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

Contenu

Introduction

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

Conditions préalables

Conditions requises

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

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

Components Used

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

- Catalyst 6500 qui exécute le logiciel CatOS version 8.5(6) sur le Supervisor Engine et le logiciel Cisco IOS version 12.2(18)SXF sur la carte MSFC**Remarque :** Vous avez besoin de CatOS version 6.2 ou ultérieure pour prendre en charge l'authentification basée sur les ports 802.1x.**Remarque :** avant la version 7.2(2) du logiciel, une fois l'hôte 802.1x authentifié, il rejoint un VLAN configuré en mémoire NVRAM. Avec les versions 7.2(2) et ultérieures du logiciel, après authentification, un hôte 802.1x peut recevoir son affectation VLAN du serveur RADIUS.
- Cet exemple utilise Cisco Secure Access Control Server (ACS) 4.1 comme serveur RADIUS.**Remarque :** un serveur RADIUS doit être spécifié avant d'activer 802.1x sur le commutateur.
- Clients PC prenant en charge l'authentification 802.1x.**Remarque :** Cet exemple utilise des clients Microsoft Windows XP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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 IEEE 802.1x définit un protocole de contrôle d'accès et d'authentification basé sur le serveur client qui empêche les périphériques non autorisés de se connecter à un réseau local via des ports accessibles au public. 802.1x contrôle l'accès au réseau en créant deux points d'accès virtuels distincts sur chaque port. Un point d'accès est un port non contrôlé ; l'autre est un port contrôlé. Tout le trafic via le port unique est disponible pour les deux points d'accès. 802.1x authentifie chaque périphérique utilisateur connecté à un port de commutateur et attribue le port à un VLAN avant de rendre disponibles tous les services proposés par le commutateur ou le réseau local. Tant que le périphérique n'est pas authentifié, le contrôle d'accès 802.1x n'autorise que le trafic EAP (Extensible Authentication Protocol) sur le LAN (EAPOL) via le port auquel le périphérique est connecté. Une fois l'authentification réussie, le trafic normal peut passer par le port.

Configuration

Dans cette section, vous trouverez les informations nécessaires à la configuration de la fonctionnalité 802.1x décrite dans ce document.

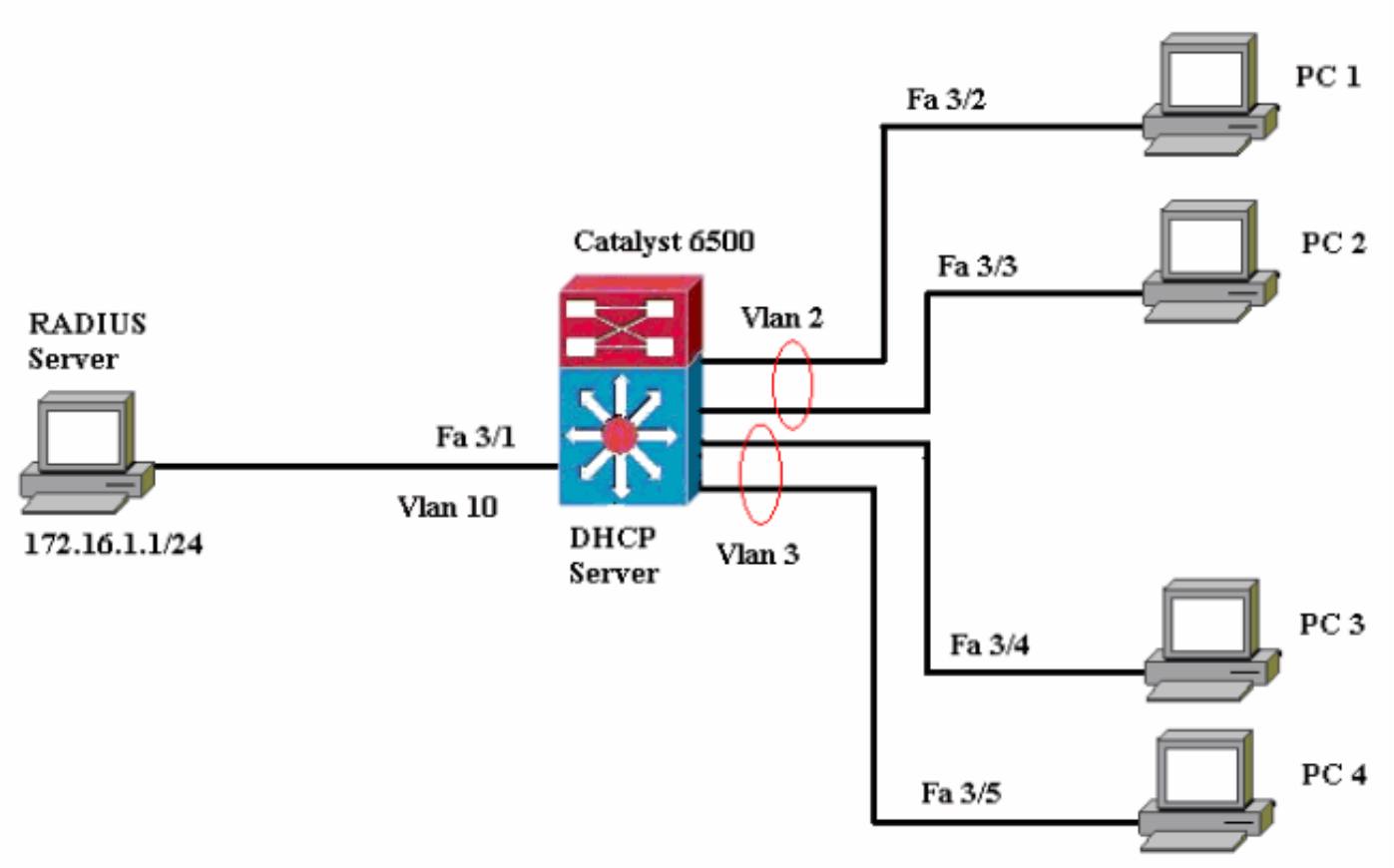
Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Cette configuration requiert les étapes suivantes :

- Configuration du commutateur Catalyst pour l'authentification 802.1x
- Configurer le serveur RADIUS
- Configurer les clients PC pour utiliser l'authentification 802.1x

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



- Serveur RADIUS : effectue l'authentification réelle du client. Le serveur RADIUS valide l'identité du client et indique au commutateur si le client est autorisé ou non à accéder aux services du réseau local et du commutateur. Ici, le serveur RADIUS est configuré pour l'authentification et l'affectation de VLAN.
- Switch : contrôle l'accès physique au réseau en fonction de l'état d'authentification du client. Le commutateur agit comme un intermédiaire (proxy) entre le client et le serveur RADIUS, demandant des informations d'identité au client, vérifiant ces informations avec le serveur RADIUS et relayant une réponse au client. Ici, le commutateur Catalyst 6500 est également configuré en tant que serveur DHCP. La prise en charge de l'authentification 802.1x pour le protocole DHCP (Dynamic Host Configuration Protocol) permet au serveur DHCP d'attribuer les adresses IP aux différentes classes d'utilisateurs finaux en ajoutant l'identité d'utilisateur authentifié dans le processus de détection DHCP.
- Clients : périphériques (stations de travail) qui demandent l'accès aux services LAN et de commutation et répondent aux demandes du commutateur. Ici, les PC 1 à 4 sont les clients qui demandent un accès réseau authentifié. Les PC 1 et 2 utilisent les mêmes informations d'identification de connexion que dans le VLAN 2. De même, les PC 3 et 4 utilisent des informations d'identification de connexion pour VLAN 3. Les clients PC sont configurés pour obtenir l'adresse IP à partir d'un serveur DHCP.**Remarque :** Dans cette configuration, tout client qui échoue à l'authentification ou tout client non compatible 802.1x se connectant au

commutateur se voit refuser l'accès au réseau en les déplaçant vers un VLAN inutilisé (VLAN 4 ou 5) à l'aide de l'échec d'authentification et des fonctionnalités du VLAN invité.

Configuration du commutateur Catalyst pour l'authentification 802.1x

Cet exemple de configuration de commutateur inclut :

- Activez l'authentification 802.1x et les fonctions associées sur les ports FastEthernet.
- Connectez le serveur RADIUS au VLAN 10 derrière le port FastEthernet 3/1.
- Configuration du serveur DHCP pour deux pools d'adresses IP, l'un pour les clients du VLAN 2 et l'autre pour les clients du VLAN 3.
- Routage entre réseaux locaux virtuels pour établir une connectivité entre les clients après authentification.

Reportez-vous aux Directives de configuration de l'authentification pour obtenir les instructions relatives à la configuration de l'authentification 802.1x.

Remarque : Assurez-vous que le serveur RADIUS 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
successful 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.
```

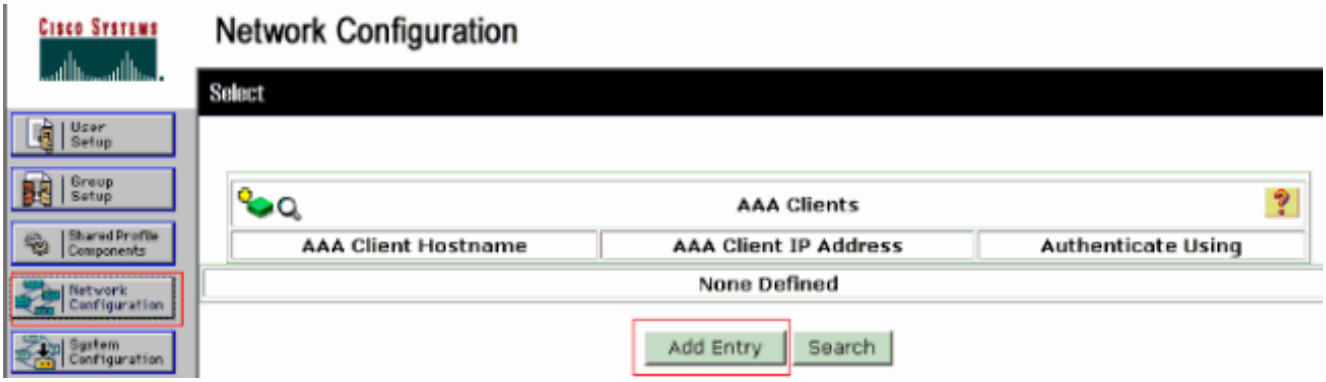
```
Router(config)#interface vlan 10
Router(config-if)#ip address 172.16.1.3 255.255.255.0
!--- This is used as the gateway address in RADIUS
server. Router(config-if)#no shut
Router(config-if)#interface vlan 2
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#no shut
!--- This 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)
```

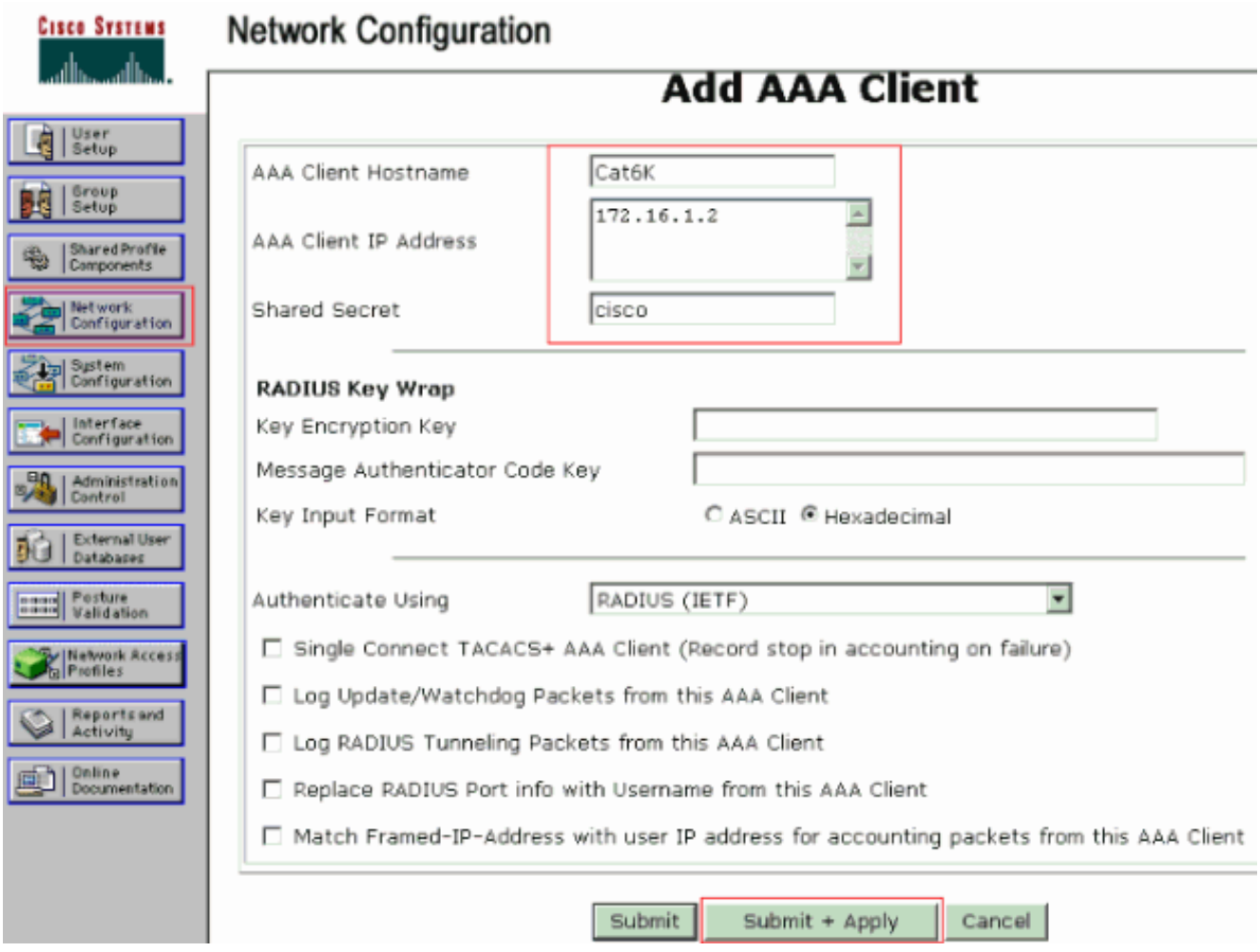
Configurer le serveur RADIUS

Le serveur RADIUS est configuré avec l'adresse IP statique 172.16.1.1/24. Complétez ces étapes afin de configurer le serveur RADIUS pour un client AAA :

1. Afin de configurer un client AAA, cliquez sur **Configuration réseau** dans la fenêtre d'administration ACS.
2. Cliquez sur **Ajouter une entrée** sous la section clients AAA.



3. Configurez le nom d'hôte du client AAA, l'adresse IP, la clé secrète partagée et le type d'authentification comme suit :Nom d'hôte du client AAA = Nom d'hôte du commutateur (**Cat6K**).Adresse IP du client AAA = Adresse IP de l'interface de gestion (sc0)du commutateur (**172.16.1.2**).Shared Secret = Radius Key configuré sur le commutateur (**cisco**).Authentifier à l'aide de = **RADIUS IETF**.**Remarque :** pour un fonctionnement correct, la clé secrète partagée doit être identique sur le client AAA et ACS. Les touches sont sensibles à la casse.
4. Cliquez sur **Soumettre + Appliquer** pour que ces modifications prennent effet, comme le montre cet exemple :

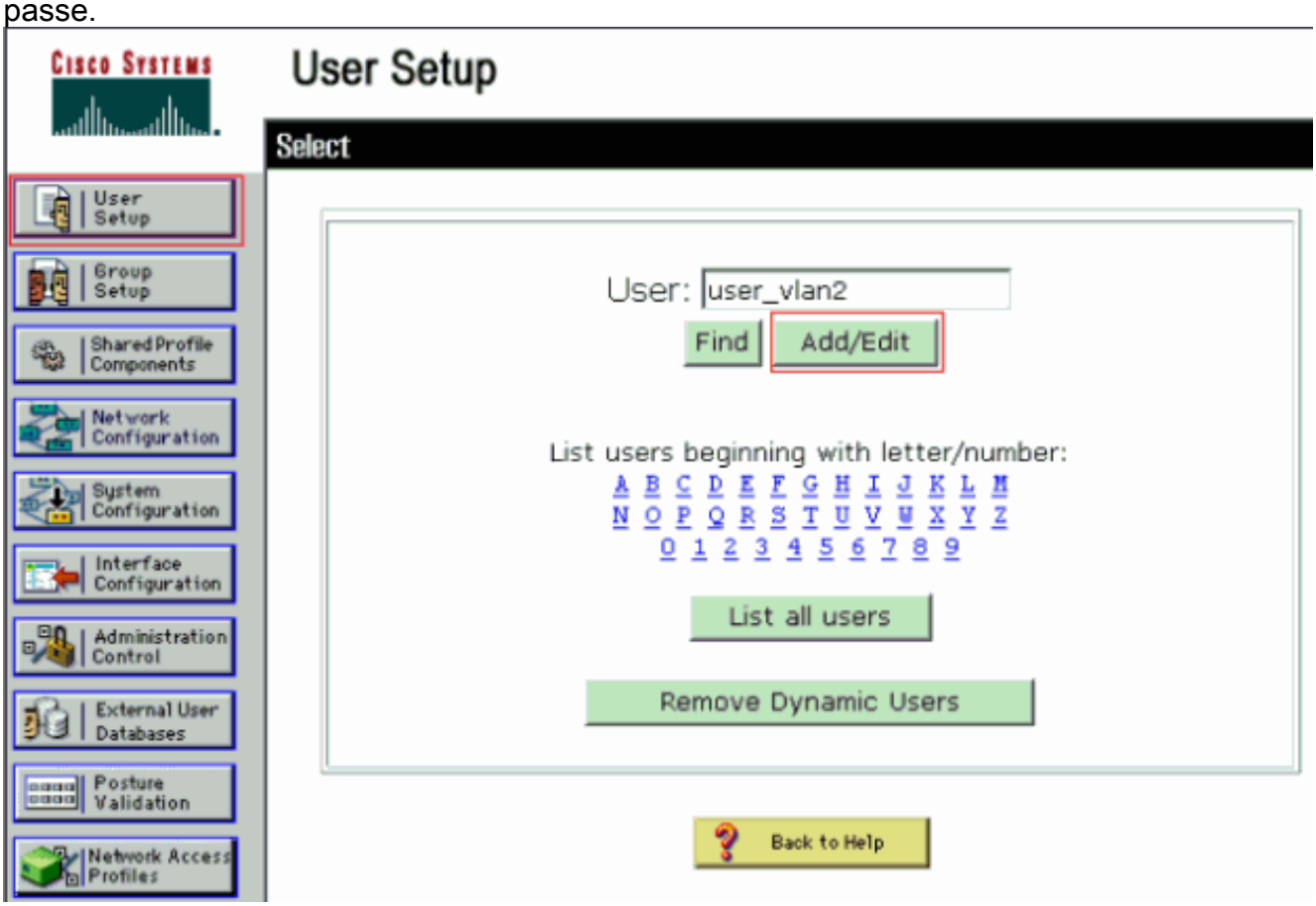


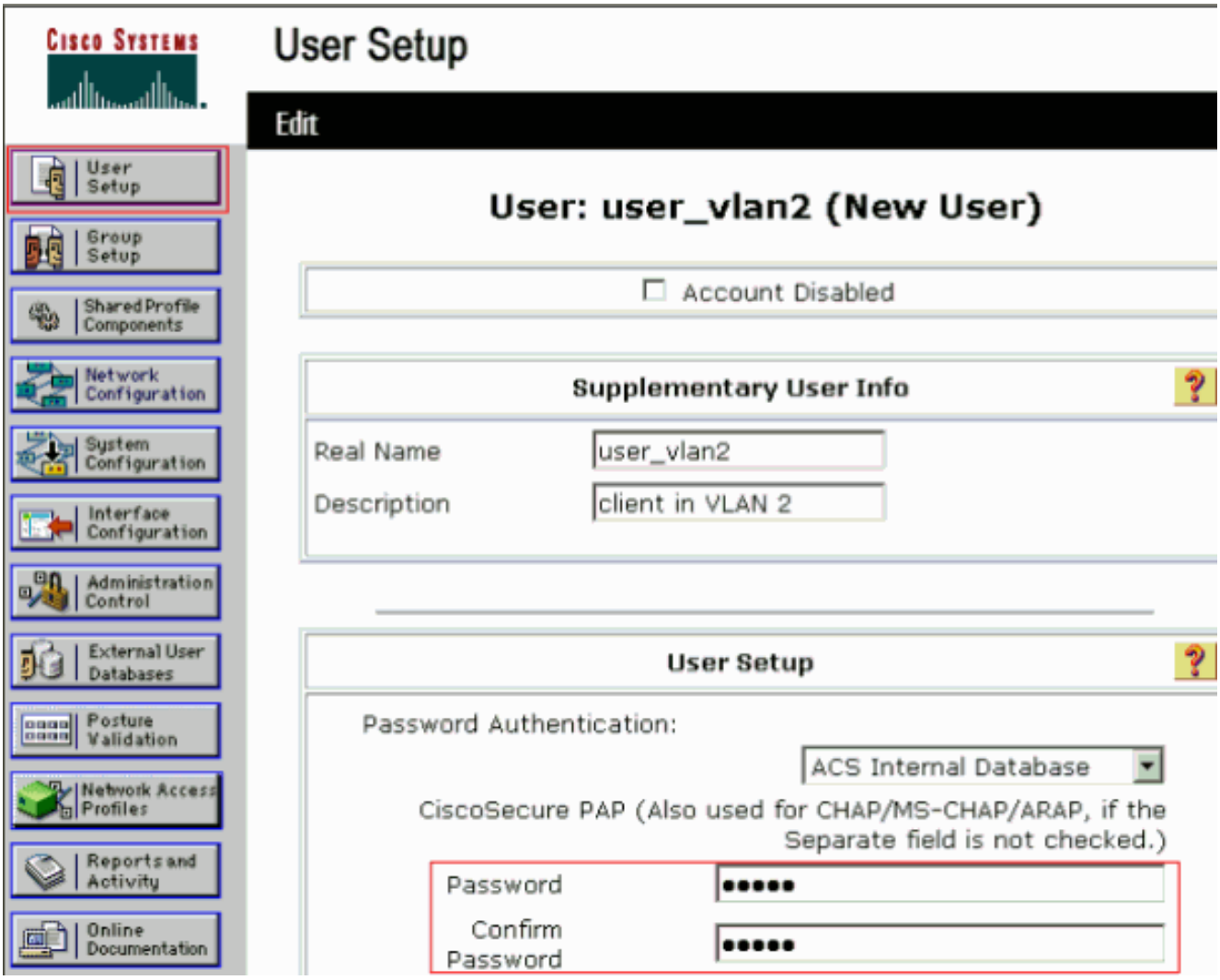
Complétez ces étapes afin de configurer le serveur RADIUS pour l'authentification, le VLAN et l'affectation d'adresses IP :

Deux noms d'utilisateur doivent être créés séparément pour les clients qui se connectent au VLAN 2 et pour le VLAN 3. Ici, un utilisateur **user_vlan2** pour les clients se connectant au VLAN 2 et un autre utilisateur **user_vlan3** pour les clients se connectant au VLAN 3 sont créés à cette fin.

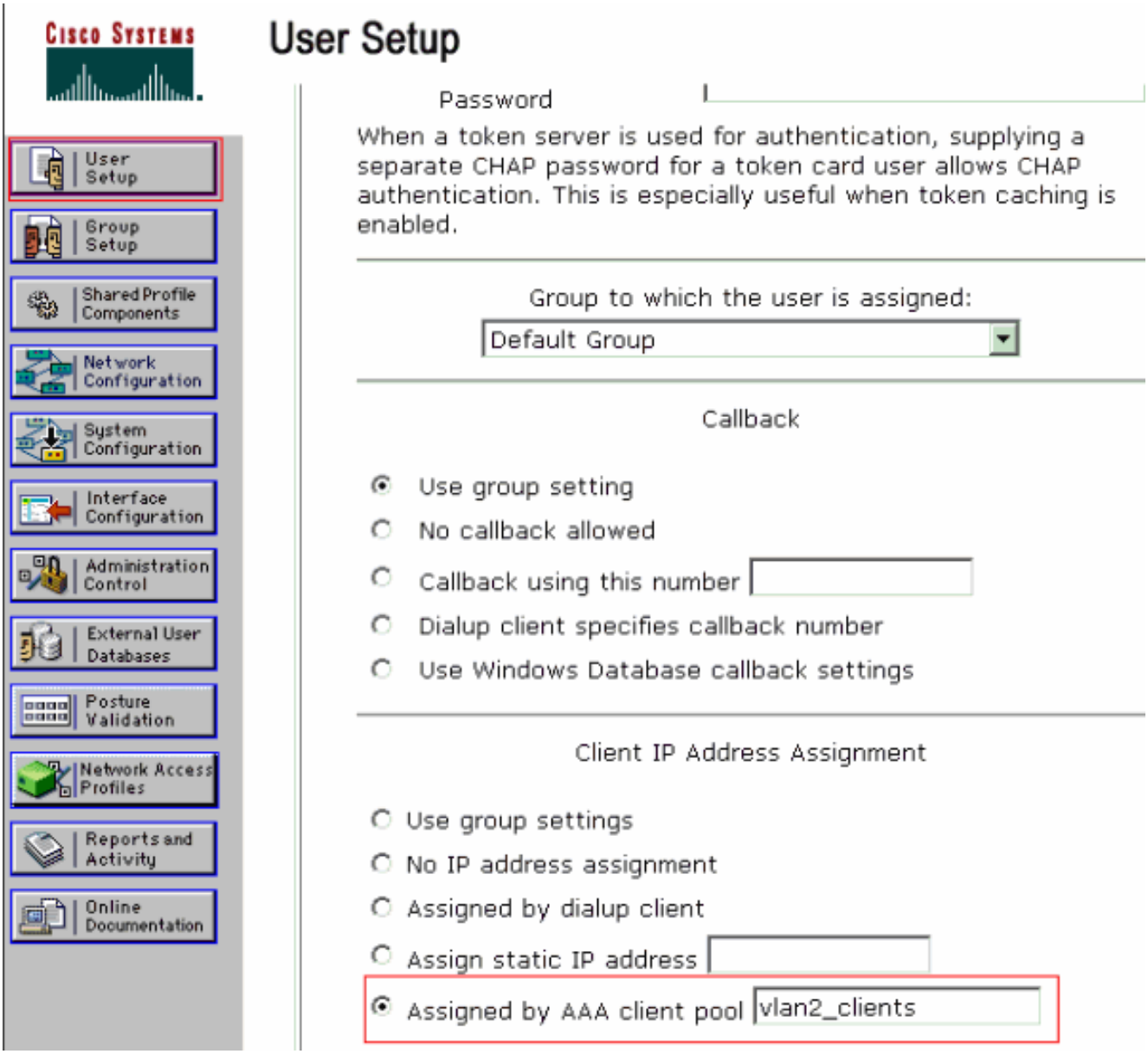
Remarque : ici, la configuration utilisateur est affichée pour les clients qui se connectent uniquement au VLAN 2. Pour les utilisateurs qui se connectent au VLAN 3, procédez de la même manière.

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



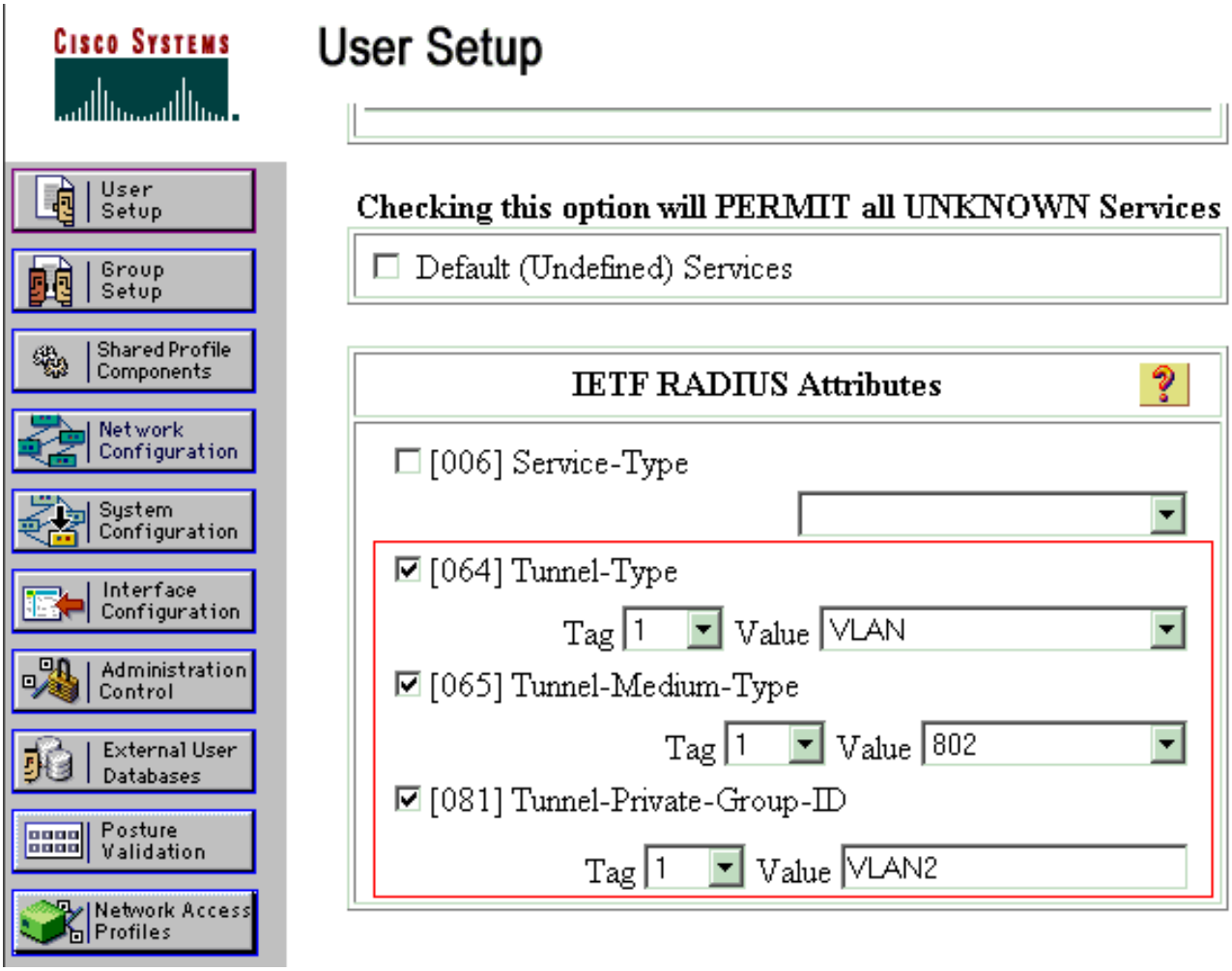


2. Définissez l'affectation d'adresse IP du client comme **Attribué par le pool de clients AAA**. Entrez le nom du pool d'adresses IP configuré sur le commutateur pour les clients VLAN 2.



Remarque : sélectionnez cette option et tapez le nom du pool d'adresses IP du client AAA dans la zone, uniquement si l'adresse IP de cet utilisateur doit être attribuée par un pool d'adresses IP configuré sur le client AAA.

3. Définissez les attributs 64 et 65 de l'IETF (Internet Engineering Task Force).Assurez-vous que les balises des valeurs sont définies sur 1, comme le montre cet exemple. Catalyst ignore toute balise autre que 1. Pour affecter un utilisateur à un VLAN spécifique, vous devez également définir l'attribut 81 avec un *nom* VLAN qui correspond.**Remarque :** Le *nom* du VLAN doit être exactement identique à celui configuré dans le commutateur.**Remarque :** l'affectation VLAN basée sur le *numéro* VLAN n'est pas prise en charge avec CatOS.

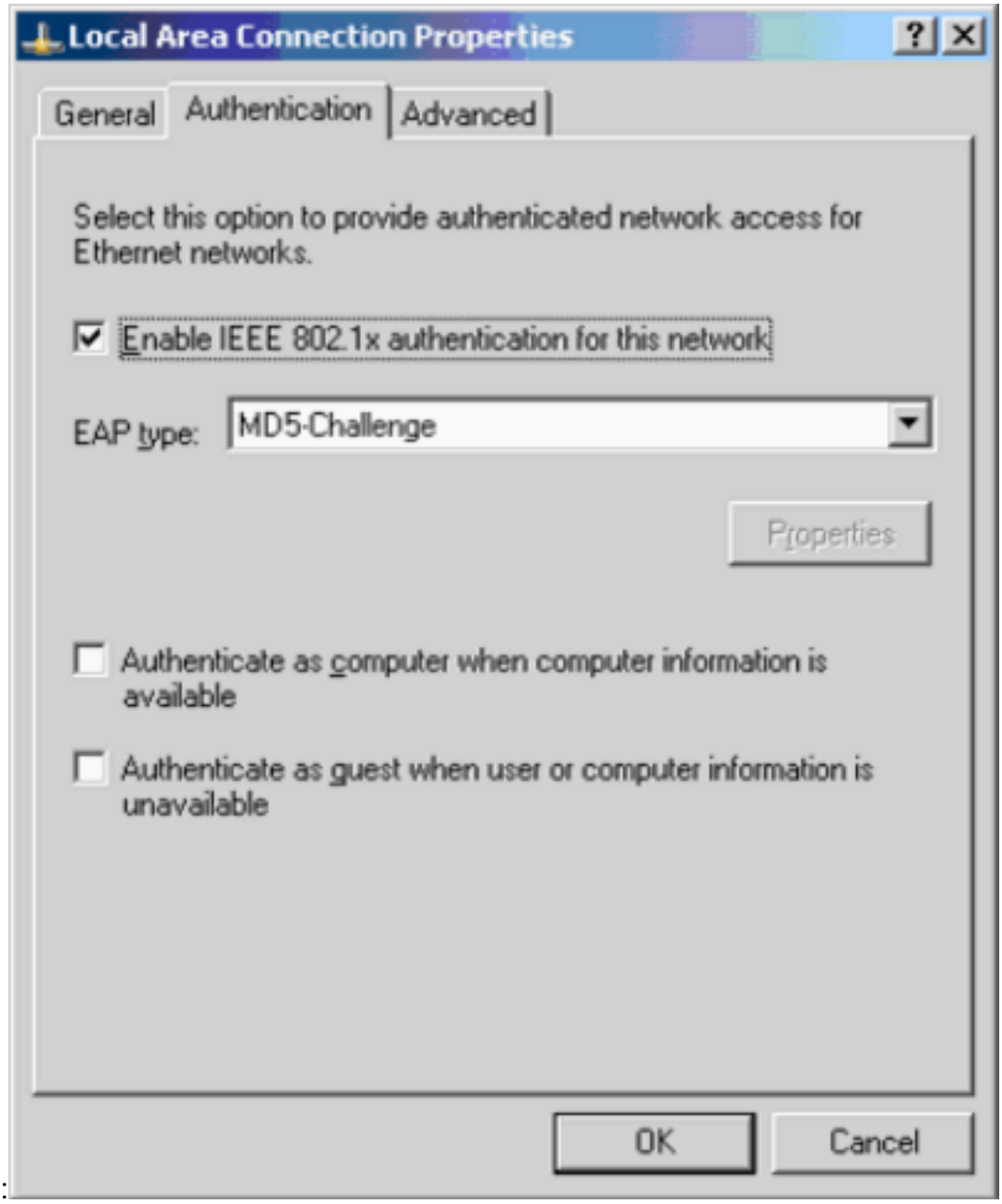


Reportez-vous à RFC 2868: Attributs RADIUS pour la prise en charge du protocole de tunnel pour plus d'informations sur ces attributs IETF.**Remarque :** dans la configuration initiale du serveur ACS, les attributs RADIUS IETF peuvent ne pas s'afficher dans le **programme d'installation de l'utilisateur**. Choisissez **Interface configuration > RADIUS (IETF)** afin d'activer les attributs IETF dans l'écran de configuration utilisateur. Ensuite, vérifiez les attributs **64**, **65** et **81** dans les colonnes Utilisateur et Groupe.

Configurer les clients PC pour utiliser l'authentification 802.1x

Cet exemple est spécifique au client EAP (Extensible Authentication Protocol) sur LAN de Microsoft Windows XP (EAPOL). Procédez comme suit :

1. Choisissez **Démarrer > Panneau de configuration > Connexions réseau**, puis cliquez avec le bouton droit sur votre **Connexion au réseau local** et choisissez **Propriétés**.
2. Cochez **l'icône Afficher dans la zone de notification lorsque vous êtes connecté** sous l'onglet Général.
3. Sous l'onglet Authentification, cochez la case **Activer l'authentification IEEE 802.1x pour ce réseau**.
4. Définissez le type EAP sur **MD5-Challenge**, comme le montre cet exemple

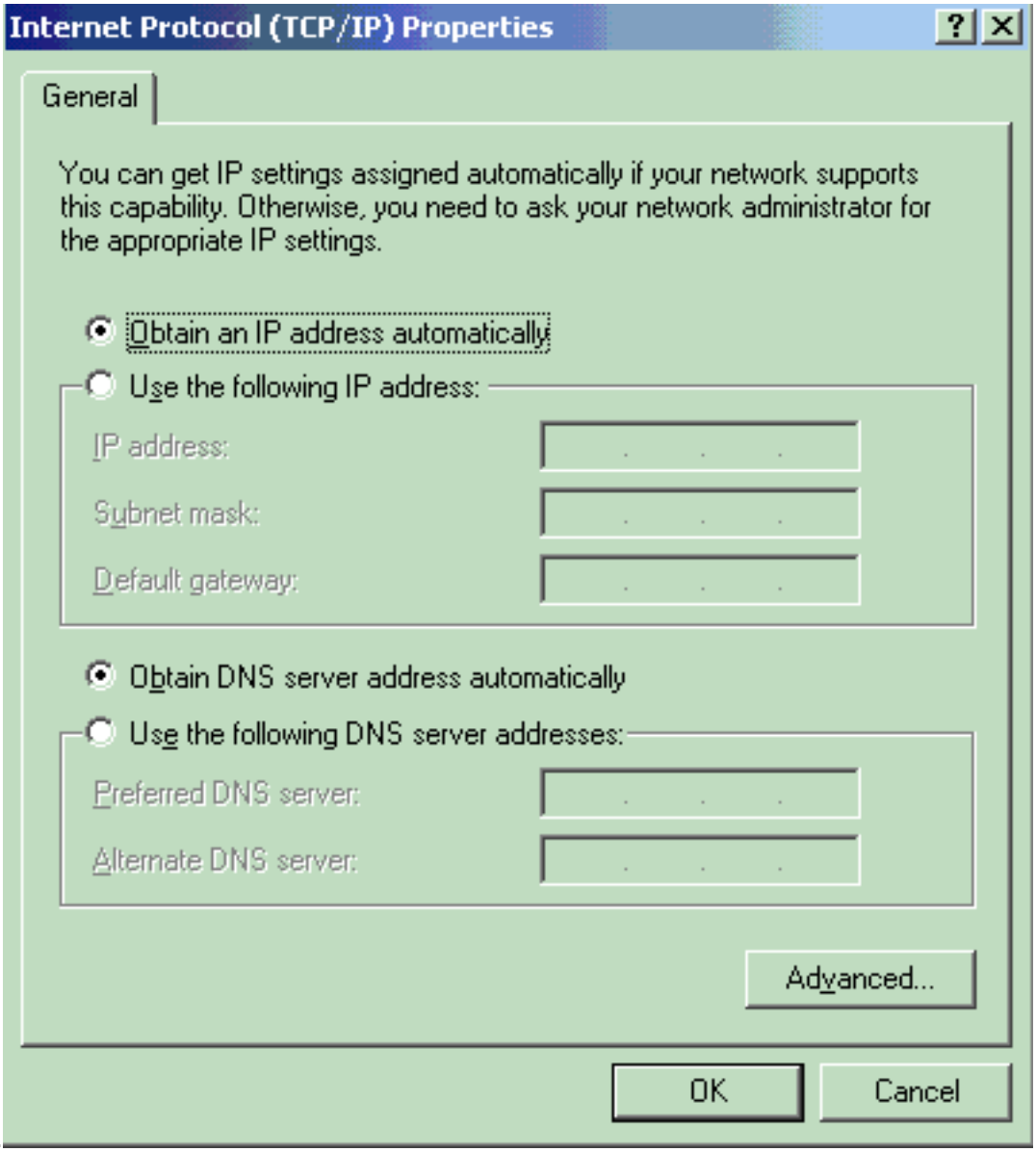


:

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

1. Choisissez **Démarrer > Panneau de configuration > Connexions réseau**, puis cliquez avec le bouton droit sur votre **Connexion au réseau local** et choisissez **Propriétés**.
2. Sous l'onglet General, cliquez sur **Internet Protocol (TCP/IP)**, puis sur **Properties**.
3. Choisissez **Obtain an IP address**

automatically.



Vérification

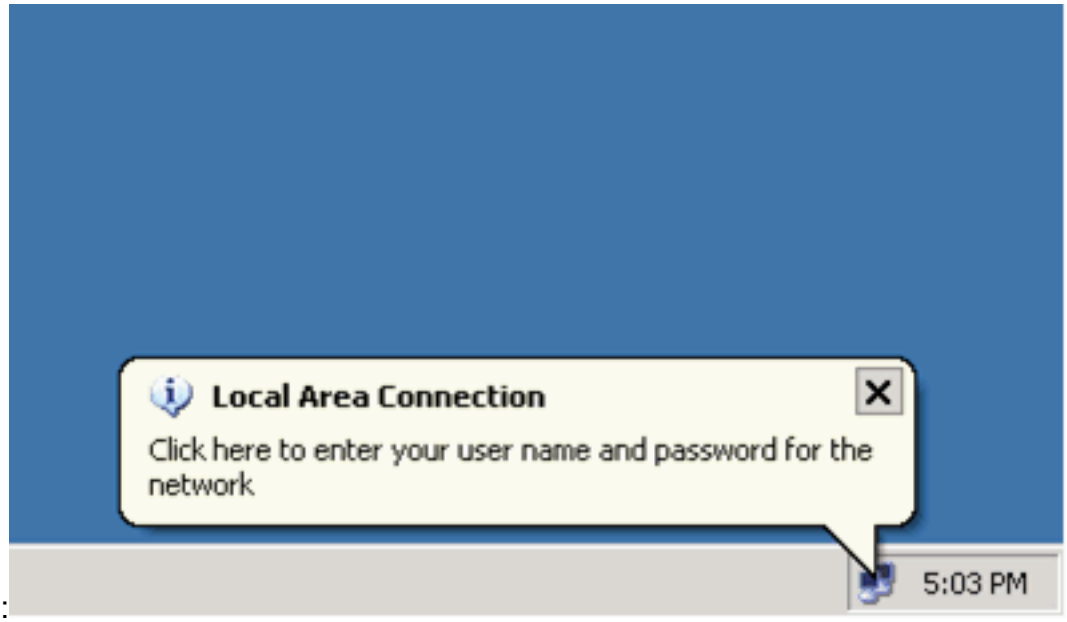
Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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

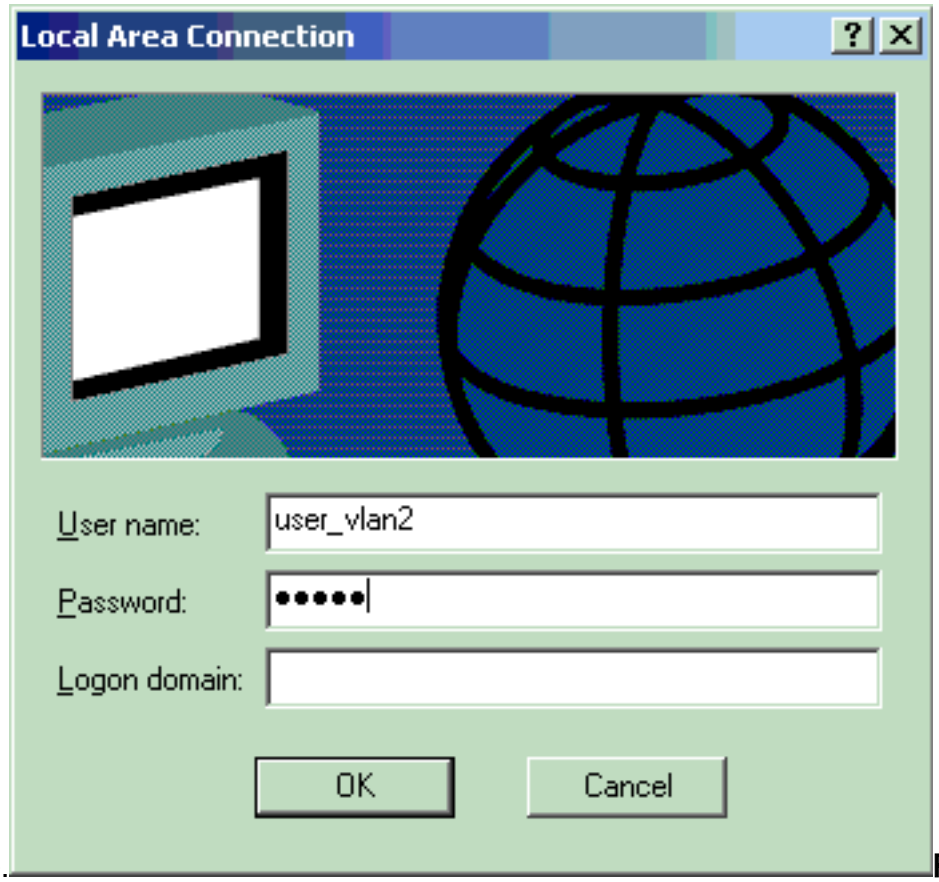
Si vous avez correctement terminé la configuration, les clients PC affichent une invite contextuelle pour saisir un nom d'utilisateur et un mot de passe.

1. Cliquez sur l'invite, que cet exemple montre

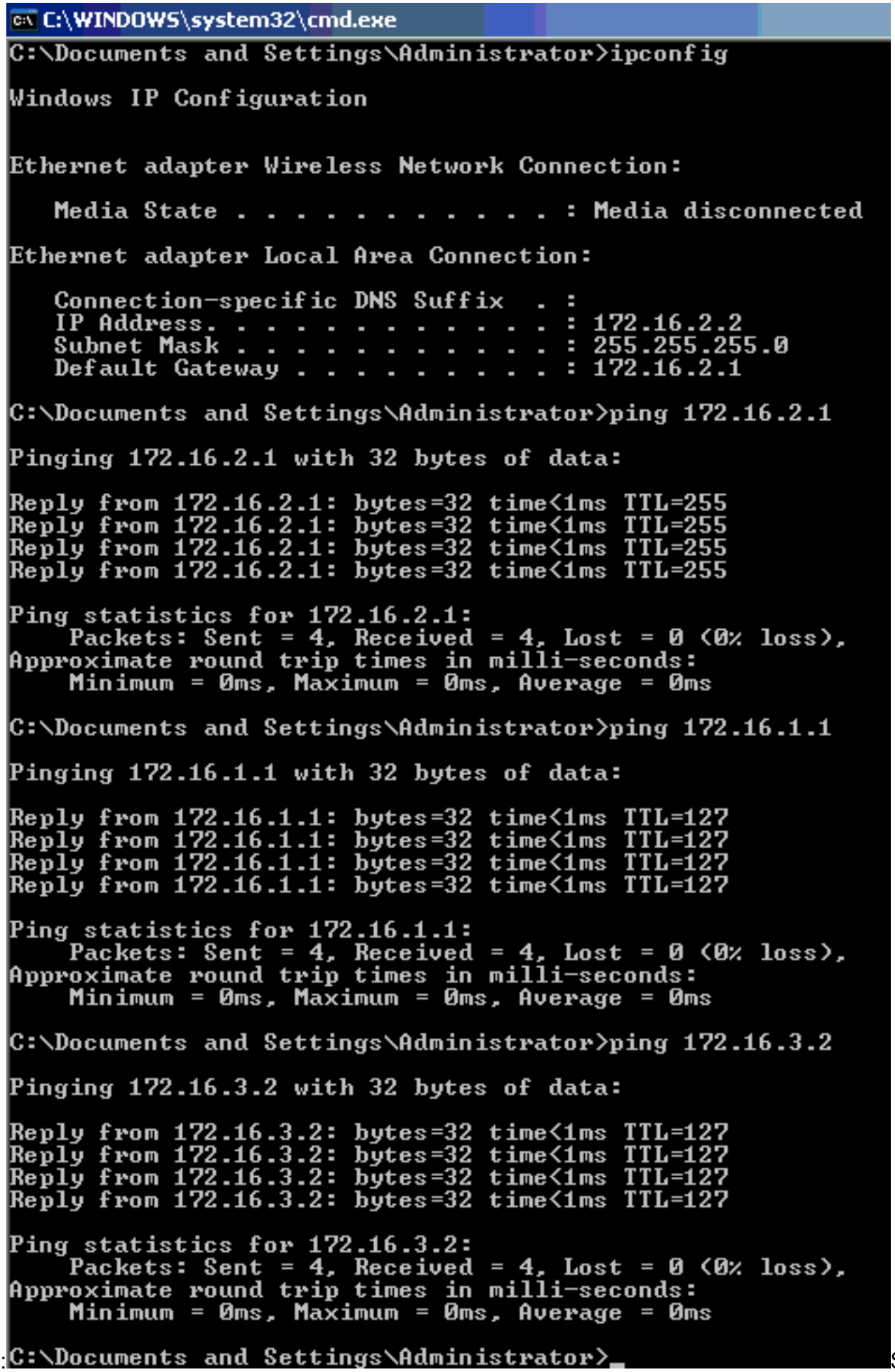


: Une fenêtre de saisie de nom d'utilisateur et de mot de passe s'affiche.

2. Saisissez le nom d'utilisateur et mot de passe. **Remarque :** Dans PC 1 et 2, saisissez les informations d'identification de l'utilisateur VLAN 2. Dans PC 3 et PC 4, saisissez les informations d'identification de l'utilisateur VLAN 3.

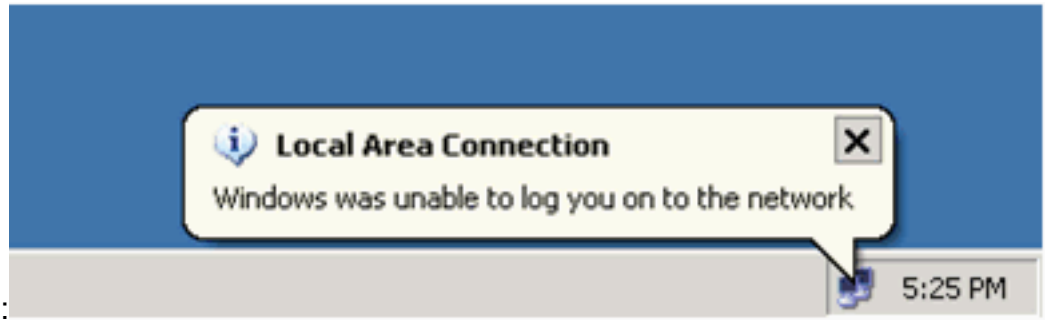


3. Si aucun message d'erreur n'apparaît, vérifiez la connectivité avec les méthodes habituelles, telles que l'accès aux ressources réseau et la commande **ping**. Ceci est une sortie du PC 1, qui montre une **requête ping** réussie vers PC 4



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

:



Catalyst 6500

Si le mot de passe et le nom d'utilisateur semblent corrects, vérifiez l'état du port 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 du VLAN après une 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 à partir du module de routage (MSFC) après une 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
```

Dépannage

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
- Guide de déploiement Catalyst Switching et ACS
- RFC 2868 : Attributs RADIUS pour la prise en charge du protocole de tunnel
- Configuration de l'authentification 802.1x
- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems