

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](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurez le commutateur de Catalyst pour l'authentification de Multi-domaine de 802.1x](#)

[Configurez le serveur de RAYON](#)

[Configurez les clients PC pour utiliser l'authentification de 802.1x](#)

[Configurez les Téléphones IP pour utiliser l'authentification de 802.1x](#)

[Vérifiez](#)

[Clients PC](#)

[Téléphones IP](#)

[Commutateur de la couche 3](#)

[Dépannez](#)

[L'authentification de téléphone IP échoue](#)

[Informations connexes](#)

[Introduction](#)

L'authentification de Multi-domaine permet à un téléphone IP et à un PC pour authentifier sur le même port de commutateur tandis qu'elle les place sur la Voix et les données appropriées VLAN. Ce document explique comment configurer l'authentification de Multi-domaine de 802.1x d'IEEE (MDA) sur des Commutateurs de configuration fixe de la couche 3 de Cisco Catalyst.

[Conditions préalables](#)

[Conditions requises](#)

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

- [Fonctionnement de RADIUS](#)
- [Commutation de Catalyst et guide de déploiement ACS](#)
- [Guide utilisateur pour le Cisco Secure Access Control Server 4.1](#)
- [Un aperçu du téléphone IP unifié Cisco](#)

Composants utilisés

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

- Commutateur de gamme Cisco Catalyst 3560 qui exécute la version de logiciel 12.2(37)SE1 de Cisco IOS®**Remarque:** Le support d'authentification de Multi-domaine est fourni seulement par le Logiciel Cisco IOS version 12.2(35)SE et plus tard.
- Cet exemple utilise le Cisco Secure Access Control Server (ACS) 4.1 en tant que serveur de RAYON.**Remarque:** Un serveur de RAYON doit être spécifié avant que vous activiez le 802.1x sur le commutateur.
- Clients PC qui prend en charge l'authentification de 802.1x**Remarque:** Cet exemple utilise des clients de Microsoft Windows XP.
- Téléphone IP Cisco Unified 7970G avec la version 8.2(1) de micrologiciels de SCCP
- Téléphone IP Cisco Unified 7961G avec la version 8.2(2) de micrologiciels de SCCP
- Serveur de Couverture de médias (MCS) avec Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

Cette configuration peut également être utilisée avec ces matériels :

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

Remarque: Le commutateur de gamme Cisco Catalyst 3550 ne prend en charge pas l'authentification de Multi-domaine de 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 de 802.1x d'IEEE définit un protocole basé par client-serveur de contrôle d'accès et d'authentification qui limite les périphériques non autorisés de se connecter à un RÉSEAU LOCAL

par les ports publiquement accessibles. Le 802.1x contrôle l'accès au réseau par la création de deux Points d'accès virtuels distincts à chaque port. Un Point d'accès est un port incontrôlé ; l'autre est un port commandé. Tout le trafic par le port unique est disponible aux deux Points d'accès. Le 802.1x authentifie chaque périphérique d'utilisateur qui est connecté à un port de commutateur et assigne le port à un VLAN avant qu'il fasse disponible tous les services qui sont offerts par le commutateur ou le RÉSEAU LOCAL. Jusqu'à ce que le périphérique soit authentifié, le contrôle d'accès de 802.1x permet seulement Extensible Authentication Protocol au-dessus du trafic du RÉSEAU LOCAL (EAPOL) par le port auquel le périphérique est connecté. Après l'authentification est réussie, le trafic normal peut traverser le port.

Le 802.1x est composé de trois composants principaux. Chacun est mentionné comme une entité d'Access de port (PAE).

- Suppliant — Périphérique de client qui demande l'accès au réseau, par exemple, les Téléphones IP et les PC reliés
- Authentificateur — Périphérique de réseau qui facilite les demandes d'autorisation de suppliant, par exemple, Cisco Catalyst 3560
- Serveur d'authentification — Un serveur (RADIUS) d'utilisateur en accès entrant d'authentification à distance, qui fournit le service d'authentification, par exemple, Cisco Secure Access Control Server

Les Téléphones IP de Cisco Unified contiennent également un suppliant de 802.1X. Ce suppliant permet à des administrateurs réseau pour contrôler la Connectivité des Téléphones IP aux ports de commutateur de RÉSEAU LOCAL. La version initiale du suppliant de 802.1X de téléphone IP implémente l'option EAP-MD5 pour l'authentification de 802.1X. Dans une configuration de multi-domaine, le téléphone IP et le PC relié doivent indépendamment demander l'accès au réseau par la spécification d'un nom d'utilisateur et mot de passe. Le périphérique d'authentificateur peut exiger les informations du RAYON appelé les attributs. Les attributs spécifient les informations d'autorisation supplémentaires comme si on permet l'accès à un VLAN particulier pour un suppliant. Ces attributs peuvent être particularité de constructeur. Cisco emploie les Cisco-poids du commerce-paires d'attribut RADIUS afin d'indiquer l'authentificateur (Cisco Catalyst 3560) qu'à un suppliant (téléphone IP) est permis sur la Voix VLAN.

