC 1, qui affiche un **ping** réussi à PC 4



: Si cette erreur apparaît, vérifiez que le nom d'utilisateur et mot de passe sont correct



:

Catalyst 6500

Si le mot de passe et le nom d'utilisateur semblent être corrects, vérifiez l'État du port de 802.1x sur le commutateur.

1. Recherchez un état de port qui indique autorisé.`Cat6K> (enable) **show port dot1x 3/1-5** Port Auth-State BEnd-State Port-Control Port-Status ----- ------------------ ---------- ------- ----------- ------------ ------------- 3/1 **force-authorized** idle force-authorized **authorized** *!--- This is the port to which RADIUS server is connected.* 3/2 **authenticated** idle auto **authorized** 3/3 **authenticated** idle auto **authorized** 3/4 **authenticated** idle auto **authorized** 3/5 **authenticated** idle auto **authorized** Port Port-Mode Re-authentication Shutdown-timeout ----- ------------ ---------- ---------------- ---------------- 3/1 SingleAuth disabled disabled 3/2 SingleAuth disabled disabled 3/3 SingleAuth disabled disabled 3/4 SingleAuth disabled disabled 3/5 SingleAuth disabled disabled` Vérifiez l'état VLAN après l'authentification réussie.`Cat6K> (enable) **show vlan** VLAN Name Status IfIndex Mod/Ports, Vlans ---- -------------------------------- ------ --- ------- ------------------------ 1 default active 6 2/1-2 3/6-48 **2 VLAN2 active 83 3/2-3 3 VLAN3 active 84 3/4-5** 4 AUTHFAIL_VLAN active 85 5 GUEST_VLAN active 86 10 RADIUS_SERVER active 87 3/1 1002 fddi-default active 78 1003 token-ring-default active 81 1004 fddinet-default active 79 1005 trnet-default active 80 *!--- Output suppressed.*`
2. Vérifiez l'état de liaison DHCP du module de routage (MSFC) après l'authentification réussie.`Router#**show ip dhcp binding** IP address Hardware address Lease expiration Type 172.16.2.2 0100.1636.3333.9c Feb 14 2007 03:00 AM Automatic 172.16.2.3 0100.166F.3CA3.42 Feb 14 2007 03:03 AM Automatic 172.16.3.2 0100.145e.945f.99 Feb 14 2007 03:05 AM Automatic 172.16.3.3 0100.1185.8D9A.F9 Feb 14 2007 03:07 AM Automatic`

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant Cisco IOS
- Commutation de Catalyst et guide de déploiement ACS
- RFC 2868 : Attributs RADIUS pour le support de Protocol de tunnel
- Configurer l'authentification de 802.1x
- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems