Exemple de configuration de l'authentification sur plusieurs domaines IEEE 802.1x sur les commutateurs Cisco Catalyst de couche 3 à configuration fixe

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Produits connexes
Conventions
Informations générales
Configuration
Diagramme du réseau
Configurer le commutateur Catalyst pour l'authentification multidomaine 802.1x
Configurer le serveur RADIUS
Configurer les clients PC pour utiliser l'authentification 802.1x
Configurer les téléphones IP pour utiliser l'authentification 802.1x
Vérification
Clients PC
Téléphones IP
Commutateur de couche 3
Dépannage
Échec de l'authentification du téléphone IP
Informations connexes

Introduction

L'authentification multidomaine permet à un téléphone IP et à un PC de s'authentifier sur le même port de commutateur, tout en les plaçant sur les VLAN voix et données appropriés. Ce document explique comment configurer l'authentification multidomaine IEEE 802.1x (MDA) sur les commutateurs de configuration fixe de couche 3 Cisco Catalyst.

Conditions préalables

Conditions requises

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

- Fonctionnement de RADIUS
- Guide de déploiement Catalyst Switching et ACS
- Guide de l'utilisateur de Cisco Secure Access Control Server 4.1
- Présentation du téléphone IP Cisco Unified

Components Used

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

- Commutateur de la gamme Cisco Catalyst 3560 qui exécute le logiciel Cisco IOS® Version 12.2(37)SE1**Remarque : la** prise en charge de l'authentification multidomaine est disponible uniquement à partir du logiciel Cisco IOS Version 12.2(35)SE et ultérieure.
- 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.
- Téléphone IP Cisco Unified 7970G avec microprogramme SCCP version 8.2(1)
- Téléphone IP Cisco Unified 7961G avec microprogramme SCCP version 8.2(2)
- Media Covergence Server (MCS) avec Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2

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.

Produits connexes

Cette configuration peut également être utilisée avec ce qui suit :

- Commutateur de la gamme Cisco Catalyst 3560-E
- Commutateur de la gamme Cisco Catalyst 3750
- Commutateur de la gamme Cisco Catalyst 3750-E

Remarque : Le commutateur de la gamme Cisco Catalyst 3550 ne prend pas en charge l'authentification multidomaine 802.1x.

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.

802.1x comprend trois composants principaux. Chacun est appelé PAE (Port Access Entity).

- Supplicant : périphérique client qui demande l'accès au réseau, par exemple, les téléphones IP et les ordinateurs connectés
- Authentificateur : périphérique réseau qui facilite les demandes d'autorisation du demandeur, par exemple Cisco Catalyst 3560
- Authentication Server : serveur RADIUS (Remote Authentication Dial-In User Server) qui fournit le service d'authentification, par exemple Cisco Secure Access Control Server

Les téléphones IP Cisco Unified contiennent également un demandeur 802.1X. Ce demandeur permet aux administrateurs réseau de contrôler la connectivité des téléphones IP aux ports de commutation LAN. La version initiale du demandeur du téléphone IP 802.1X implémente l'option EAP-MD5 pour l'authentification 802.1X. Dans une configuration multidomaine, le téléphone IP et l'ordinateur connecté doivent demander indépendamment l'accès au réseau en spécifiant un nom d'utilisateur et un mot de passe. Le périphérique Authenticator peut demander des informations à partir de RADIUS appelées attributs. Les attributs spécifient des informations d'autorisation supplémentaires telles que si l'accès à un VLAN particulier est autorisé pour un demandeur. Ces attributs peuvent être spécifiques au fournisseur. Cisco utilise l'attribut RADIUS `cisco-av-pair` afin de dire à l'authentificateur (Cisco Catalyst 3560) qu'un demandeur (téléphone IP) est autorisé sur le VLAN voix.

Configuration

Dans cette section, vous trouverez les informations nécessaires à la configuration de la fonction d'authentification multidomaine 802.1x décrite dans ce document.

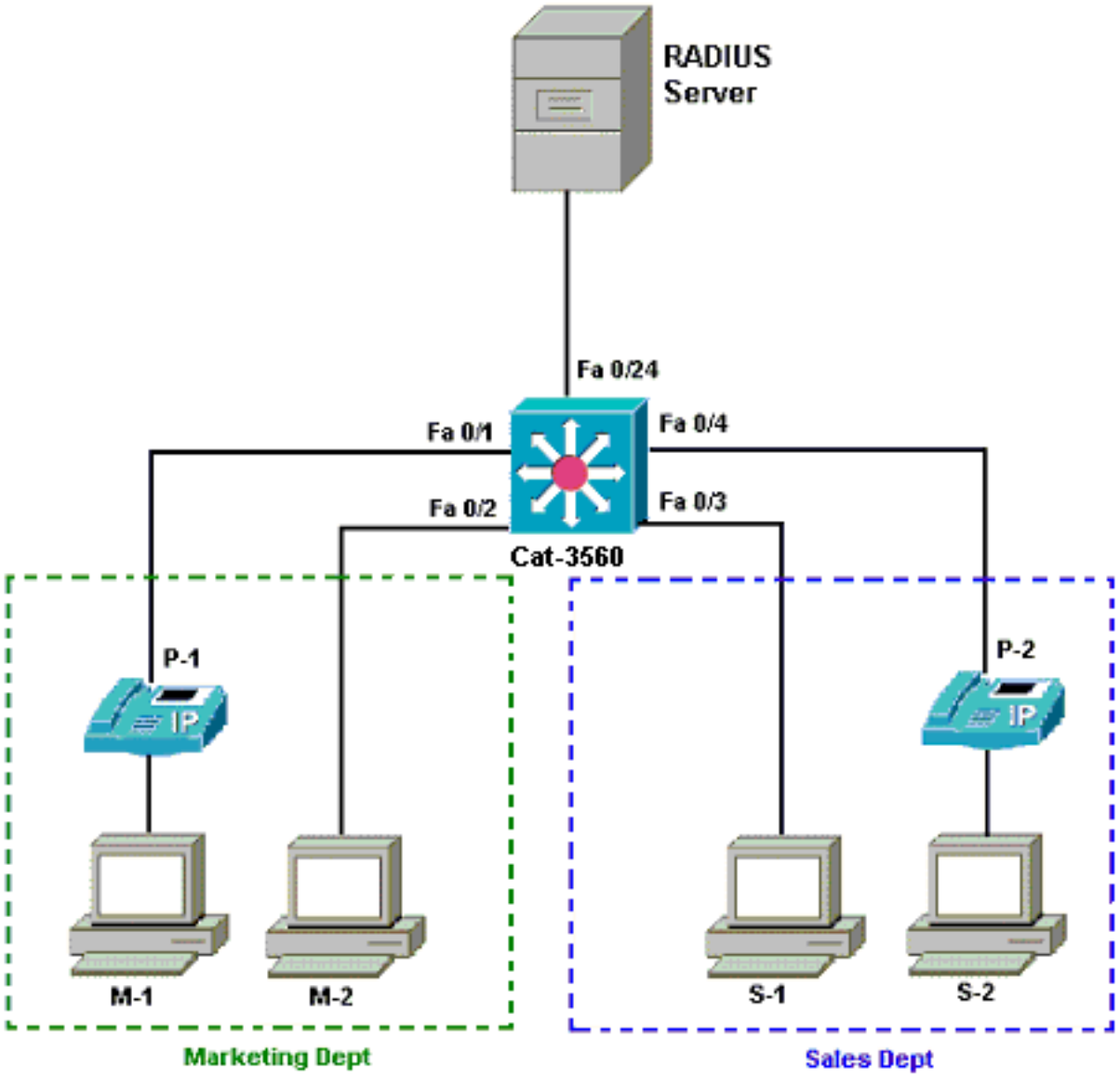
Cette configuration requiert les étapes suivantes :

- Configurez le commutateur Catalyst pour l'authentification multidomaine 802.1x.
- Configurez le serveur RADIUS.
- Configurez les clients PC pour utiliser l'authentification 802.1x.
- Configurez les téléphones IP pour utiliser l'authentification 802.1x.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin de trouver plus d'informations sur les commandes utilisées dans ce document.

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, Cisco ACS est installé et configuré sur un serveur de convergence des supports (MCS) pour l'authentification et l'affectation de VLAN. Le MCS est également le serveur TFTP et Cisco Unified Communications Manager (Cisco CallManager) pour les téléphones IP.
- 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 3560 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. Pour ce faire, il ajoute l'identité de l'utilisateur authentifié au processus de détection DHCP. Les ports FastEthernet 0/1 et 0/4 sont les seuls ports configurés pour l'authentification multidomaine 802.1x. Les ports FastEthernet 0/2 et 0/3 sont en mode hôte unique 802.1x par défaut. Le port FastEthernet 0/24 se connecte au serveur RADIUS.**Remarque :** Si vous utilisez un serveur DHCP externe, n'oubliez pas d'ajouter la commande **ip helper-address** sur l'interface SVI (vlan), dans laquelle réside le client, qui pointe vers le serveur DHCP.

- Clients : il s'agit de périphériques, par exemple, de téléphones IP ou de stations de travail, qui demandent l'accès aux services LAN et de commutateur et répondent aux demandes du commutateur. Ici, les clients sont configurés afin d'atteindre l'adresse IP à partir d'un serveur DHCP. Les périphériques M-1, M-2, S-1 et S-2 sont les clients de station de travail qui demandent l'accès au réseau. P-1 et P-2 sont les clients de téléphone IP qui demandent l'accès au réseau. M-1, M-2 et P-1 sont des appareils clients du service marketing. S-1, S-2 et P-2 sont des périphériques clients du service des ventes. Les téléphones IP P-1 et P-2 sont configurés pour être dans le même VLAN voix (VLAN 3). Les stations de travail M-1 et M-2 sont configurées pour se trouver dans le même VLAN de données (VLAN 4) après une authentification réussie. Les stations de travail S-1 et S-2 sont également configurées pour être dans le même VLAN de données (VLAN 5) après une authentification réussie.**Remarque :** Vous pouvez utiliser l'affectation de VLAN dynamique à partir d'un serveur RADIUS uniquement pour les périphériques de données.

Configurer le commutateur Catalyst pour l'authentification multidomaine 802.1x

Cet exemple de configuration de commutateur inclut :

- Comment activer l'authentification multidomaine 802.1x sur les ports de commutateur
- Configuration liée au serveur RADIUS
- Configuration du serveur DHCP pour l'attribution d'adresses IP
- Routage inter-VLAN pour établir la connectivité entre les clients après authentification

Référez-vous à Utilisation de l'authentification multidomaine pour plus d'informations sur les directives de configuration de MDA.

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

Remarque : Seule la configuration appropriée est affichée ici.

Cat -3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
!--- Sets the hostname for the switch. Cat-
3560(config)#vlan 2
Cat-3560(config-vlan)#name SERVER
Cat-3560(config-vlan)#vlan 3
Cat-3560(config-vlan)#name VOICE
Cat-3560(config-vlan)#vlan 4
Cat-3560(config-vlan)#name MARKETING
Cat-3560(config-vlan)#vlan 5
Cat-3560(config-vlan)#name SALES
Cat-3560(config-vlan)#vlan 6
Cat-3560(config-vlan)#name GUEST_and_AUTHFAIL
!--- VLAN should already exist in the switch for a
successful authentication. Cat-3560(config-vlan)#exit
Cat-3560(config)#interface vlan 2
Cat-3560(config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for the RADIUS Server.
Cat-3560(config-if)#interface vlan 3
Cat-3560(config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for IP Phone clients in
```

```
VLAN 3. Cat-3560(config-if)#interface vlan 4
Cat-3560(config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
4. Cat-3560(config-if)#interface vlan 5
Cat-3560(config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
5. Cat-3560(config-if)#exit
Cat-3560(config)#ip routing
!--- Enables IP routing for interVLAN routing. Cat-
3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#shut
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
!--- This is a dedicated VLAN for the RADIUS server.
Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 ,
fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
!--- You must configure the voice VLAN for the IP phone
when the !--- host mode is set to multidomain. !---
Note: If you use a dynamic VLAN in order to assign a
voice VLAN !--- on an MDA-enabled switch port, the voice
device fails authorization.

Cat-3560(config-if-range)#dot1x port-control auto
!--- Enables IEEE 802.1x authentication on the port.
Cat-3560(config-if-range)#dot1x host-mode multi-domain
!--- Allow both a host and a voice device to be !---
authenticated on an IEEE 802.1x-authorized port. Cat-
3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
!--- The guest VLAN and restricted VLAN features only
apply to the data devices !--- on an MDA enabled port.
Cat-3560(config-if-range)#dot1x reauthentication
!--- Enables periodic re-authentication of the client.
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
!--- Set the number of seconds between re-authentication
attempts. Cat-3560(config-if-range)#dot1x auth-fail max-
attempts 2
!--- Specifies the number of authentication attempts to
allow !--- before a port moves to the restricted VLAN.
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
!--- By default a 802.1x authorized port allows only a
single client. Cat-3560(config-if-range)#dot1x guest-
vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- This pool assigns ip address for IP Phones. !---
```

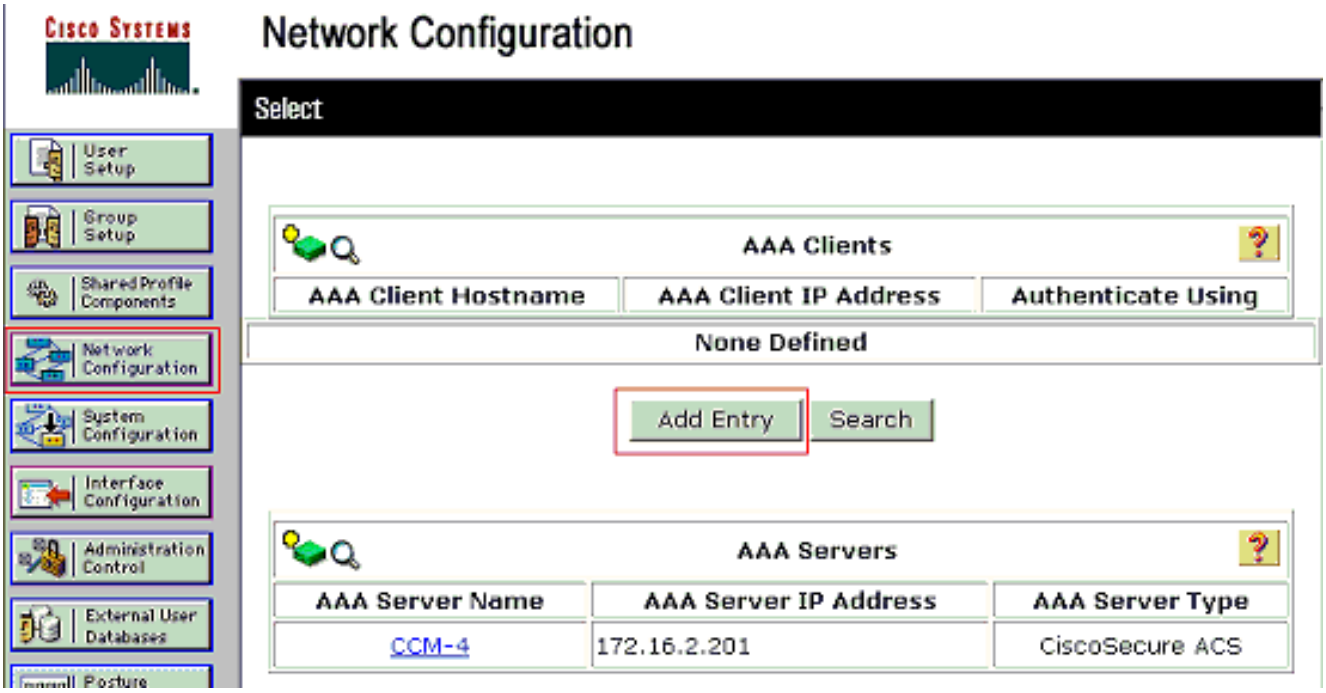
```
Option 150 is for the TFTP server. Cat-3560(dhcp-
config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- This pool assigns ip address for PC clients in
Marketing Dept. Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
!--- This pool assigns ip address for PC clients in
Sales Dept. Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1
Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group
radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat-3560(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat-3560(config)#radius-server host
172.16.2.201 key CisCo123
!--- The key must match the key used on the RADIUS
server. Cat-3560(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat-3560(config)#interface
range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------
-----------------------
1    default                           active    Fa0/1,
Fa0/2, Fa0/3, Fa0/4
                                                 Fa0/5,
Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9,
Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13,
Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17,
Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21,
Fa0/22, Fa0/23, Gi0/1
                                                 Gi0/2
2    SERVER                            active    Fa0/24
3    VOICE                             active    Fa0/1,
Fa0/4
4    MARKETING                         active
5    SALES                             active
6    GUEST_and_AUTHFAIL                active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

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

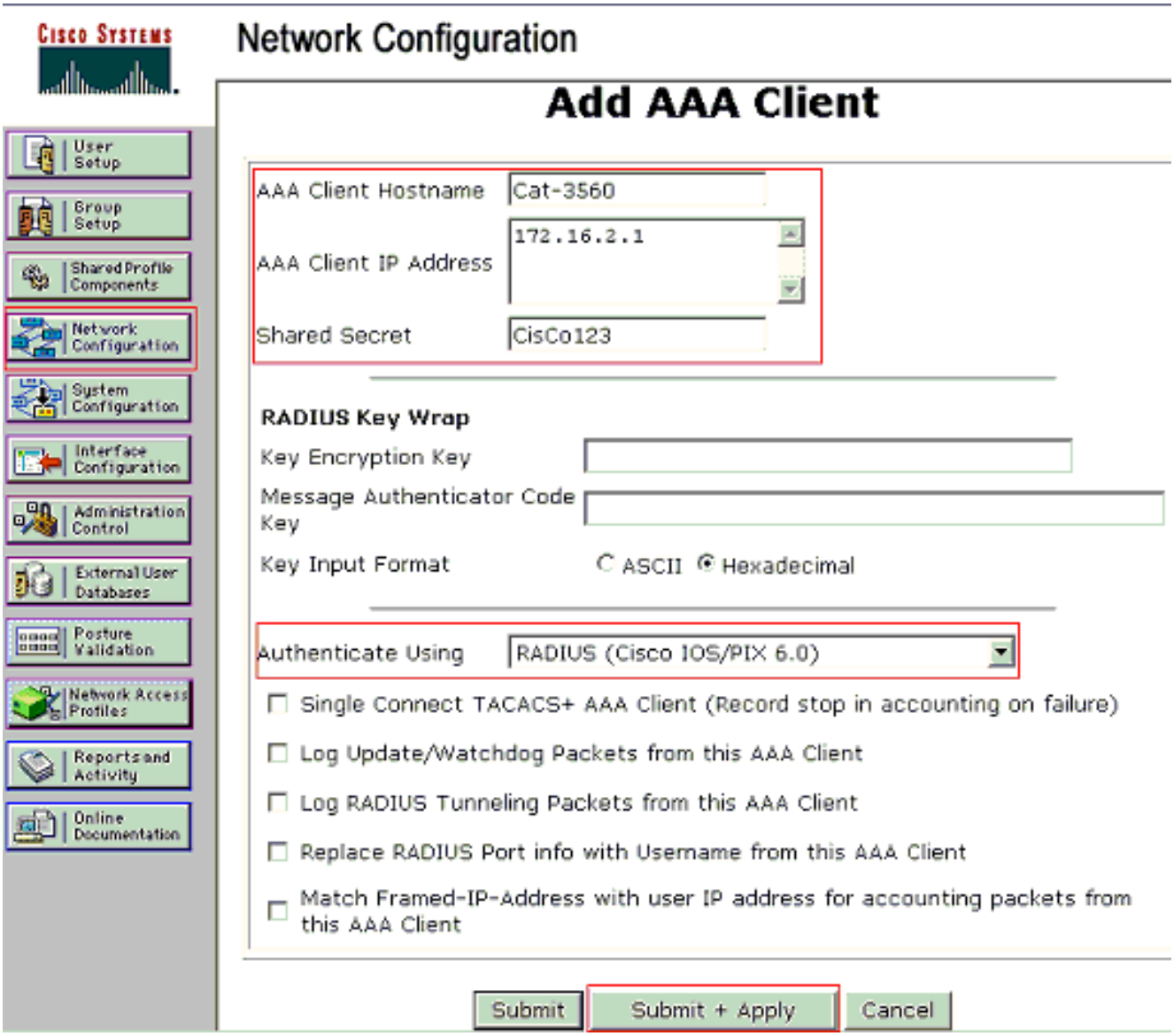
Configurer le serveur RADIUS

Le serveur RADIUS est configuré avec l'adresse IP statique 172.16.2.201/24. 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 (**Cat-3560**).Adresse IP du client AAA = Adresse IP de l'interface de gestion du commutateur (**172.16.2.1**).Shared Secret = clé RADIUS configurée sur le commutateur (**CisCo123**).**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.Authentifier à l'aide de = **RADIUS (Cisco IOS/PIX 6.0)**.**Remarque :** l'attribut de paire Cisco Attribute-Value (AV) est disponible sous cette option.
4. Cliquez sur **Soumettre + Appliquer** afin de rendre ces modifications effectives, comme le montre cet exemple :



Configuration du groupe

Reportez-vous à ce tableau afin de configurer le serveur RADIUS pour l'authentification.

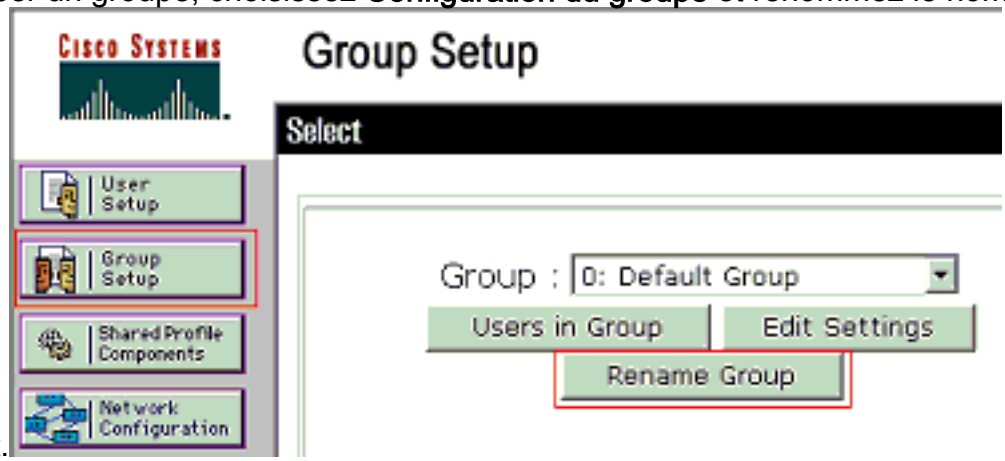
Périphérique	Dépôt	Groupe	Utilisateur	Mot de passe	VLAN	Pool DHCP
M-1	Marketing	Marketing	mkt-manager	Cisco	MARKETING	Marketing
M-2	Marketing	Marketing	mkt-staff	MScisco	MARKETING	Marketing
S-2	Ventes	Ventes	gestionnaire de ventes	SMcisco	VENTES	Ventes
S-1	Ventes	Ventes	personnel de	Cisco	VENTES	Ventes

			vente			
P-1	Marketing	Téléphones IP	CP-7970G-SEP001759E7492C	P1cisco	VOIX	Téléphones IP
P-2	Ventes	Téléphones IP	CP-7961G-SEP001A2F80381F	P2cisco	VOIX	Téléphones IP

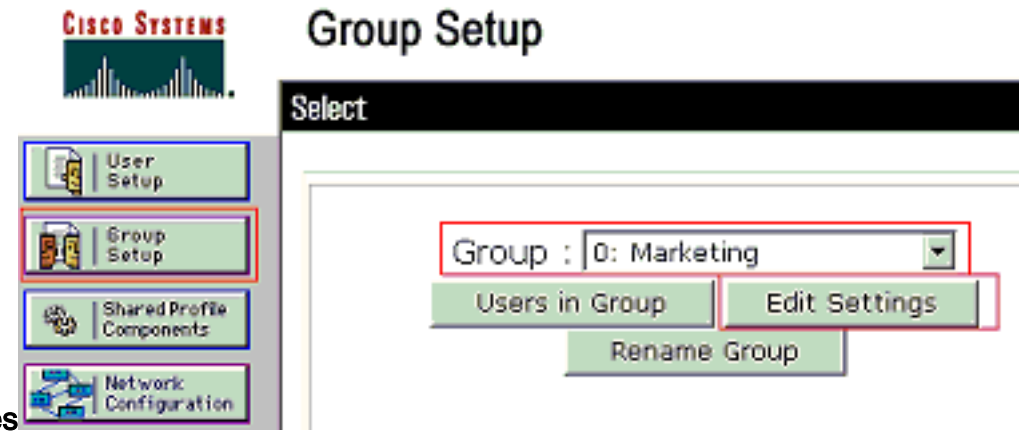
Créez des groupes pour les clients qui se connectent aux VLAN 3 (VOIX), 4 (MARKETING) et 5 (VENTES). Ici, les groupes **Téléphones IP**, **Marketing** et **Ventes** sont créés à cette fin.

Remarque : Il s'agit de la configuration des groupes **Marketing** et **Téléphones IP**. Pour la configuration du groupe **Sales**, complétez les étapes pour le groupe **Marketing**.

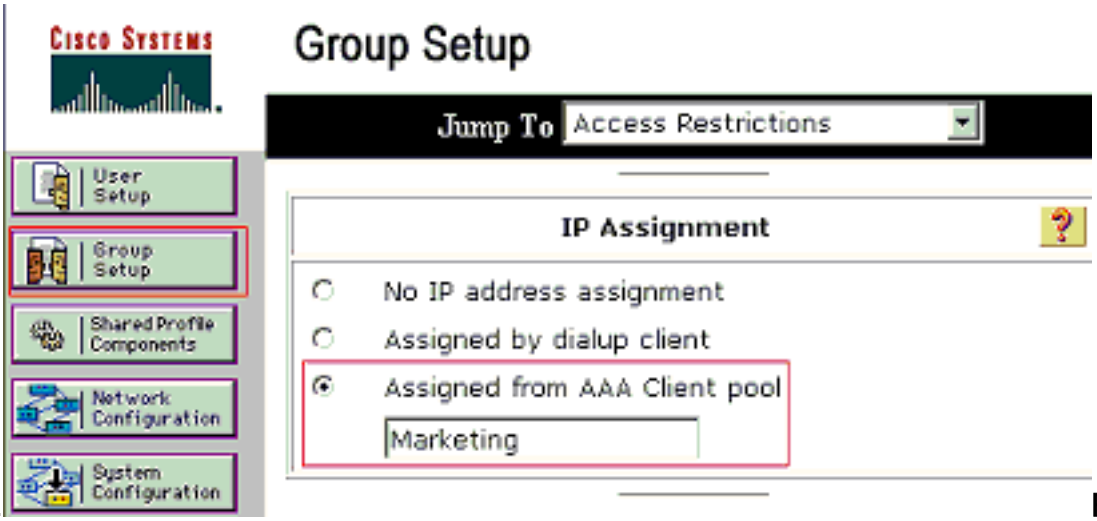
1. Afin de créer un groupe, choisissez **Configuration du groupe** et renommez le nom de groupe par défaut.



2. Afin de configurer un groupe, choisissez le groupe dans la liste et cliquez sur **Modifier les paramètres**

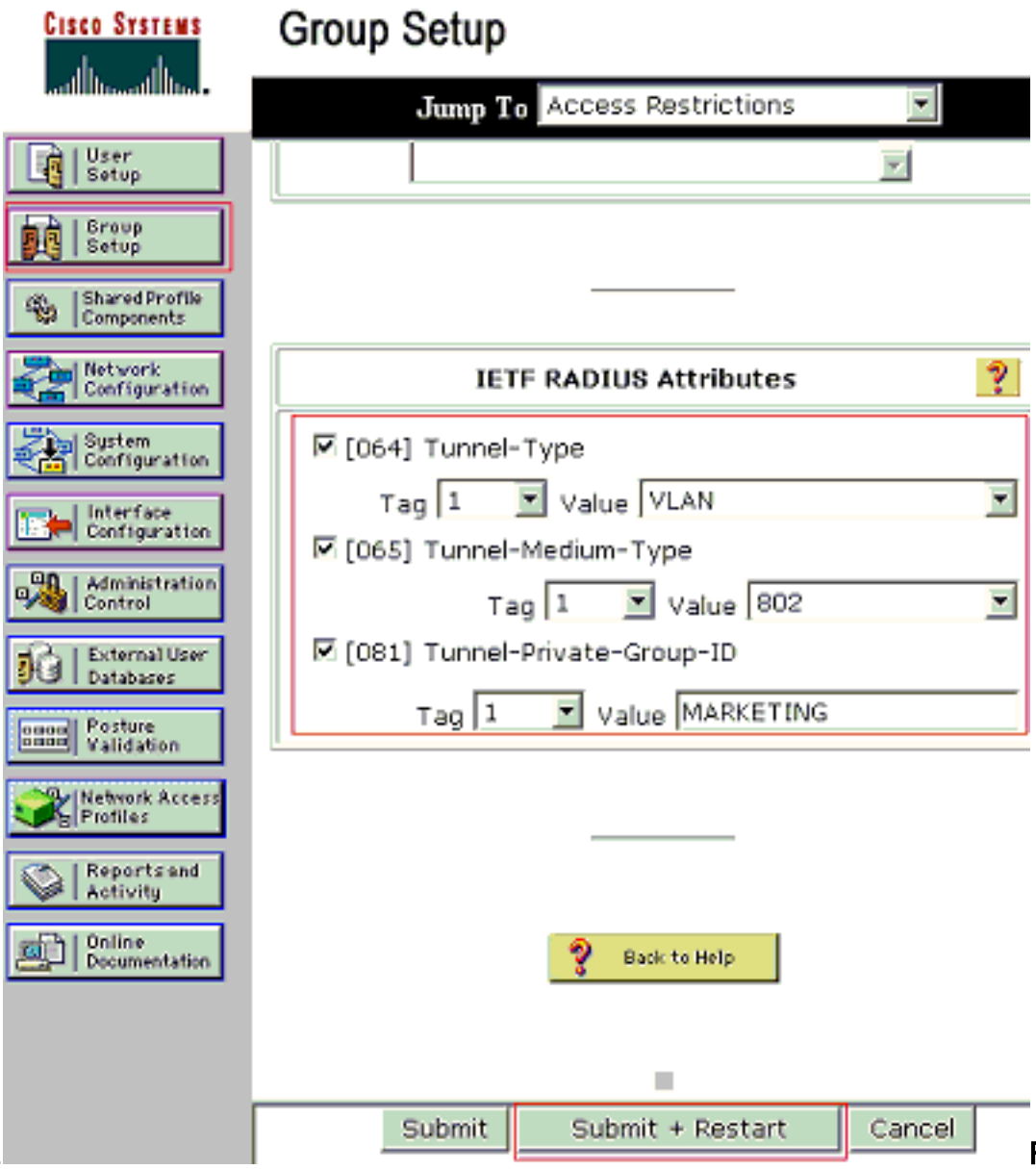


3. Définissez l'affectation d'adresse IP du client comme **Attribué par le pool de clients AAA**. Entrez le nom du pool d'adresses IP configuré sur le commutateur pour ce groupe de



clients.**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.**Remarque :** Pour la configuration du groupe de **téléphones IP** uniquement, ignorez l'étape suivante, l'étape 4, et passez à l'étape 5.

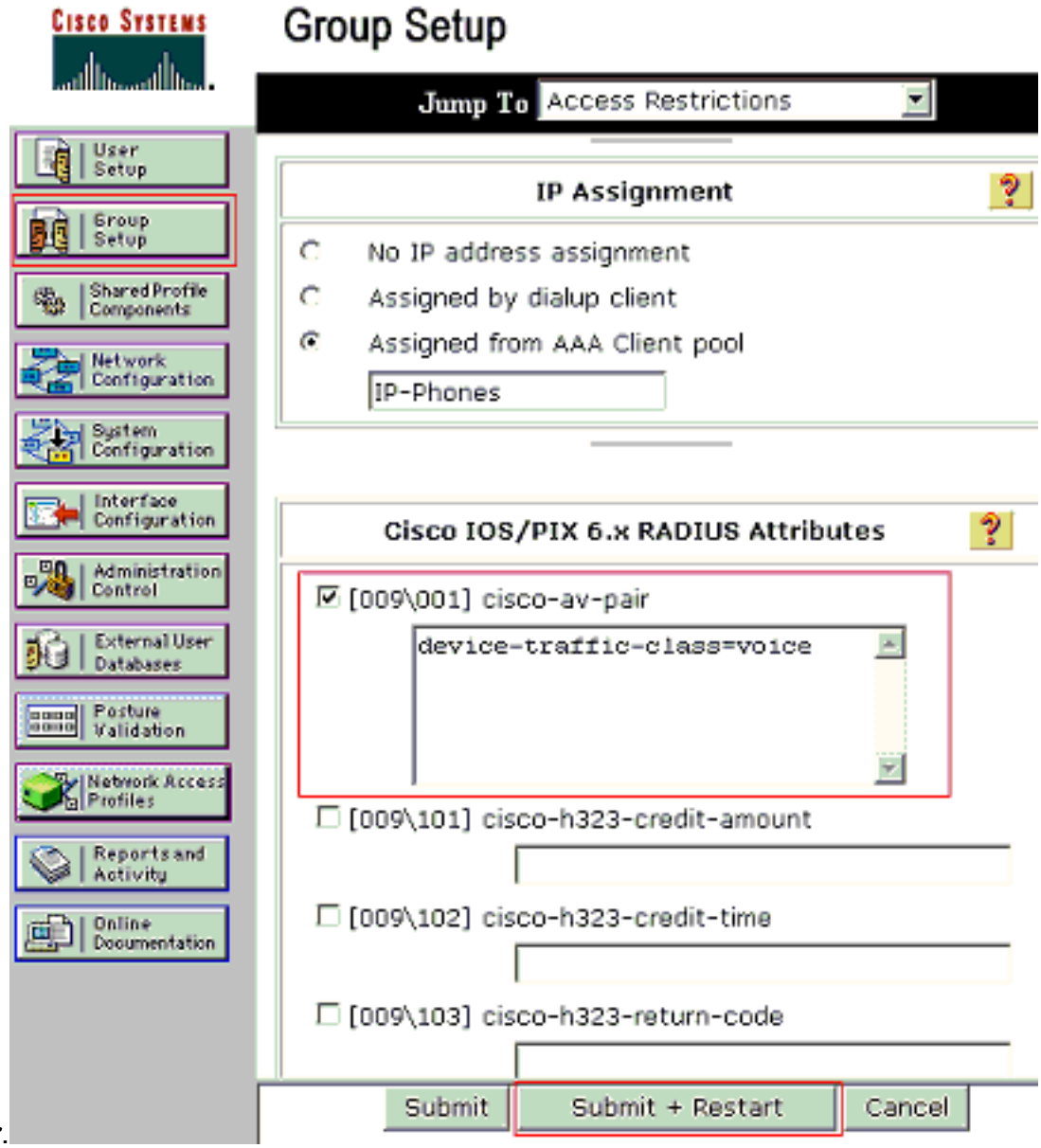
4. Définissez les attributs **64**, **65** et **81** de l'IETF (Internet Engineering Task Force), puis cliquez sur **Soumettre + Redémarrer**.Assurez-vous que les balises des valeurs sont définies sur **1**, comme le montre cet exemple. Catalyst ignore toute balise autre que 1. Pour affecter un utilisateur 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 :** reportez-vous à la [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**. 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 est affecté 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.**Remarque :** L'étape suivante ne s'applique qu'au groupe **de téléphones IP**.

5. Configurez le serveur RADIUS pour envoyer un attribut de paire Cisco Attribute-Value (AV) pour autoriser un périphérique vocal. Sans cela, le commutateur traite le périphérique vocal comme un périphérique de données. Définissez l'attribut de paire Attribut-Valeur (AV) Cisco avec la valeur *device-traffic-class=voice* et cliquez sur **Soumettre +**

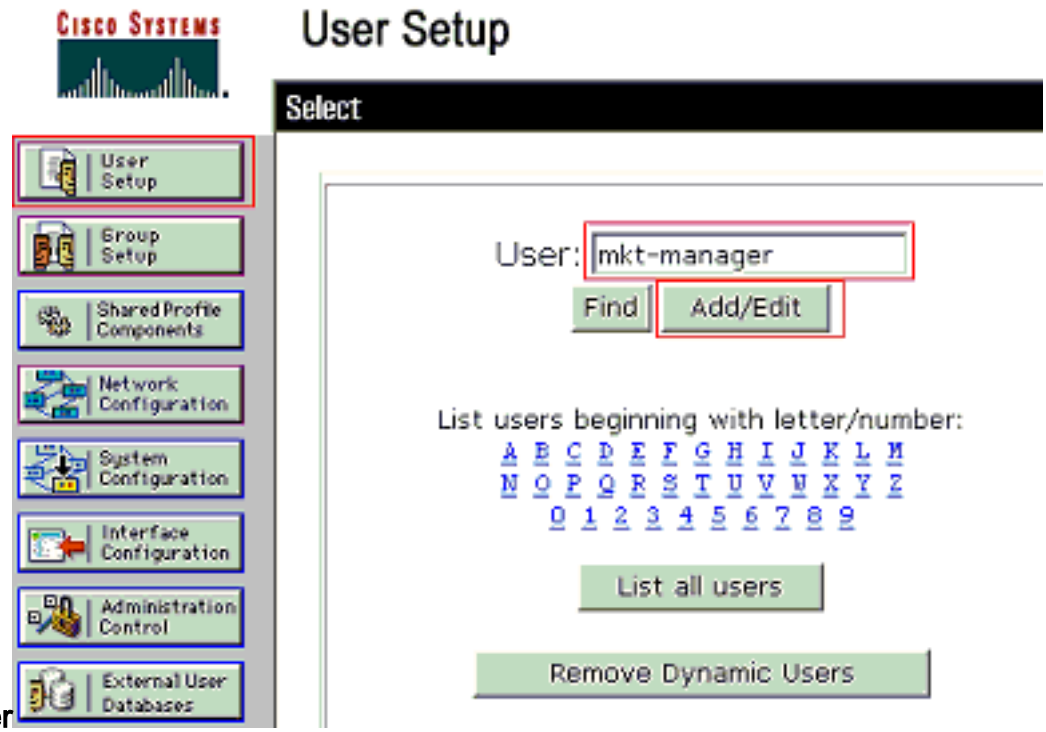
Redémarrer.



Configuration utilisateur

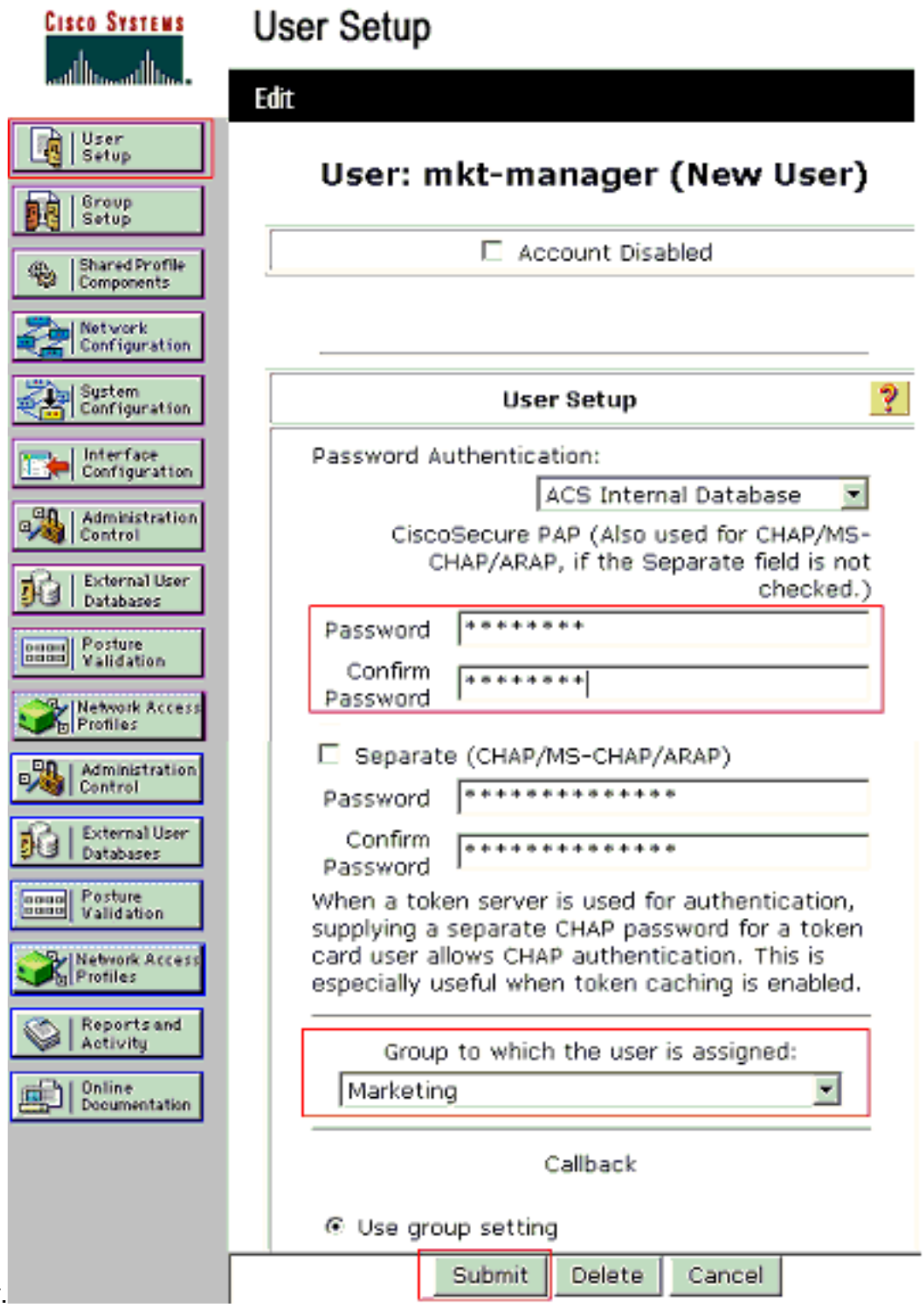
Complétez ces étapes afin d'ajouter et de configurer un utilisateur.

1. Afin d'ajouter et de configurer des utilisateurs, choisissez **User Setup**. Entrez le nom d'utilisateur et cliquez sur



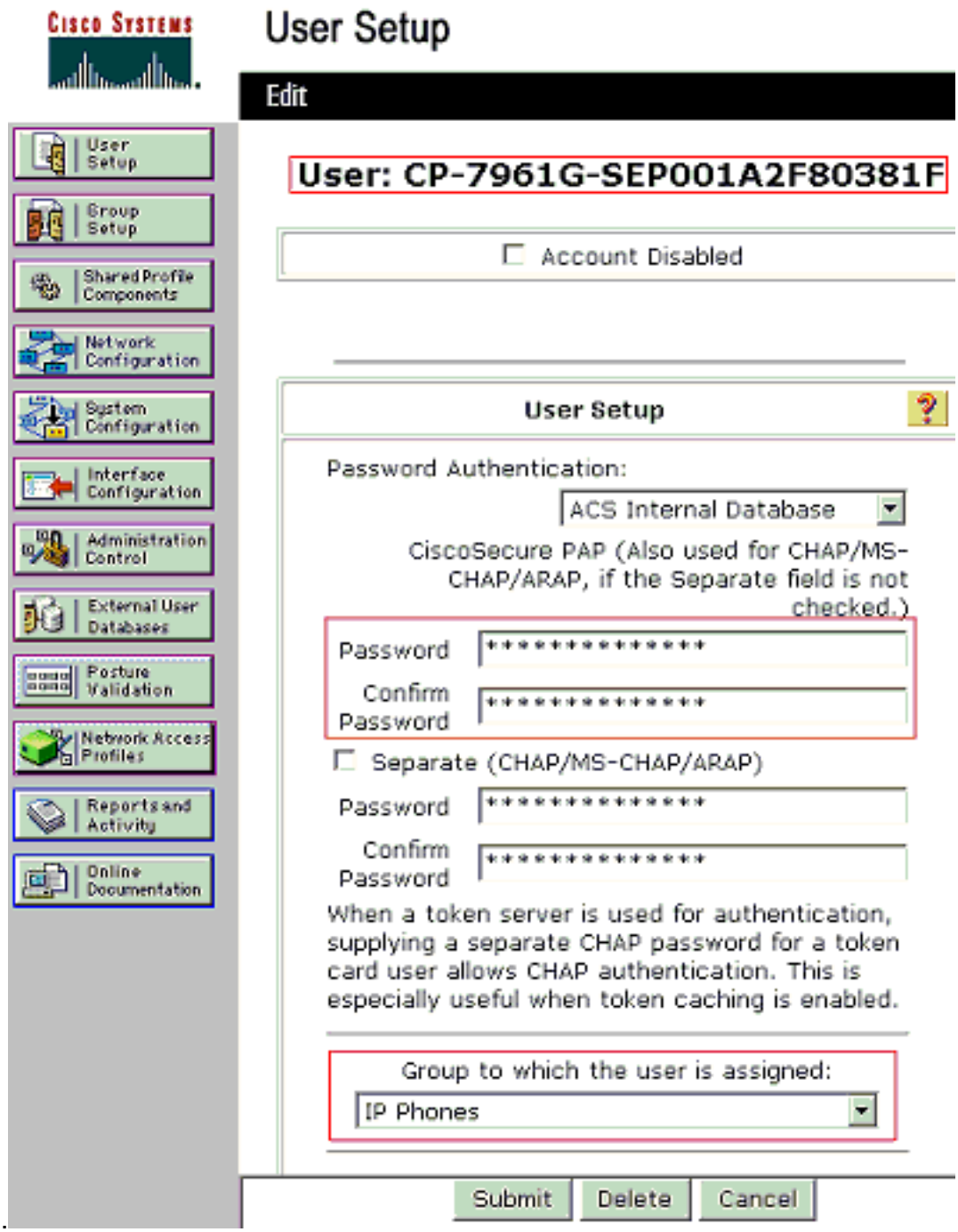
Ajouter/Modifier

2. Définissez le nom d'utilisateur, le mot de passe et le groupe de



l'utilisateur.

3. Le téléphone IP utilise son ID de périphérique comme nom d'utilisateur et secret partagé comme mot de passe d'authentification. Ces valeurs doivent correspondre sur le serveur RADIUS. Pour les téléphones IP P-1 et P-2, créez des noms d'utilisateur identiques à leur ID de périphérique et à leur mot de passe identiques au secret partagé configuré. Reportez-vous à la section Configurer les téléphones IP pour utiliser l'authentification 802.1x pour plus d'informations sur l'ID de périphérique et le secret partagé sur un téléphone

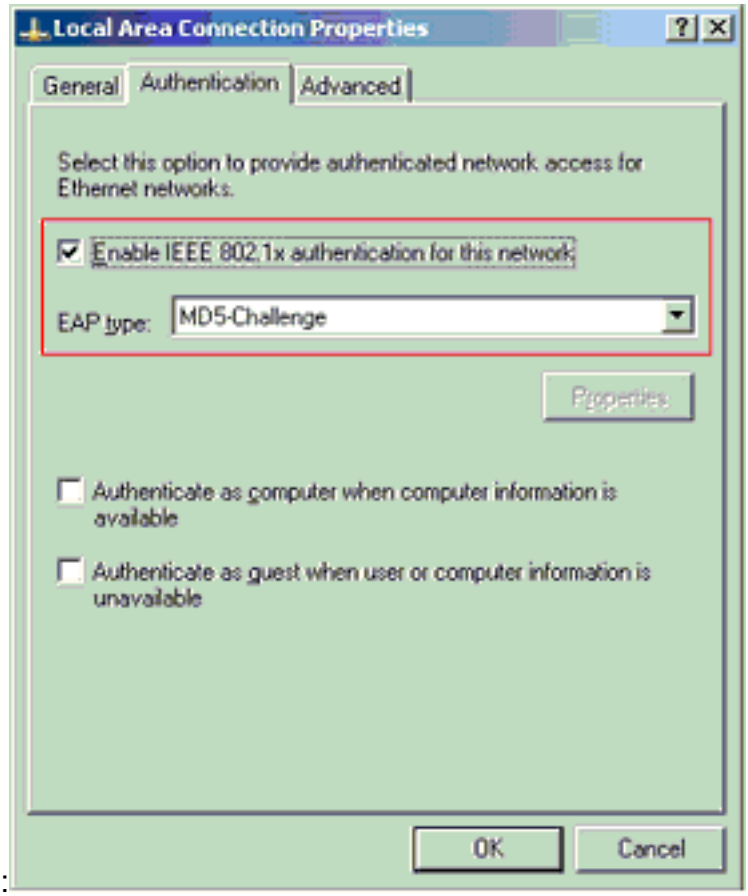


IP.

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) :

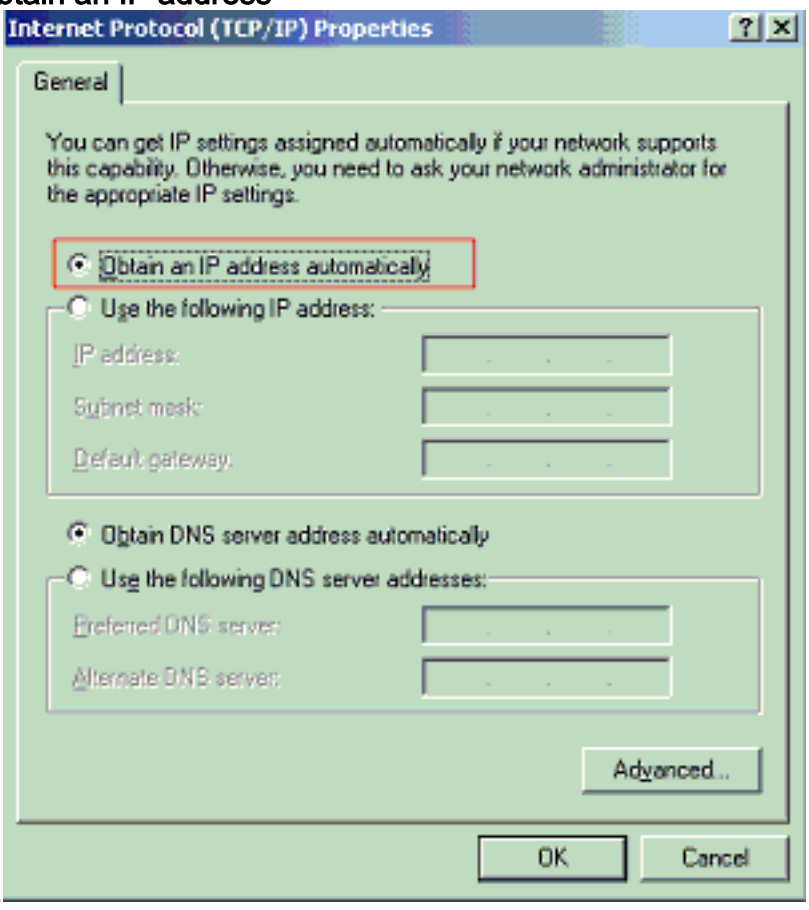
1. Choisissez **Démarrer > Panneau de configuration > Connexions réseau**, puis cliquez avec le bouton droit sur votre **Connexion au réseau local** et choisissez **Propriétés**.
2. Cochez **l'icône Afficher dans la zone de notification lorsque vous êtes connecté** sous l'onglet Général.
3. Sous l'onglet 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



:

Complétez ces étapes afin de configurer les clients pour obtenir 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.

Configurer les téléphones IP pour utiliser l'authentification 802.1x

Complétez ces étapes afin de configurer les téléphones IP pour l'authentification 802.1x.

1. Appuyez sur le bouton **Paramètres** afin d'accéder aux paramètres **d'authentification 802.1X** et choisissez **Configuration de sécurité > Authentification 802.1X > Authentification du périphérique**.
2. Définissez l'option **Authentification du périphérique** sur **Activé**.
3. Appuyez sur la touche **Save.**
4. Choisissez **802.1X Authentication > EAP-MD5 > Shared Secret** afin de définir un mot de passe sur le téléphone.
5. Entrez le secret partagé et appuyez sur **Enregistrer**.**Remarque :** Le mot de passe doit comporter entre six et 32 caractères, composés de n'importe quelle combinaison de chiffres ou de lettres. `Cette clé n'est pas active ici`, un message s'affiche et le mot de passe n'est pas enregistré si cette condition n'est pas remplie.**Remarque :** si vous désactivez l'authentification 802.1X ou effectuez une réinitialisation d'usine sur le téléphone, le secret partagé MD5 précédemment configuré est supprimé.**Remarque :** Les autres options, ID de périphérique et domaine ne peuvent pas être configurées. L'ID de périphérique est utilisé comme nom d'utilisateur pour l'authentification 802.1x. Il s'agit d'un dérivé du numéro de modèle du téléphone et de l'adresse MAC unique affichés dans ce format : CP-<model>-SEP-<MAC>. Par exemple, **CP-7970G-SEP001759E7492C**. Référez-vous à Paramètres d'authentification 802.1X pour plus d'informations.

Complétez ces étapes afin de configurer le téléphone IP pour obtenir l'adresse IP d'un serveur DHCP.

1. Appuyez sur le bouton **Paramètres** afin d'accéder aux paramètres **Configuration réseau** et choisissez **Configuration réseau**.
2. Déverrouiller les options **de configuration réseau**. Pour déverrouiller, appuyez sur ****#**.**Remarque :** N'appuyez pas ****#** pour déverrouiller les options, puis immédiatement sur ****#** pour verrouiller les options. Le téléphone interprète cette séquence comme ****#****, qui réinitialise le téléphone. Afin de verrouiller les options après les déverrouiller, attendez au moins 10 secondes avant d'appuyer à nouveau sur ****#**.
3. Faites défiler jusqu'à l'option DHCP Enabled et appuyez sur la touche de fonction **Yes** afin d'activer DHCP.
4. Appuyez sur la touche **Save.**

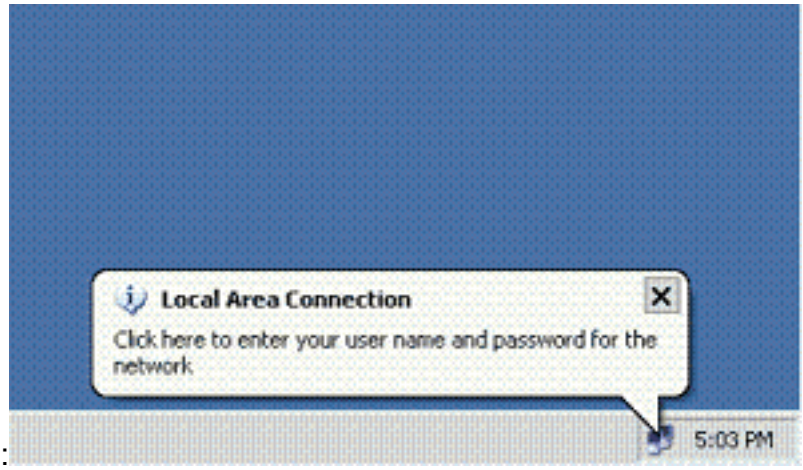
Vérification

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

Clients PC

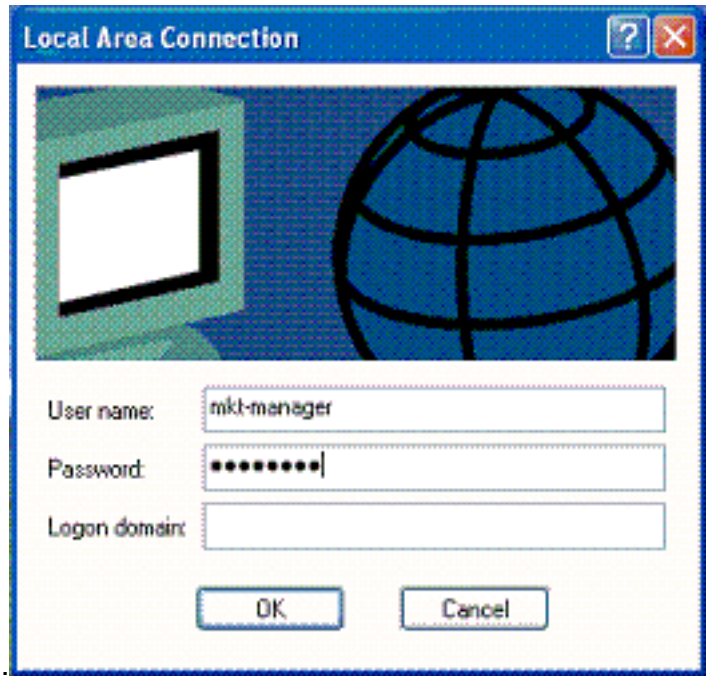
Si vous avez correctement terminé la configuration, les clients PC affichent une invite contextuelle pour saisir un nom d'utilisateur et un mot de passe.

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



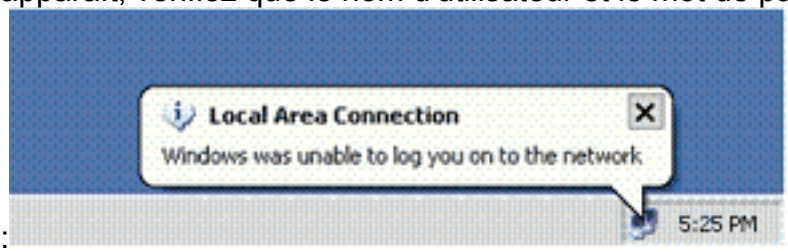
: Une fenêtre de saisie de nom d'utilisateur et de mot de passe s'affiche.**Remarque :** MDA n'applique pas l'ordre d'authentification des périphériques. Mais pour obtenir de meilleurs résultats, Cisco recommande qu'un périphérique vocal soit authentifié avant un périphérique de données sur un port MDA activé.

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



passe.

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



:

Téléphones IP

Le menu 802.1X Authentication Status (Etat d'authentification) des téléphones IP permet de surveiller l'état d'authentification.

1. Appuyez sur le bouton **Paramètres** afin d'accéder aux statistiques en temps réel

d'authentification 802.1X et sélectionnez **Configuration de sécurité > 802.1X Authentication Status**.
2. Le **statut de la transaction** doit être **authentifié**. Référez-vous à État en temps réel de l'authentification 802.1X pour plus d'informations.**Remarque :** L'état de l'authentification peut également être vérifié à partir de **Paramètres > État > Messages d'état**.

Commutateur de couche 3

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.

```
Cat-3560#show dot1x all summary
Interface       PAE     Client          Status
---------------------------------------------------------
Fa0/1           AUTH    0016.3633.339c  AUTHORIZED
                        0017.59e7.492c  AUTHORIZED
Fa0/2           AUTH    0014.5e94.5f99  AUTHORIZED
Fa0/3           AUTH    0011.858D.9AF9  AUTHORIZED
Fa0/4           AUTH    0016.6F3C.A342  AUTHORIZED
                        001a.2f80.381f  AUTHORIZED


Cat-3560#show dot1x interface fastEthernet 0/1 details

Dot1x Info for FastEthernet0/1
-----------------------------------
PAE                     = AUTHENTICATOR
PortControl             = AUTO
ControlDirection        = Both
HostMode                = MULTI_DOMAIN
ReAuthentication        = Enabled
QuietPeriod             = 10
ServerTimeout           = 30
SuppTimeout             = 30
ReAuthPeriod            = 60 (Locally configured)
ReAuthMax               = 2
MaxReq                  = 2
TxPeriod                = 30
RateLimitPeriod         = 0
Auth-Fail-Vlan          = 6
Auth-Fail-Max-attempts  = 2
Guest-Vlan              = 6

Dot1x Authenticator Client List
-------------------------------
Domain                  = DATA
Supplicant              = 0016.3633.339c
    Auth SM State       = AUTHENTICATED
    Auth BEND SM State  = IDLE
Port Status             = AUTHORIZED
ReAuthPeriod            = 60
ReAuthAction            = Reauthenticate
TimeToNextReauth        = 29
Authentication Method   = Dot1x
Authorized By           = Authentication Server
Vlan Policy             = 4

Domain                  = VOICE
Supplicant              = 0017.59e7.492c
```

```
    Auth SM State          = AUTHENTICATED
    Auth BEND SM State     = IDLE
Port Status                = AUTHORIZED
ReAuthPeriod               = 60
ReAuthAction               = Reauthenticate
TimeToNextReauth           = 15
Authentication Method      = Dot1x
Authorized By              = Authentication Server
```

Vérifiez l'état du VLAN après une authentification réussie.

```
Cat-3560#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Gi0/1
                                                Gi0/2
2    SERVER                           active    Fa0/24
3    VOICE                            active    Fa0/1, Fa0/4
4    MARKETING                        active    Fa0/1, Fa0/2
5    SALES                            active    Fa0/3, Fa0/4
6    GUEST_and_AUTHFAIL               active
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 après une authentification réussie.

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.3.2       0100.1759.e749.2c       Aug 24 2007 06:35 AM    Automatic
172.16.3.3       0100.1a2f.8038.1f       Aug 24 2007 06:43 AM    Automatic
172.16.4.2       0100.1636.3333.9c       Aug 24 2007 06:50 AM    Automatic
172.16.4.3       0100.145e.945f.99       Aug 24 2007 08:17 AM    Automatic
172.16.5.2       0100.166F.3CA3.42       Aug 24 2007 08:23 AM    Automatic
172.16.5.3       0100.1185.8D9A.F9       Aug 24 2007 08:51 AM    Automatic
```

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

Dépannage

Échec de l'authentification du téléphone IP

L'état du téléphone IP affiche `Configuration d'IP` ou `Enregistrement` en cas d'échec de l'authentification 802.1x. Complétez ces étapes afin de résoudre ces problèmes :

- Vérifiez que le 802.1x est activé sur le téléphone IP.
- Vérifiez que l'ID de périphérique est entré sur le serveur d'authentification (RADIUS) en tant que nom d'utilisateur.
- Vérifiez que le secret partagé est configuré sur le téléphone IP.
- Si le secret partagé est configuré, vérifiez que le même secret partagé est entré sur le serveur d'authentification.
- Vérifiez que vous avez correctement configuré les autres périphériques requis, par exemple le

commutateur et le serveur d'authentification.

Informations connexes

- Configuration de l'authentification basée sur les ports IEEE 802.1x
- Configurer le téléphone IP pour utiliser l'authentification 802.1x
- 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
- Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant Cisco IOS
- Exemple de configuration de l'authentification IEEE 802.1x avec Catalyst 6500/6000 exécutant CatOS
- Pages de support pour les produits LAN
- Page de support sur la commutation LAN
- Support et documentation techniques - Cisco Systems