# Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant Cisco IOS

## Contenu



# Introduction

Ce document explique comment configurer IEEE 802.1x sur un Catalyst 6500/6000 qui s'exécute en mode natif (une seule image du logiciel Cisco IOS® pour Supervisor Engine et 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 Cisco IOS Version 12.2(18)SXF sur Supervisor Engine**Remarque :** Vous avez besoin du logiciel Cisco IOS Version 12.1(13)E ou ultérieure pour prendre en charge l'authentification basée sur les ports 802.1x.
- 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 mettre à disposition 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 EAPOL (Extensible Authentication Protocol over LAN) via le port auquel le périphérique est connecté. Une fois l'authentification réussie, le trafic normal peut passer par le port.

**Remarque :** si le commutateur reçoit des paquets EAPOL du port qui n'est pas configuré pour l'authentification 802.1x ou si le commutateur ne prend pas en charge l'authentification 802.1x, les paquets EAPOL sont abandonnés et ne sont transférés à aucun périphérique en amont.

## Configuration

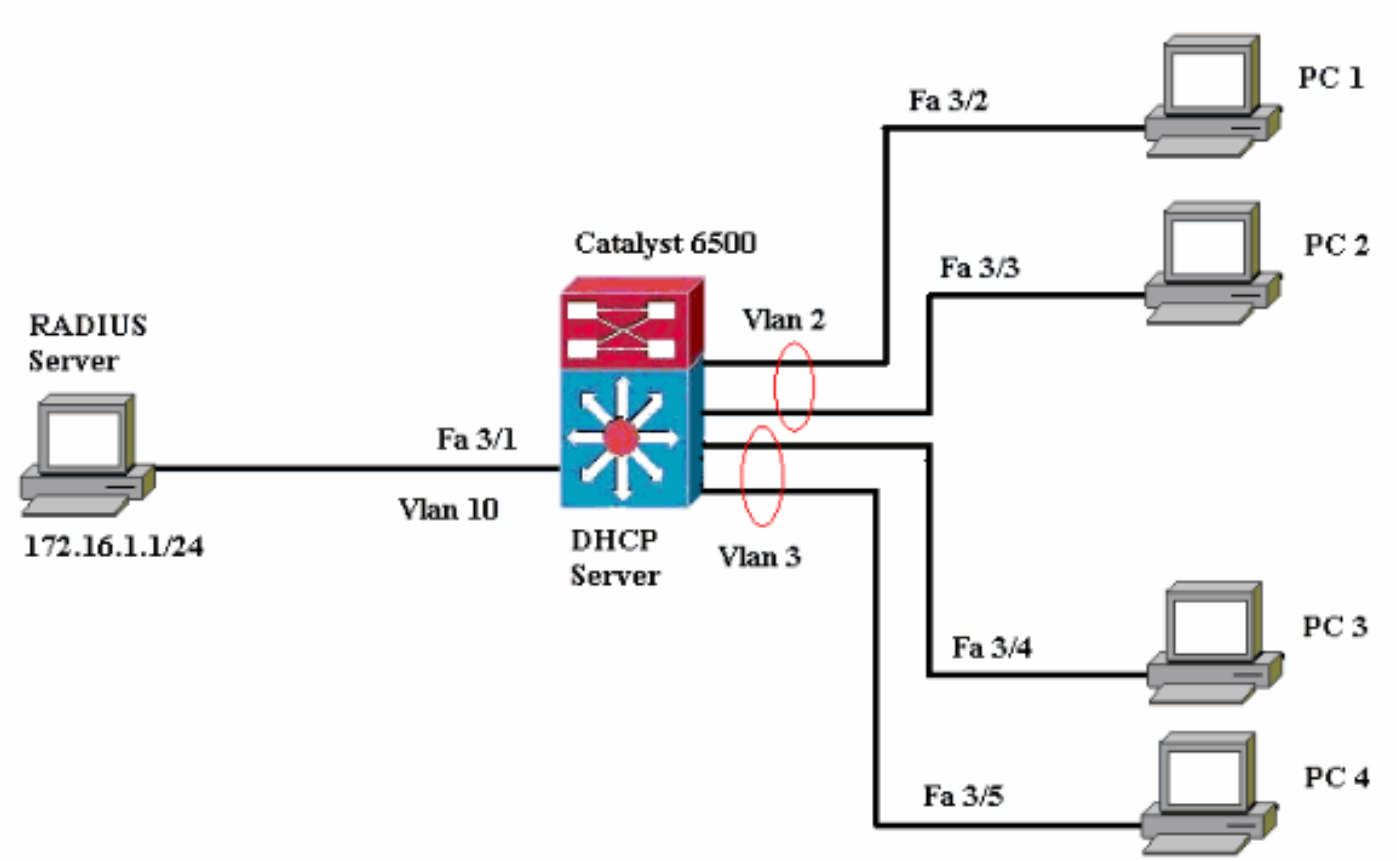
Dans cette section, vous trouverez les informations nécessaires à la configuration de la fonctionnalité 802.1x décrite dans ce document.

Cette configuration requiert les étapes suivantes :

- Configurez le commutateur Catalyst pour l'authentification 802.1x.
- Configurez le serveur RADIUS.
- Configurez 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. Il demande des informations d'identité au client, vérifie ces informations avec le serveur RADIUS et relaie 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 requêtes 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 celles du 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.

## Configuration du commutateur Catalyst pour l'authentification 802.1x

Cet exemple de configuration de commutateur inclut :

- Comment activer l'authentification 802.1x sur les ports FastEthernet.
- Comment connecter un serveur RADIUS au VLAN 10 derrière le port FastEthernet 3/1.
- Configuration d'un 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.

Référez-vous aux directives et restrictions d'authentification basée sur les ports 802.1x pour les directives sur la configuration de l'authentification 802.1x.