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer la fonction d'authentification de multi-domaine de 802.1x décrite dans ce document.

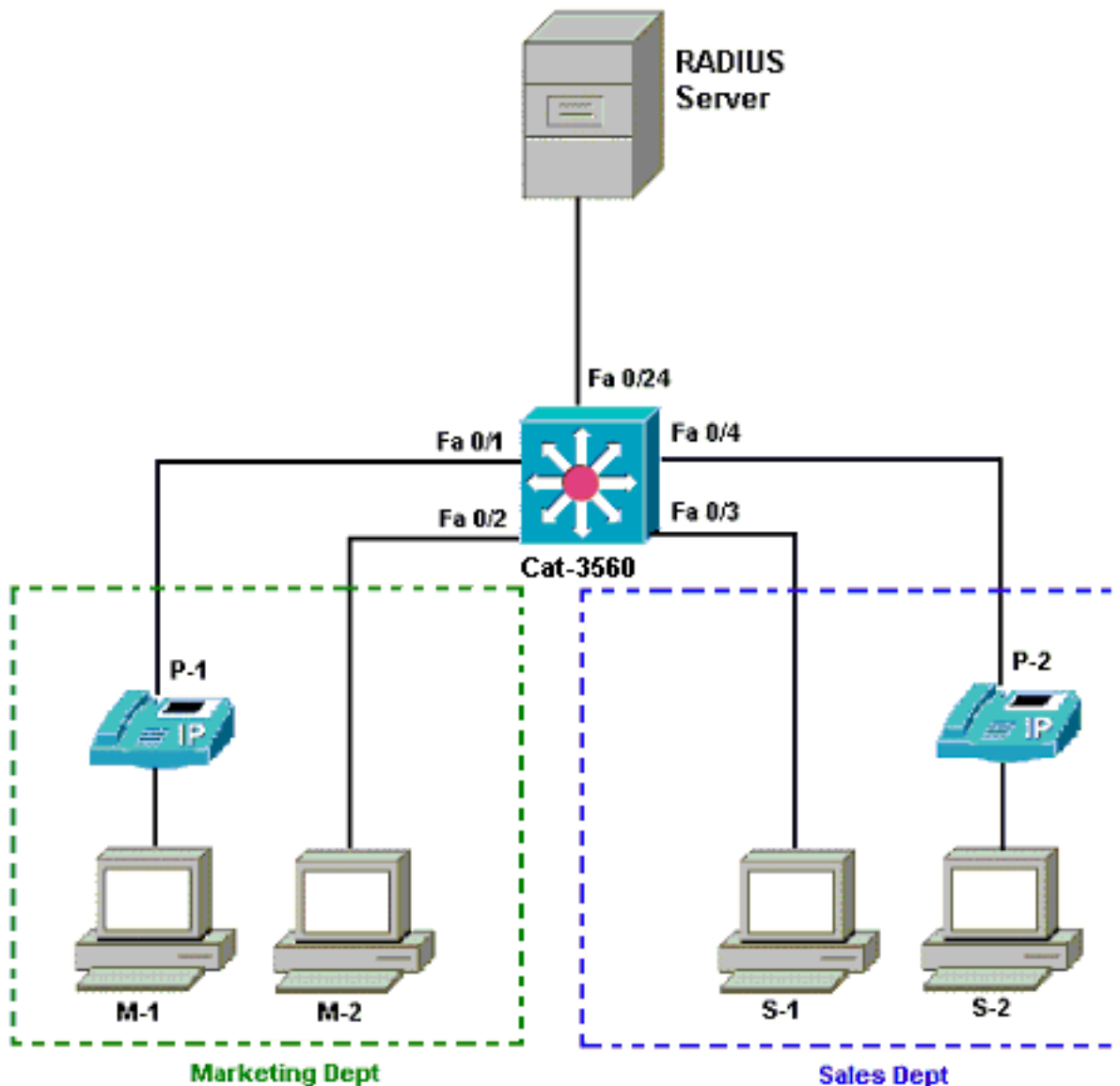
Cette configuration requiert les étapes suivantes :

- [Configurez le commutateur de Catalyst pour l'authentification de Multi-domaine de 802.1x.](#)
- [Configurez le serveur de RAYON.](#)
- [Configurez les clients PC pour utiliser l'authentification de 802.1x.](#)
- [Configurez les Téléphones IP pour utiliser l'authentification de 802.1x.](#)

Remarque: Utilisez l'[outil de recherche de commande](#) (réservé aux [clients inscrits](#)) pour plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



- Serveur de RAYON — Ceci exécute l'authentification réelle du client. Le serveur de RAYON valide l'identité du client et informe le commutateur si le client est autorisé à accéder au RÉSEAU LOCAL et à commuter des services. Ici, Cisco ACS est installé et configuré sur un serveur de Convergence de medias (MCS) pour l'authentification et l'affectation VLAN. Les MCS sont également le serveur TFTP et Cisco Unified Communications Manager (Cisco CallManager) pour les Téléphones IP.
- Commutateur — Ceci contrôle l'accès physique au réseau basé sur l'état d'authentification du client. Le commutateur agit en tant qu'intermédiaire (proxy) entre le client et le serveur de RAYON. Il demande les informations d'identité du client, vérifie ces informations avec le serveur de RAYON, et transmet par relais une réponse au client. Ici, le commutateur de Catalyst 3560 est également configuré comme serveur DHCP. Le soutien d'authentification de 802.1x du protocole DHCP (DHCP) permet au serveur DHCP pour assigner les adresses IP aux classes différentes d'utilisateurs finaux. Afin de faire ceci, il ajoute l'identité de l'utilisateur authentifiée dans le processus de découverte DHCP. Les ports FastEthernet 0/1 et 0/4 sont les seuls ports configurés pour l'authentification de multi-domaine de 802.1x. Les ports FastEthernet 0/2 et 0/3 sont en mode par défaut de seul hôte de 802.1x. Le port FastEthernet 0/24 se connecte au serveur de RAYON. **Remarque:** Si vous utilisez un serveur DHCP externe, n'oubliez pas d'ajouter la commande de **helper-address d'IP** sur l'interface SVI (VLAN), dans laquelle le client réside, qui indique le serveur DHCP.

- Clients — Ce sont des périphériques, par exemple, des Téléphones IP ou des postes de travail, cet accès de demande au RÉSEAU LOCAL et aux services de commutateur et répondent aux demandes du commutateur. Ici, des clients sont configurés afin d'atteindre l'adresse IP d'un serveur DHCP. Les périphériques M-1, m2, S1 et S-2 sont les clients de poste 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, m2 et P-1 sont des périphériques de client au service marketing. Le S1, les S-2 et les P-2 sont des périphériques de client au service de vente. Les Téléphones IP P-1 et P-2 sont configurés pour être dans la même Voix VLAN (VLAN 3). Les postes de travail M-1 et m2 sont configurés pour être dans les mêmes données VLAN (VLAN 4) après une authentification réussie. Les postes de travail S1 et S-2 sont également configurés pour être dans les mêmes données VLAN (VLAN 5) après une authentification réussie. **Remarque:** Vous pouvez utiliser l'affectation dynamique VLAN d'un serveur de RAYON seulement pour les périphériques de données.

[Configurez le commutateur de Catalyst pour l'authentification de Multi-domaine de 802.1x](#)

Cette configuration de commutateur témoin inclut :

- Comment activer l'authentification de multi-domaine de 802.1x sur les ports de commutateur
- Configuration relative de serveur de RAYON
- Configuration du serveur DHCP pour l'affectation d'adresse IP
- Routage inter-VLAN pour avoir la Connectivité entre les clients après authentification

Référez-vous [en utilisant l'authentification de Multidomain](#) pour plus d'informations sur les instructions sur la façon dont configurer MDA.

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

Remarque: Seulement 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 commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

[Configurez le serveur de RAYON](#)

Le serveur de RAYON est configuré avec une adresse IP statique de 172.16.2.201/24. Terminez-vous ces étapes afin de configurer le serveur de RAYON pour un client d'AAA :

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

The screenshot displays the Cisco Systems Network Configuration interface. On the left, a sidebar contains various configuration options, with 'Network Configuration' highlighted. The main content area is titled 'Network Configuration' and features a 'Select' dropdown menu. Below this, there are two main sections: 'AAA Clients' and 'AAA Servers'. The 'AAA Clients' section is currently empty, showing a table with columns for 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. Below the table, there is an 'Add Entry' button and a 'Search' button. The 'AAA Servers' section shows a table with columns for 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type'. One server is listed: 'CCM-4' with IP address '172.16.2.201' and type 'CiscoSecure ACS'.

3. Configurez l'adresse Internet de client d'AAA, l'adresse IP, la clé secrète partagée et le type d'authentification en tant que :Adresse Internet de client d'AAA = nom de hôte du commutateur (Cat-3560).Adresse IP de client d'AAA = adresse IP d'interface de gestion du

commutateur (172.16.2.1). Secret partagé = RAYON clé configuré sur le commutateur (CisCo123). **Remarque:** Pour l'exécution correcte, la clé secrète partagée doit être identique sur le client d'AAA et l'ACS. Les clés distinguent les majuscules et minuscules. Authentifiez utilisant = RAYON (Cisco IOS/PIX 6.0). **Remarque:** L'attribut de paires de l'Attribut-valeur de Cisco (poids du commerce) est disponible sous cette option.

4. Cliquez sur Submit + appliquez afin d'apporter ces modifications efficaces, comme indiqué dans cet exemple

CISCO SYSTEMS Network Configuration

Add AAA Client

AAA Client Hostname: Cat-3560
 AAA Client IP Address: 172.16.2.1
 Shared Secret: CisCo123

RADIUS Key Wrap
 Key Encryption Key:
 Message Authenticator Code Key:
 Key Input Format: ASCII Hexadecimal

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Submit Submit + Apply Cancel

Group Setup

Référez-vous à cette table afin de configurer le serveur de RAYON pour l'authentification.

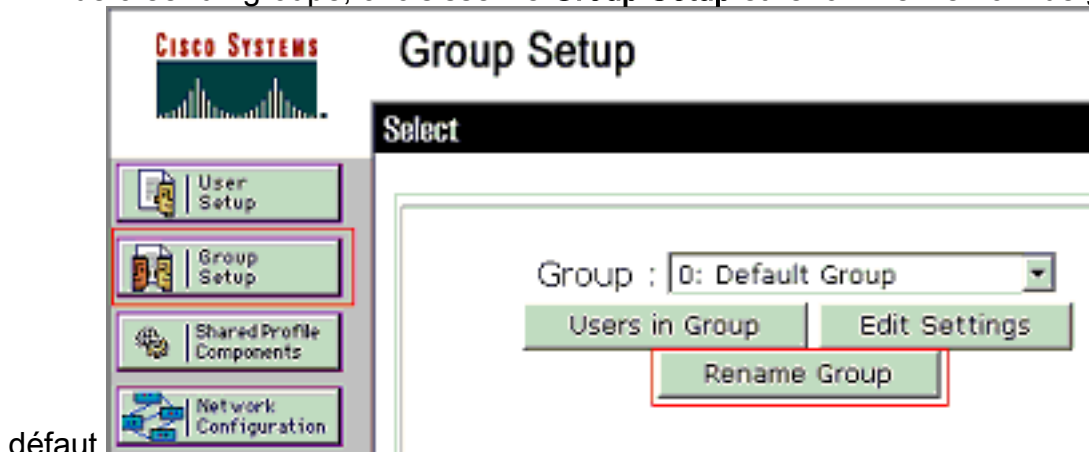
| Périphérique | Service | Groupe | Utilisateur | Mot de passe | VLAN | Pool DHCP |
|--------------|-------------------|-------------------|------------------|--------------|-------------------|-------------------|
| M-1 | Commercialisation | Commercialisation | mkt-gestionnaire | MMcis co | COMMERCIALISATION | Commercialisation |

| | | | | | | |
|-----|-------------------|-------------------|--------------------------|---------|-------------------|-------------------|
| M2 | Commercialisation | Commercialisation | mkt-personnel | MScisco | COMMERCIALISATION | Commercialisation |
| S-2 | Ventes | Ventes | directeur des ventes | SMcisco | VENTES | Ventes |
| S1 | Ventes | Ventes | personnel de vente | SScisco | VENTES | Ventes |
| P-1 | Commercialisation | Téléphones IP | CP-7970G-SEP001759E7492C | P1cisco | VOIX | Téléphones IP |
| P-2 | Ventes | Téléphones IP | CP-7961G-SEP001A2F80381F | P2cisco | VOIX | Téléphones IP |

Créez les groupes pour les clients qui se connectent à VLAN 3 (VOIX), 4 (VENTE) et 5 (des VENTES). Ici, des **Téléphones IP de groupes**, la **vente** et les **ventes** sont créés à cet effet.

Remarque: C'est la configuration des groupes de **vente** et de **Téléphones IP**. En **ventes** groupez la configuration, se terminent les étapes pour le **groupe marketing**.

1. Afin de créer un groupe, choisissez le **Group Setup** et renommez le nom de groupe par



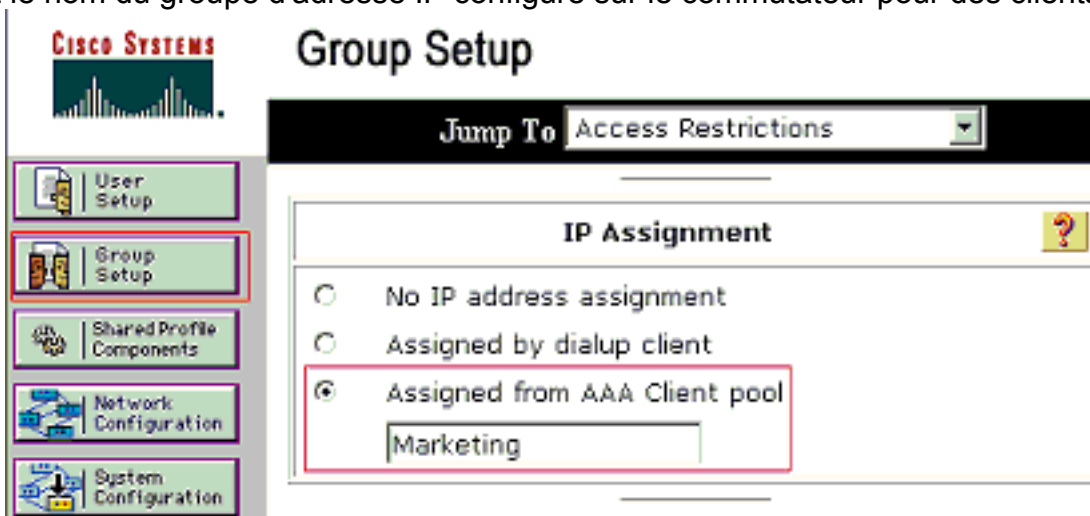
défaut.

2. Afin de configurer un groupe, choisissez le groupe de la liste et cliquez sur Edit les



configurations

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



groupe.

Remarq

ue: Choisissez cette option et introduisez le nom de client ip pool d'AAA dans la case, seulement si cet utilisateur doit faire assigner l'adresse IP par un groupe d'adresse IP configuré sur le client d'AAA. **Remarque:** Pour seule la configuration de groupe de **Téléphones IP**, ignorez l'étape suivante, étape 4, et passez à l'étape 5.

4. Définissez les attributs de l'Internet Engineering Task Force (IETF) **64**, **65** et **81** et puis cliquez sur Submit + **reprise**. Assurez-vous que les balises des valeurs sont placés à **1**, comme indiqué dans cet exemple. Le Catalyst ignore n'importe quelle balise autre que **1**. afin d'affecter un utilisateur à une particularité VLAN, vous devez également définir l'attribut **81** avec un *nom* VLAN ou le *nombre* VLAN qui correspondent. **Remarque:** Si vous utilisez le *nom* VLAN, il devrait être exactement même que celui configuré dans le



Group Setup

Jump To Access Restrictions

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Posture Validation

Network Access Profiles

Reports and Activity

Online Documentation

IETF RADIUS Attributes

[064] Tunnel-Type
Tag 1 Value VLAN

[065] Tunnel-Medium-Type
Tag 1 Value 802

[081] Tunnel-Private-Group-ID
Tag 1 Value MARKETING

Back to Help

Submit Submit + Restart Cancel

commutateur.

Re
marque: Référez-vous à [RFC 2868 : Attributs RADIUS pour le support de Protocol de tunnel](#) pour plus d'informations sur ces attributs IETF.
Remarque: En configuration initiale du serveur ACS, les attributs RADIUS IETF peuvent pour afficher dans l'installation utilisateur. Afin d'activer des attributs IETF dans des écrans de configuration utilisateur, choisissez la **configuration d'interface > le RAYON (IETF)**. Puis, le contrôle attribue **64**, **65**, et **81** dans les colonnes d'utilisateur et de groupe.
Remarque: Si vous ne définissez pas l'attribut **81** IETF et le port est un port de commutateur dans le mode d'accès, le client est assigné à l'accès VLAN du port. Si vous avez défini l'attribut **81** pour l'affectation dynamique VLAN et le port est un port de commutateur dans le mode d'accès, vous devez émettre la commande de **rayon de groupe par défaut d'aaa authorization network** sur le commutateur. Cette commande assigne le port au VLAN que le serveur de RAYON fournit. Autrement, le 802.1x déplace le port à l'état **AUTORISÉ** après authentification de l'utilisateur ; mais le port est toujours dans le par défaut VLAN du port, et la Connectivité peut échouer.
Remarque: L'étape suivante s'applique seulement au groupe de **Téléphones IP**.

5. Configurez le serveur de RAYON pour envoyer un attribut de paires de l'Attribut-valeur de Cisco (poids du commerce) pour autoriser un périphérique vocal. Sans ceci, le commutateur traite le périphérique vocal comme périphérique de données. Définissez l'attribut de paires de l'Attribut-valeur de Cisco (poids du commerce) avec une valeur de *device-traffic-class=voice* et cliquez sur **Submit +**

CISCO SYSTEMS

Group Setup

Jump To Access Restrictions

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Posture Validation

Network Access Profiles

Reports and Activity

Online Documentation

IP Assignment

No IP address assignment

Assigned by dialup client

Assigned from AAA Client pool

Cisco IOS/PIX 6.x RADIUS Attributes

[009\001] cisco-av-pair

[009\101] cisco-h323-credit-amount

[009\102] cisco-h323-credit-time

[009\103] cisco-h323-return-code

reprise.

[Installation utilisateur](#)

Terminez-vous ces étapes afin d'ajouter et configurer un utilisateur.

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



User Setup

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

User:

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

Add/l'éditez

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



User: mkt-manager (New User)

Account Disabled

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password *****
 Confirm Password *****

Separate (CHAP/MS-CHAP/ARAP)

Password *****
 Confirm Password *****

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Marketing

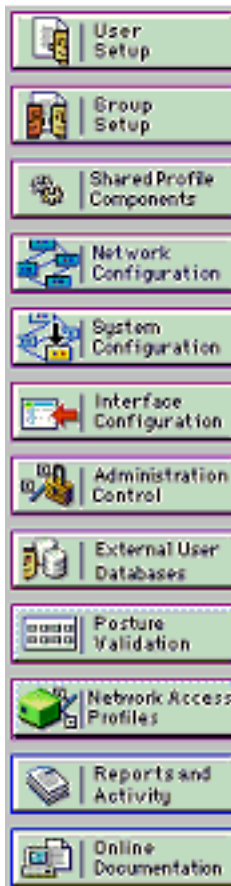
Callback

Use group setting

Submit Delete Cancel

l'utilisateur.

- Le téléphone IP utilise son ID de périphérique comme nom d'utilisateur et secret partagé comme mot de passe pour l'authentification. Ces valeurs devraient s'assortir sur le serveur de RAYON. Pour les Téléphones IP P-1 et P-2 créez les noms d'utilisateur mêmes que leur ID de périphérique et mot de passe mêmes que le secret partagé configuré. Voyez le [configurer les Téléphones IP pour utiliser la section d'authentification de 802.1x](#) pour plus d'informations sur l'ID de périphérique et le secret partagé sur un téléphone



User: CP-7961G-SEP001A2F80381F

Account Disabled

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password *****

Confirm Password *****

Separate (CHAP/MS-CHAP/ARAP)

Password *****

Confirm Password *****

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IP Phones

Submit

Delete

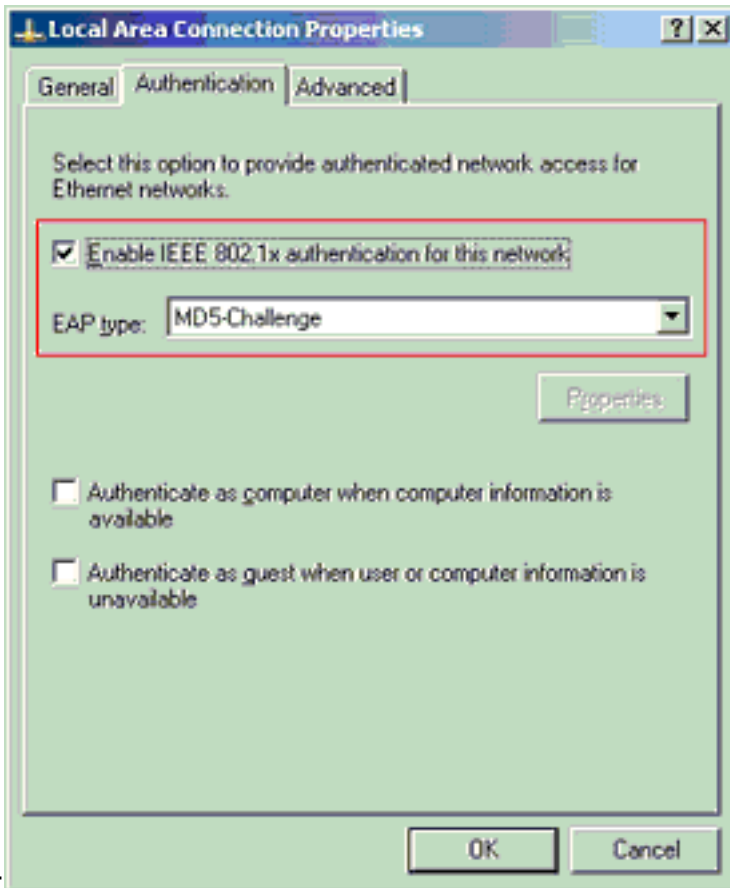
Cancel

IP.

[Configurez les clients PC pour utiliser l'authentification de 802.1x](#)

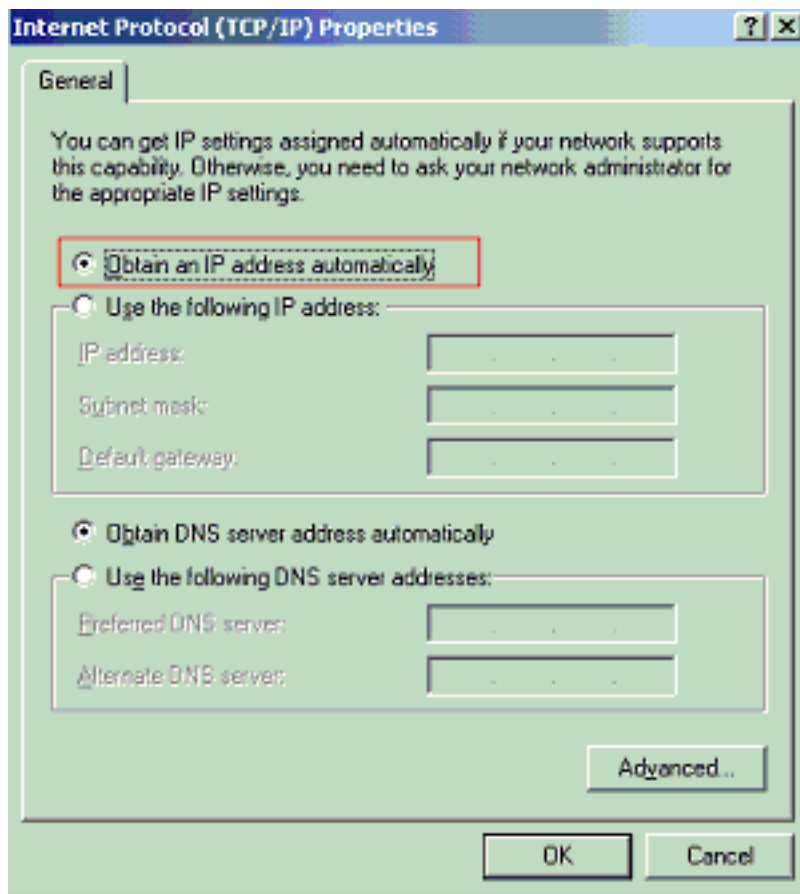
Cet exemple est spécifique au Protocole EAP (Extensible Authentication Protocol) de Microsoft Windows XP au-dessus du client du RÉSEAU LOCAL (EAPOL) :

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



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

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



automatically.

[Configurez les Téléphones IP pour utiliser l'authentification de 802.1x](#)

Terminez-vous ces étapes afin de configurer les Téléphones IP pour l'authentification de 802.1x.

1. Appuyez sur le bouton **Settings** afin d'accéder aux configurations d'**authentification de 802.1X** et choisir la configuration de sécurité > l'authentification de 802.1X > l'authentification de périphérique.
2. Placez l'option d'**authentification de périphérique** à activer.
3. Appuyez sur la touche **Save**.
4. Choisissez l'**authentification de 802.1X > l'EAP-MD5 > secret partagé** afin de placer un mot de passe au téléphone.
5. Écrivez le secret partagé et appuyez sur la **sauvegarde**. **Remarque:** Le mot de passe doit être entre six et 32 caractères, qui se composent de n'importe quelle combinaison des nombres ou des lettres. Que la clé n'est pas ici message actif est affiché et le mot de passe n'est pas enregistré si cette condition n'est pas satisfaite. **Remarque:** Si vous désactivez l'authentification de 802.1X ou exécutez une réinitialisation aux paramètres d'usine au téléphone, le secret partagé par MD5 précédemment configuré est supprimé. **Remarque:** Les autres options, ID de périphérique et royaume ne peuvent pas être configurés. L'ID de périphérique est utilisé comme nom d'utilisateur pour l'authentification de 802.1x. C'est un dérivé de la seule adresse MAC du téléphone du numéro de version et affichés dans ce format : CP-<model>-SEP-<MAC>. Par exemple, CP-7970G-SEP001759E7492C. Référez-vous au pour en savoir plus de [configurations d'authentification de 802.1X](#).

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

1. Appuyez sur le bouton **Settings** afin d'accéder aux configurations de **configuration réseau** et

choisir la **configuration réseau**.

2. Déverrouillez les options de **configuration réseau**. Afin de déverrouiller, appuyer sur **** #**. **Remarque:** N'appuyez sur pas **** #** afin de déverrouiller des options et puis les appuyer sur immédiatement **** #** de nouveau des options de verrouillage. Le téléphone interprète cet ordre comme **** # ****, qui remet à l'état initial le téléphone. Options de verrouillage après que vous les déverrouilliez, attente au moins 10 secondes avant que vous appuyez sur **** #** de nouveau.
3. Mettez en rouleau à Dhcp Enabled l'option et appuyez sur la touche douce d'**oui** afin d'activer le DHCP.
4. Appuyez sur la touche **Save**.

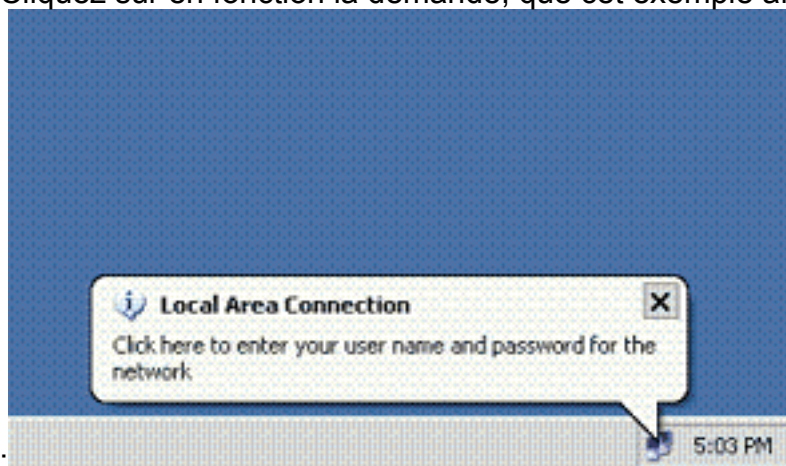
Vérifiez

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

Clients PC

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

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



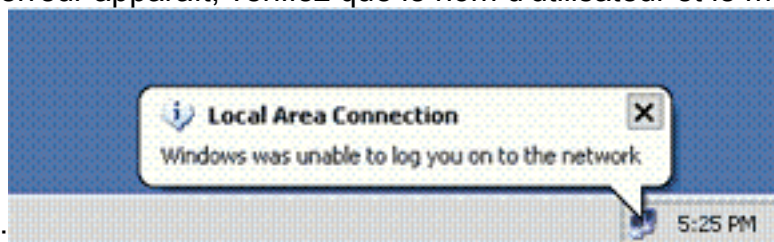
: Affichages de fenêtre d'entrée d'un nom d'utilisateur et de mot de passe. **Remarque:** MDA n'impose pas la commande de l'authentification de périphérique. Mais, pour les meilleurs résultats, Cisco recommande qu'un périphérique vocal soit authentifié avant un périphérique de données sur un port activé par MDA.

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



passee.

3. Si message d'erreur n'apparaît pas, vérifiez la Connectivité avec les méthodes habituelles, telles que l'accès traversant des ressources de réseau et avec le ping. **Remarque:** Si cette erreur apparaît, vérifiez que le nom d'utilisateur et le mot de passe sont corrects



Téléphones IP

le menu d'état d'authentification de 802.1X dans les Téléphones IP laisse surveiller l'état d'authentification.

1. Appuyez sur le bouton **Settings** afin d'accéder aux stats en temps réel d'authentification de 802.1X et choisir l'état d'authentification de configuration de sécurité > de 802.1X.
2. L'état de transaction devrait être authentifié. Référez-vous au pour en savoir plus [en temps réel d'état d'authentification de 802.1X](#). **Remarque:** L'état d'authentification peut également être vérifié des configurations > de l'état > des messages d'état.

Commutateur de la couche 3

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

1. Recherchez un état de port qui indique `AUTORISÉ.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 VLAN après l'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.

```

- 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`.

## Dépannez

### L'authentification de téléphone IP échoue

Affichages d'état de téléphone IP configurant l'IP ou s'enregistrant si l'authentification de 802.1x échoue. Terminez-vous ces étapes afin de dépanner ceci émet :

- Confirmez que le 802.1x est activé sur le téléphone IP.
- Vérifiez que vous avez l'ID de périphérique écrit sur le serveur d'authentification (RAYON) comme nom d'utilisateur.
- Confirmez que le secret partagé est configuré sur le téléphone IP.
- Si le secret partagé est configuré, vérifiez que vous avez la même chose secret partagé écrit sur le serveur d'authentification.
- Vérifiez que vous avez correctement configuré les autres périphériques priés, par exemple, le commutateur et le serveur d'authentification.

## Informations connexes

- [Configurer l'authentification basée sur port de 802.1x d'IEEE](#)
- [Configurez le téléphone IP pour utiliser l'authentification de 802.1x](#)
- [Instructions pour le déploiement du Cisco Secure ACS pour des serveurs de Windows Nt/2000 dans un environnement de commutateur Cisco Catalyst](#)
- [RFC 2868 : Attributs RADIUS pour le support de Protocol 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](#)