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

**Catalyst 6500**

```
Router#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#hostname Cat6K
!--- Sets the hostname for the switch.
Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER
!--- This is a dedicated VLAN for the RADIUS server.
Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut
!--- Assigns the port connected to the RADIUS server to
VLAN 10. !--- Note:- All the active access ports are in
VLAN 1 by default.

Cat6K(config-if)#exit
Cat6K(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat6K(config)#interface
range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut
!--- Enables 802.1x on all the FastEthernet interfaces.
Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model
!--- Enables AAA. Cat6K(config)#aaa authentication dot1x
default group radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat6K(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat6K(config)#radius-server host
172.16.1.1
!--- Sets the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco
!--- The key must match the key used on the RADIUS
server. Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
```

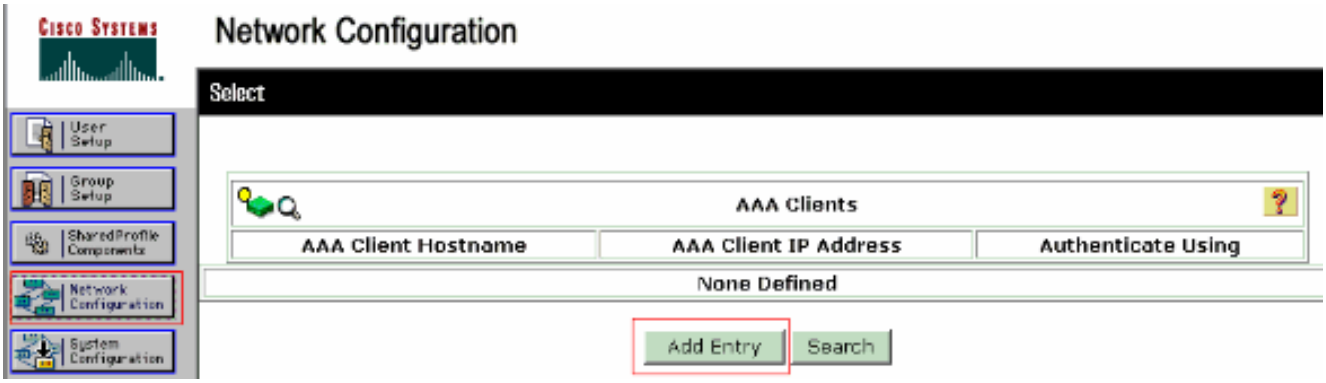
```
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients in VLAN 3.
Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.2.1
!--- This pool assigns ip address for clients in VLAN 2.
Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1
!--- This pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------
-----------------------
1    default                           active    Fa3/2,
Fa3/3, Fa3/4, Fa3/5
                                                 Fa3/6,
Fa3/7, Fa3/8, Fa3/9
                                                 Fa3/10,
Fa3/11, Fa3/12, Fa3/13
                                                 Fa3/14,
Fa3/15, Fa3/16, Fa3/17
                                                 Fa3/18,
Fa3/19, Fa3/20, Fa3/21
                                                 Fa3/22,
Fa3/23, Fa3/24, Fa3/25
                                                 Fa3/26,
Fa3/27, Fa3/28, Fa3/29
                                                 Fa3/30,
Fa3/31, Fa3/32, Fa3/33
                                                 Fa3/34,
Fa3/35, Fa3/36, Fa3/37
                                                 Fa3/38,
Fa3/39, Fa3/40, Fa3/41
                                                 Fa3/42,
Fa3/43, Fa3/44, Fa3/45
                                                 Fa3/46,
Fa3/47, Fa3/48
2    VLAN2                             active
3    VLAN3                             active
10   RADIUS_SERVER                     active    Fa3/1
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

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

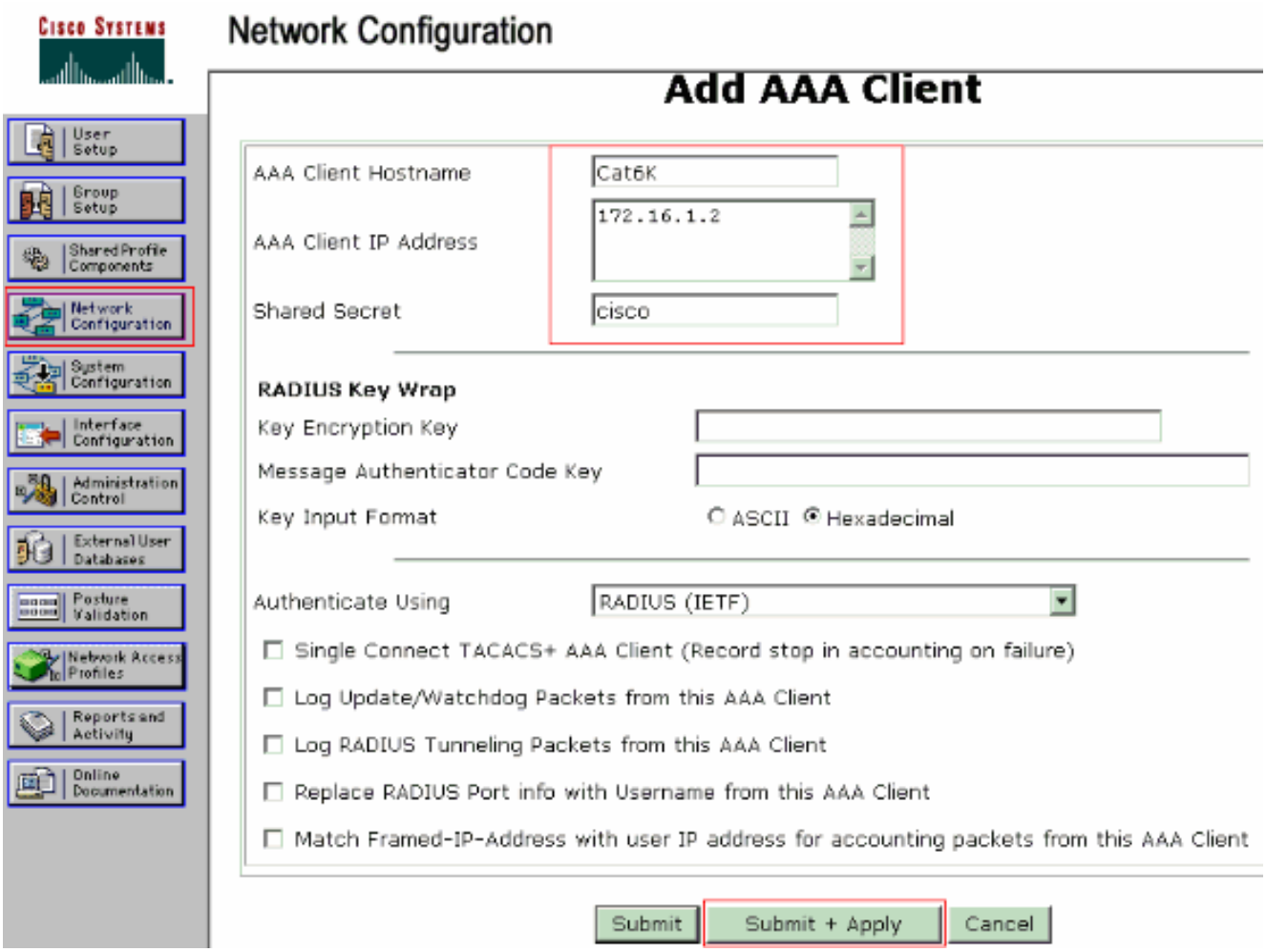
## Configurer le serveur RADIUS

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. Cliquez sur **Configuration réseau** dans la fenêtre d'administration ACS afin de configurer un client AAA.
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 du commutateur (**172.16.1.2**).Shared Secret = clé RADIUS configurée 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 :

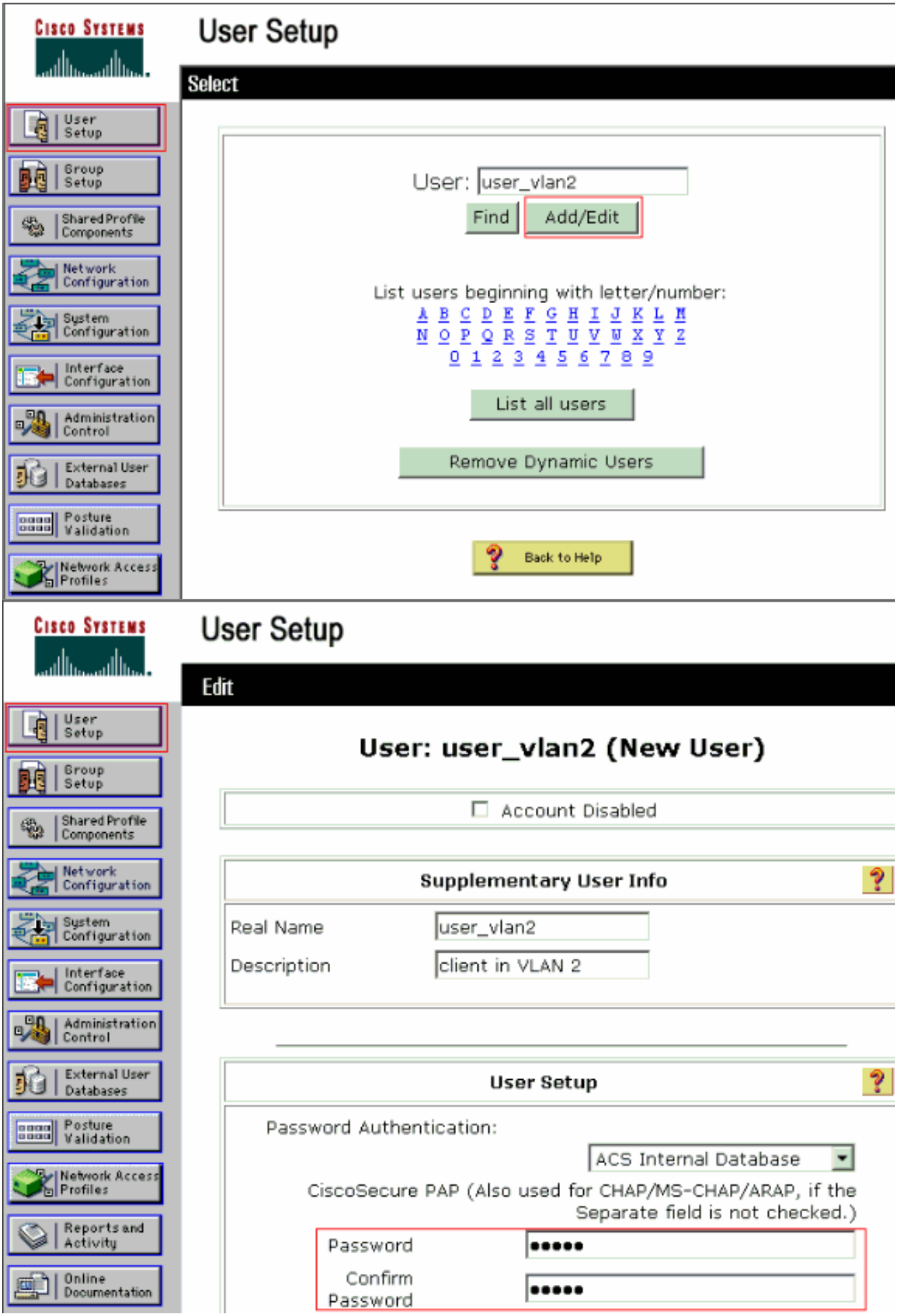



Complétez ces étapes afin de configurer le serveur RADIUS pour l'authentification, le VLAN et l'affectation d'adresses IP.

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 qui se connectent au VLAN 2 et un autre utilisateur **user_vlan3** pour les clients qui se connectent au VLAN 3 sont créés à cette fin.

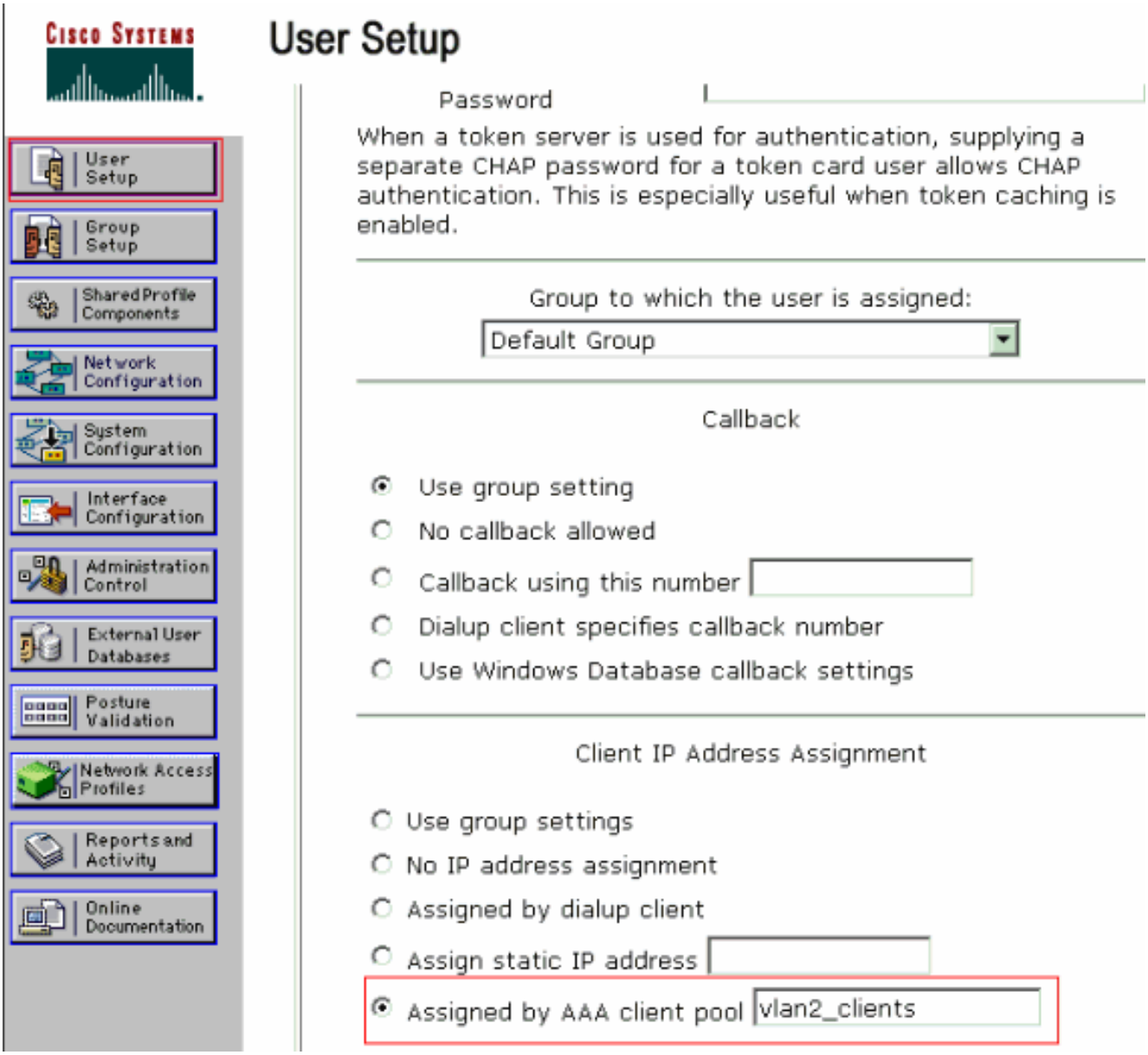
**Remarque :** ici, la configuration utilisateur est affichée pour les clients qui se connectent au VLAN 2 uniquement. Pour les utilisateurs qui se connectent au VLAN 3, suivez la même procédure.

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



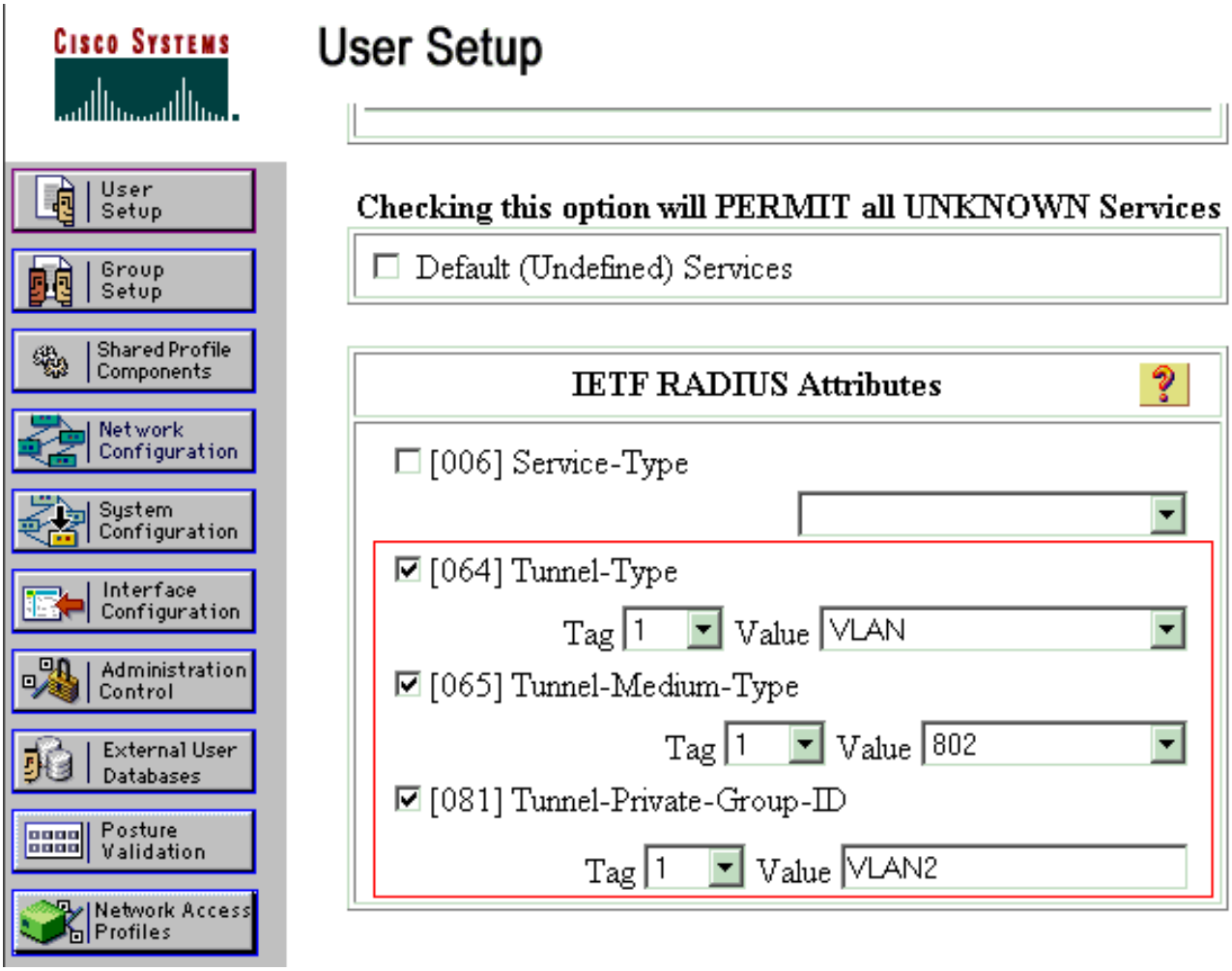

2. Définissez l'affectation d'adresse IP du client comme **Attribué par le pool de clients AAA**. Entrez le nom du pool d'adresses IP configuré sur le commutateur pour les clients VLAN

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* de VLAN ou un *numéro* de VLAN qui correspond.**Remarque :** Si vous utilisez le *nom* VLAN, il doit être exactement identique à celui configuré dans le commutateur.




**Remarque :** Pour plus d'informations sur ces attributs IETF, reportez-vous à la RFC 2868 : Attributs RADIUS pour la prise en charge du protocole de tunnel.**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**. Afin d'activer les attributs IETF dans les écrans de configuration utilisateur, choisissez **Interface configuration > RADIUS (IETF)**. Ensuite, vérifiez les attributs **64**, **65** et **81** dans les colonnes Utilisateur et Groupe.**Remarque :** Si vous ne définissez pas l'attribut IETF **81** et que le port est un port de commutateur en mode d'accès, le client a une affectation au VLAN d'accès du port. Si vous avez défini l'attribut **81** pour l'affectation de VLAN dynamique et que le port est un port de commutateur en mode d'accès, vous devez émettre la commande **aaa Authorization network default group radius** sur le commutateur. Cette commande attribue le port au VLAN fourni par le serveur RADIUS. Sinon, 802.1x déplace le port à l'état AUTORISÉ après authentification de l'utilisateur ; mais le port se trouve toujours dans le VLAN par défaut du port et la connectivité peut échouer. Si vous avez défini l'attribut **81**, mais que vous avez configuré le port en tant que port routé, un refus d'accès se produit. Ce message d'erreur s'affiche :

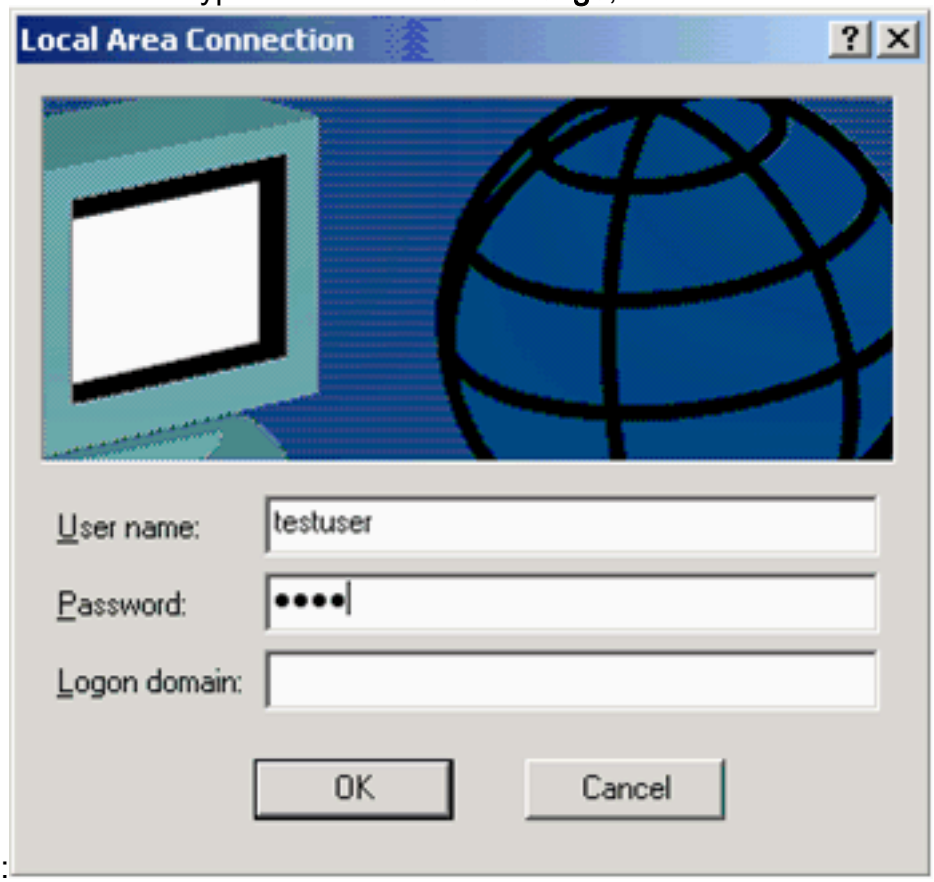
```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

## 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) :

1. Choisissez **Démarrer > Panneau de configuration > Connexions réseau**, puis cliquez avec le

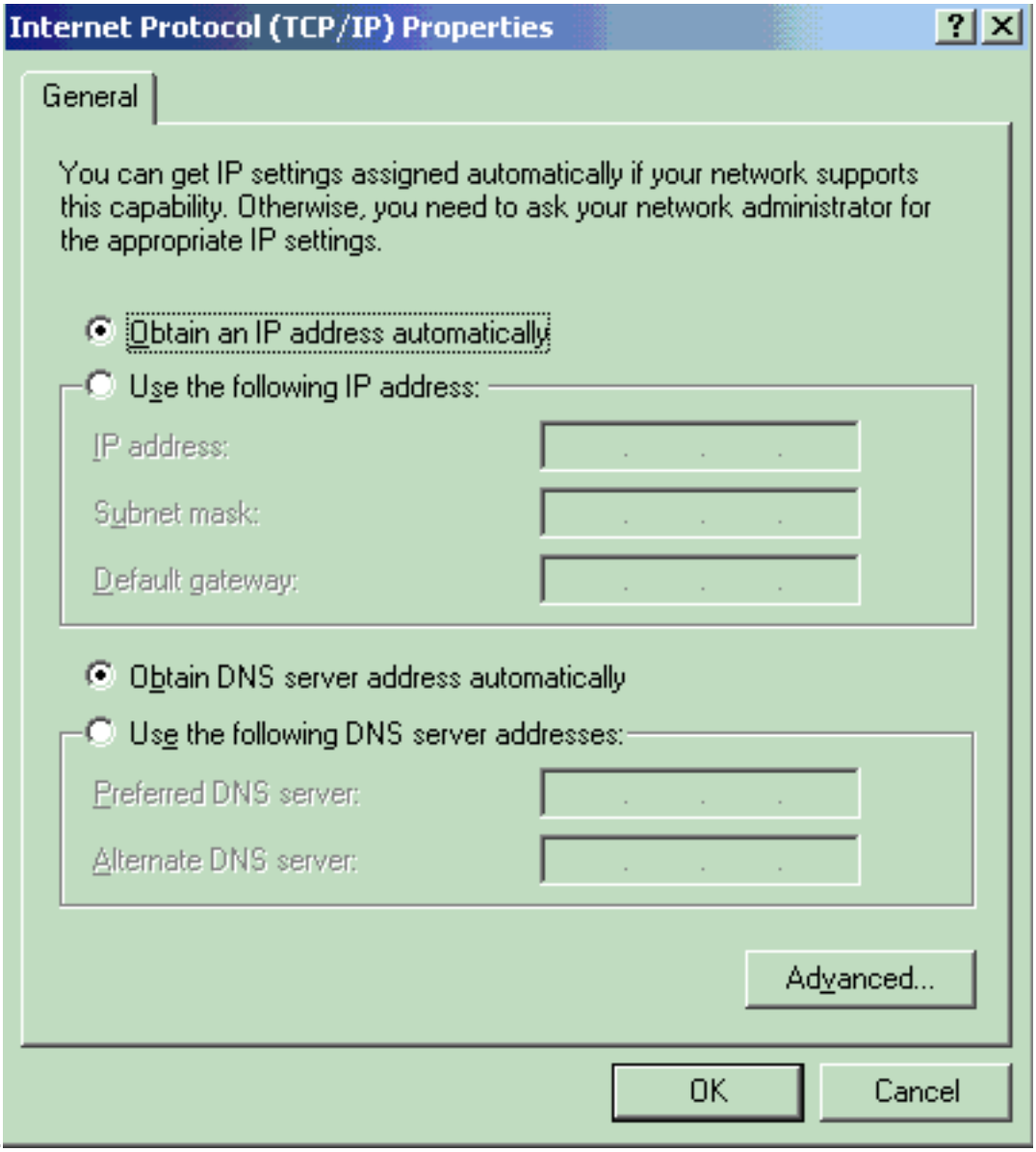
bouton droit sur votre **Connexion au réseau local** et choisissez **Propriétés**.
2. Cochez **l'icône Afficher dans la zone de notification lorsque vous êtes connecté** sous l'onglet Général.
3. Sous l'onglet Authentification, cochez la case **Activer l'authentification IEEE 802.1x pour ce réseau**.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




:

Exécutez ces étapes pour configurer les clients afin qu'ils obtiennent l'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**

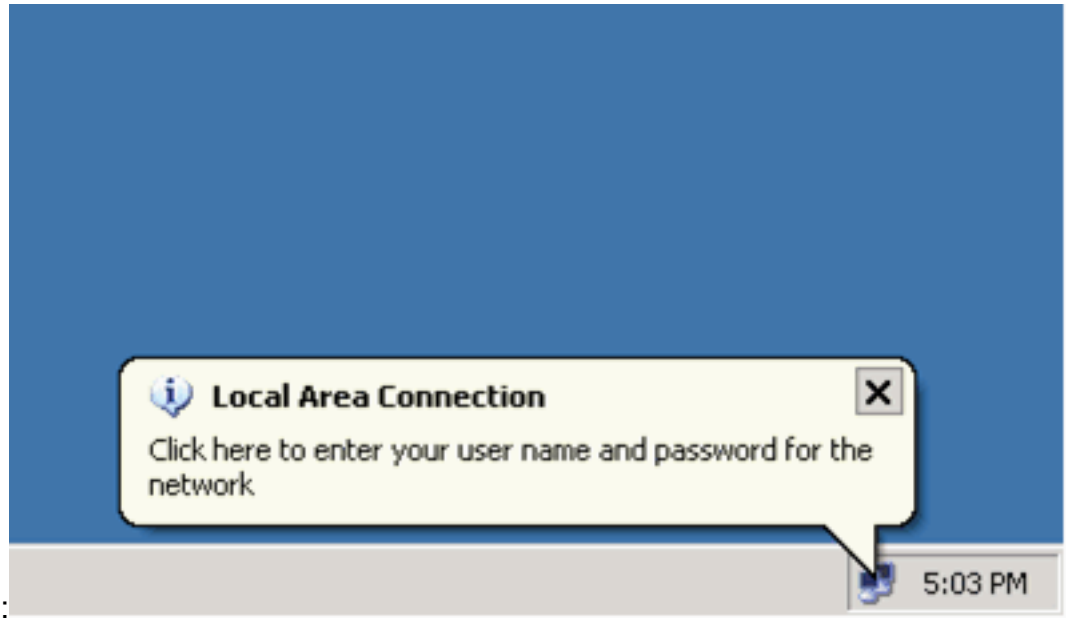
automatically. 


# Vérification

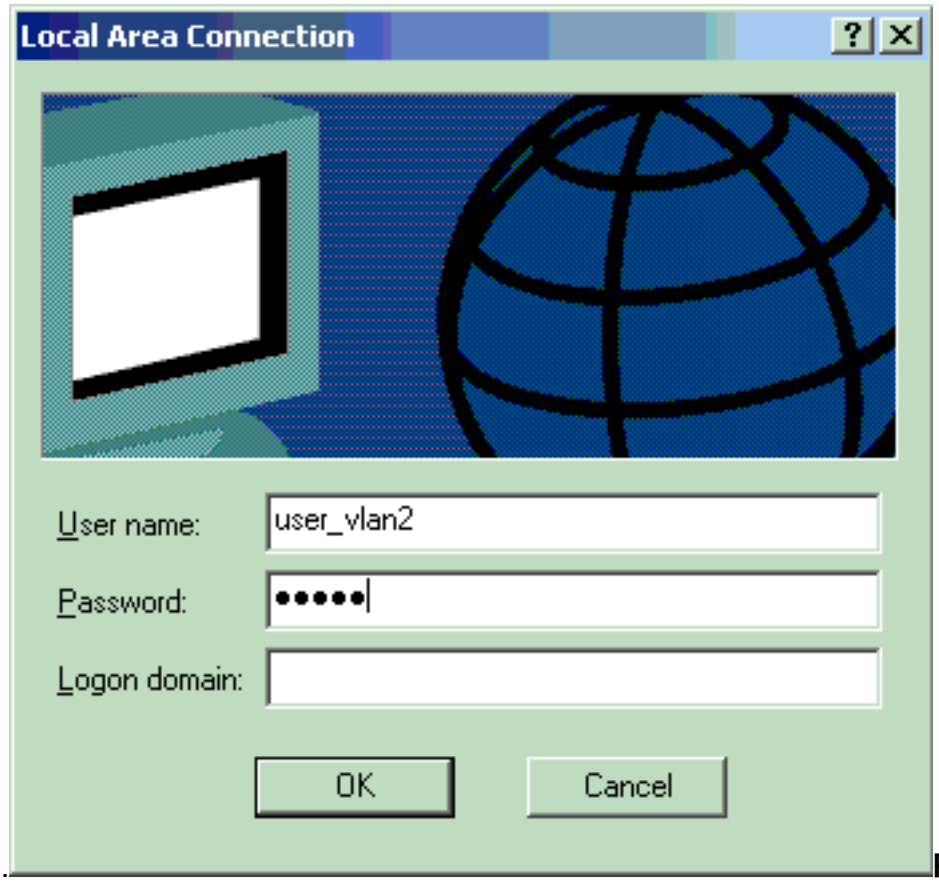
## Clients PC

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.

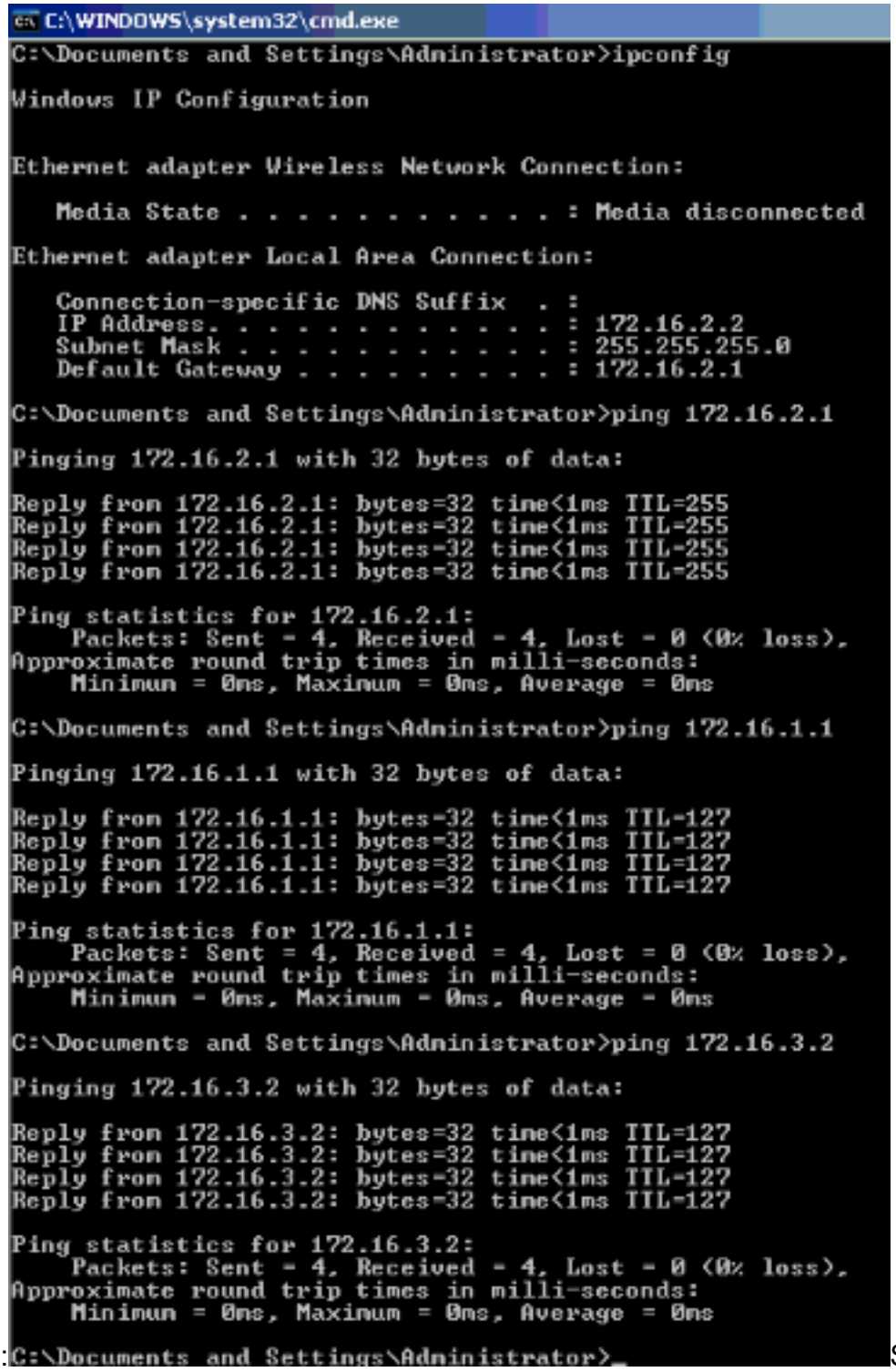
1. Cliquez sur l'invite, que cet exemple montre



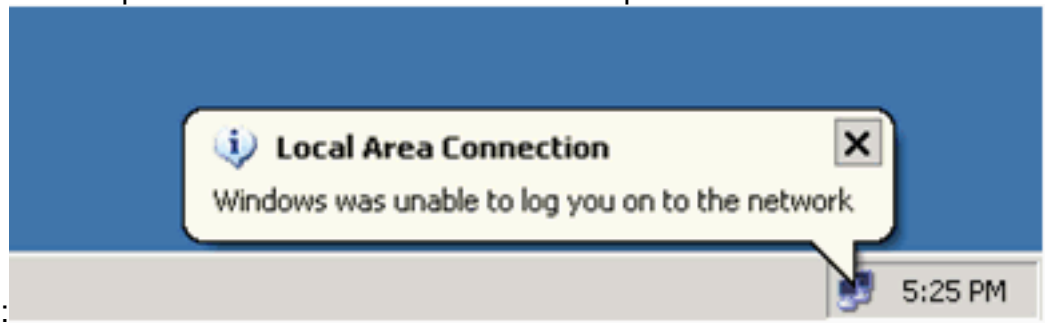
: Une fenêtre de saisie de nom d'utilisateur et de mot de passe s'affiche.

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

**Remarque :** Dans PC 1 et 2, saisissez les informations d'identification de l'utilisateur VLAN 2 et 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**. Cette sortie provient de PC 1 et 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#show dot1x

Sysauthcontrol                  = Enabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both


Cat6K#show dot1x interface fastEthernet 3/2
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/4
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Enabled
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds

Cat6K#show dot1x interface fastEthernet 3/1
Default Dot1x Configuration Exists for this interface FastEthernet3/1
AuthSM State      = FORCE AUTHORIZED
BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
MultiHosts        = Disabled
PortControl       = Force Authorized
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
```

Vérifiez l’état du VLAN après une authentification réussie.

```
Cat6K#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa3/6, Fa3/7, Fa3/8, Fa3/9,
                                                Fa3/10, Fa3/11, Fa3/12, Fa3/13,
                                                Fa3/14, Fa3/15, Fa3/16, Fa3/17,
                                                Fa3/18, Fa3/19, Fa3/20, Fa3/21,
                                                Fa3/22, Fa3/23, Fa3/24, Fa3/25,
```

```
                                                  Fa3/26, Fa3/27, Fa3/28, Fa3/29,
                                                  Fa3/30, Fa3/31, Fa3/32, Fa3/33,
                                                  Fa3/34, Fa3/35, Fa3/36, Fa3/37,
                                                  Fa3/38, Fa3/39, Fa3/40, Fa3/41,
                                                  Fa3/42, Fa3/43, Fa3/44, Fa3/45,
                                                  Fa3/46, Fa3/47, Fa3/48
2    VLAN2                          active    Fa3/2, Fa3/3
3    VLAN3                          active    Fa3/4, Fa3/5
10   RADIUS_SERVER                  active    Fa3/1
1002 fddi-default                   act/unsup
1003 token-ring-default             act/unsup
1004 fddinet-default                act/unsup
1005 trnet-default                  act/unsup
!--- Output suppressed.
```

2. Vérifiez l'état de liaison DHCP à partir de l' après l'authentification réussie.

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.2.2       0100.1636.3333.9c       Mar 04 2007 06:35 AM    Automatic
172.16.2.3       0100.166F.3CA3.42       Mar 04 2007 06:43 AM    Automatic
172.16.3.2       0100.145e.945f.99       Mar 04 2007 06:50 AM    Automatic
172.16.3.3       0100.1185.8D9A.F9       Mar 04 2007 06:57 AM    Automatic
```

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** .

# Dépannage

Collectez le résultat de ces commandes **debug** afin de dépanner :

**Remarque :** Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug dot1x events** - Active le débogage des instructions d'impression gardées par l'indicateur dot1x events.

```
Cat6K#debug dot1x events
Dot1x events debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to
send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
   is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
    this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
   this id 13
```

```
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
   id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
Cat6K#
```

*!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0 00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/4**

```
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
```

- **debug radius** : affiche les informations associées à RADIUS.

```
Cat6K#debug radius
Radius protocol debugging is on
Cat6K#
```

*!--- Debug output for PC 1 connected to Fa3/2.* 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18 CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79 00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80 18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104 00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19

```
172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80
18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124
00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8
01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36:
Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18
11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# !--- Debug
output for PC 3 connected to Fa3/4. 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS:
Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius
packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11
172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute
61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58:
Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from
id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58:
Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login:
length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58:
RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request,
len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS:
Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33
010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58:
RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from
radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request,
len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS:
Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6
0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58:
Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004
00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-
login: length of eap packet = 4 Cat6K#
```

# Informations connexes

- Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant CatOS
- Directives pour le déploiement de Cisco Secure ACS pour serveurs Windows NT/2000 dans un environnement de commutateur Cisco Catalyst
- RFC 2868 : Attributs RADIUS pour la prise en charge du protocole de tunnel
- Configuration de l'authentification basée sur les ports IEEE 802.1X
- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems