Esempio di configurazione dell'autenticazione multidominio IEEE 802.1x sugli switch a configurazione fissa Cisco Catalyst Layer 3

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Prodotti correlati](#)
[Convenzioni](#)
[Premesse](#)
[Configurazione](#)
[Esempio di rete](#)
[Configurazione dello switch Catalyst per l'autenticazione multidominio 802.1x](#)
[Configurazione del server RADIUS](#)
[Configurazione dei client PC per l'utilizzo dell'autenticazione 802.1x](#)
[Configurazione dei telefoni IP per l'autenticazione 802.1x](#)
[Verifica](#)
[Client PC](#)
[Telefoni IP](#)
[Switch Layer 3](#)
[Risoluzione dei problemi](#)
[Autenticazione telefono IP non riuscita](#)
[Informazioni correlate](#)

Introduzione

L'autenticazione multidominio consente a un telefono IP e a un PC di autenticarsi sulla stessa porta dello switch mentre li posiziona sulle VLAN voce e dati appropriate. Questo documento spiega come configurare IEEE 802.1x Multi-Domain Authentication (MDA) sugli switch Cisco Catalyst a configurazione fissa di layer 3.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Come funziona RADIUS?
- Guida allo switching Catalyst e alla distribuzione di ACS
- Guida per l'utente di Cisco Secure Access Control Server 4.1
- Panoramica di Cisco Unified IP Phone

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Cisco Catalyst serie 3560 con software Cisco IOS® versione 12.2(37)SE1**Nota: il** supporto dell'autenticazione multidominio è disponibile solo dal software Cisco IOS versione 12.2(35)SE e successive.
- In questo esempio viene utilizzato Cisco Secure Access Control Server (ACS) 4.1 come server RADIUS.**Nota:** prima di abilitare 802.1x sullo switch, è necessario specificare un server RADIUS.
- Client PC che supportano l'autenticazione 802.1x**Nota:** in questo esempio vengono utilizzati client Microsoft Windows XP.
- Cisco Unified 7970G IP Phone con firmware SCCP versione 8.2(1)
- Cisco Unified 7961G IP Phone con firmware SCCP versione 8.2(2)
- Media Convergence Server (MCS) con Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questa configurazione può essere utilizzata anche con i seguenti hardware:

- Cisco Catalyst serie 3560-E Switch
- Cisco Catalyst serie 3750 Switch
- Cisco Catalyst serie 3750-E Switch

Nota: gli switch Cisco Catalyst serie 3550 non supportano l'autenticazione multidominio 802.1x.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Lo standard IEEE 802.1x definisce un protocollo di autenticazione e controllo degli accessi basato su client-server che impedisce ai dispositivi non autorizzati di connettersi a una rete LAN tramite porte accessibili pubblicamente. 802.1x controlla l'accesso alla rete creando due punti di accesso virtuali distinti a ciascuna porta. Un punto di accesso è una porta non controllata; l'altra è una porta controllata. Tutto il traffico che attraversa la singola porta è disponibile per entrambi i punti di

accesso. La licenza 802.1x autentica ciascun dispositivo utente collegato a una porta dello switch e assegna la porta a una VLAN prima di rendere disponibili i servizi offerti dallo switch o dalla LAN. Finché il dispositivo non viene autenticato, il controllo degli accessi 802.1x consente solo il traffico EAPOL (Extensible Authentication Protocol over LAN) attraverso la porta a cui è connesso il dispositivo. Dopo l'autenticazione, il traffico normale può passare attraverso la porta.

802.1x è costituito da tre componenti principali. Ognuna di esse viene definita entità di accesso alla porta (PAE, Port Access Entity).

- Supplicant: dispositivo client che richiede accesso alla rete, ad esempio telefoni IP e PC collegati
- Autenticatore: dispositivo di rete che agevola le richieste di autorizzazione del richiedente, ad esempio Cisco Catalyst 3560.
- Server di autenticazione: server RADIUS (Remote Authentication Dial-in User Server) che fornisce il servizio di autenticazione, ad esempio Cisco Secure Access Control Server

I telefoni IP unificati Cisco contengono anche un supplicant 802.1X. Questo supplicant consente agli amministratori di rete di controllare la connettività dei telefoni IP alle porte dello switch LAN. La versione iniziale del supplicant 802.1X per telefoni IP implementa l'opzione EAP-MD5 per l'autenticazione 802.1X. In una configurazione multidominio, il telefono IP e il PC collegato devono richiedere in modo indipendente l'accesso alla rete specificando un nome utente e una password. Il dispositivo Authenticator può richiedere informazioni da RADIUS denominate attributi. Gli attributi specificano informazioni di autorizzazione aggiuntive, ad esempio se per un richiedente è consentito l'accesso a una VLAN specifica. Questi attributi possono essere specifici del fornitore. Cisco utilizza l'attributo RADIUS `cisco-av-pair` per comunicare all'autenticatore (Cisco Catalyst 3560) che un supplicant (IP Phone) è autorizzato sulla VLAN voce.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare la funzionalità di autenticazione multidominio 802.1x descritta in questo documento.

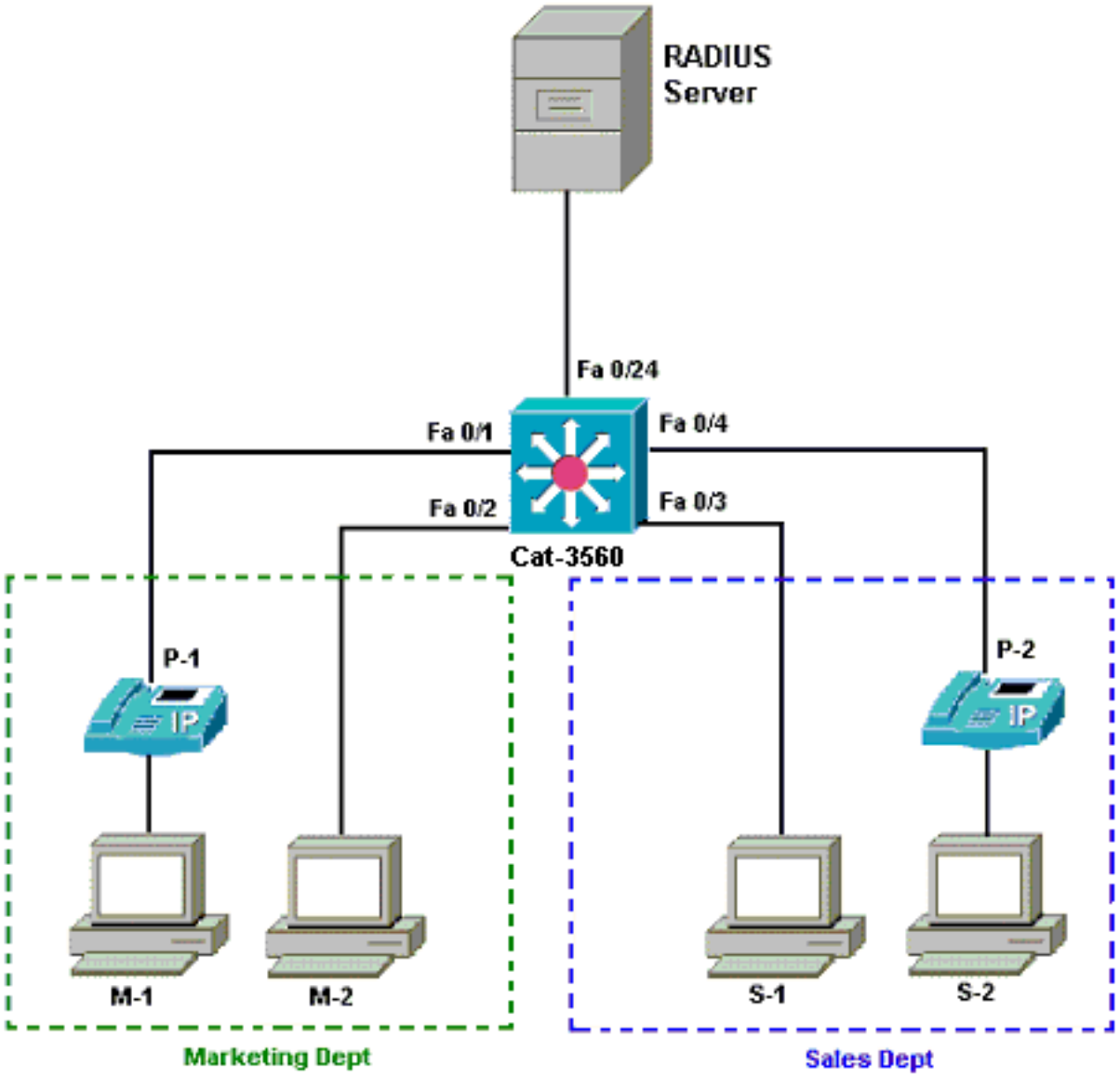
Questa configurazione richiede i seguenti passaggi:

- Configurare lo switch Catalyst per l'autenticazione multidominio 802.1x.
- Configurare il server RADIUS.
- Configurare i client PC per l'utilizzo dell'autenticazione 802.1x.
- Configurare i telefoni IP per l'utilizzo dell'autenticazione 802.1x.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



- Server RADIUS: esegue l'autenticazione effettiva del client. Il server RADIUS convalida l'identità del client e notifica allo switch se il client è autorizzato o meno ad accedere ai servizi LAN e dello switch. Qui, il Cisco ACS viene installato e configurato su un Media Convergence Server (MCS) per l'autenticazione e l'assegnazione della VLAN. MCS è anche il server TFTP e Cisco Unified Communications Manager (Cisco CallManager) per i telefoni IP.
- Switch - Controlla l'accesso fisico alla rete in base allo stato di autenticazione del client. Lo switch funge da intermediario (proxy) tra il client e il server RADIUS. Richiede informazioni sull'identità al client, verifica tali informazioni con il server RADIUS e invia una risposta al client. In questo caso, lo switch Catalyst 3560 è configurato anche come server DHCP. Il supporto dell'autenticazione 802.1x per il protocollo DHCP (Dynamic Host Configuration Protocol) consente al server DHCP di assegnare gli indirizzi IP alle diverse classi di utenti finali. A tale scopo, aggiunge l'identità dell'utente autenticato nel processo di rilevamento DHCP. Le porte Fast Ethernet 0/1 e 0/4 sono le uniche porte configurate per l'autenticazione multidominio 802.1x. Le porte Fast Ethernet 0/2 e 0/3 sono in modalità host singolo predefinita 802.1x. La porta FastEthernet 0/24 si connette al server RADIUS.**Nota:** se si usa un server DHCP esterno, non dimenticare di aggiungere il comando **ip helper-address** sull'interfaccia SVI (vlan), dove risiede il client, che punta al server DHCP.
- Client: dispositivi, ad esempio telefoni IP o workstation, che richiedono l'accesso ai servizi LAN e switch e rispondono alle richieste dello switch. In questo caso, i client sono configurati

in modo da ottenere l'indirizzo IP da un server DHCP. I dispositivi M-1, M-2, S-1 e S-2 sono i client workstation che richiedono l'accesso alla rete. P-1 e P-2 sono i client IP Phone che richiedono l'accesso alla rete. M-1, M-2 e P-1 sono dispositivi client nel reparto marketing. S-1, S-2 e P-2 sono dispositivi client nel reparto vendite. I telefoni IP P-1 e P-2 sono configurati per essere nella stessa VLAN voce (VLAN 3). Le workstation M-1 e M-2 sono configurate in modo da trovarsi nella stessa VLAN dati (VLAN 4) dopo un'autenticazione riuscita. Anche le workstation S-1 e S-2 sono configurate in modo da trovarsi nella stessa VLAN dati (VLAN 5) dopo un'autenticazione riuscita.**Nota:** è possibile utilizzare l'assegnazione dinamica di VLAN da un server RADIUS solo per i dispositivi dati.

Configurazione dello switch Catalyst per l'autenticazione multidominio 802.1x

La configurazione di esempio dello switch include:

- Come abilitare l'autenticazione multidominio 802.1x sulle porte dello switch
- Configurazione correlata al server RADIUS
- Configurazione del server DHCP per l'assegnazione dell'indirizzo IP
- Connettività tra i client del routing tra VLAN dopo l'autenticazione

Per ulteriori informazioni sulle linee guida per la configurazione dell'MDA, consultare il documento sull'uso dell'autenticazione multidominio.

Nota: verificare che il server RADIUS si connetta sempre dietro una porta autorizzata.

Nota: qui viene mostrata solo la configurazione pertinente.

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
```

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

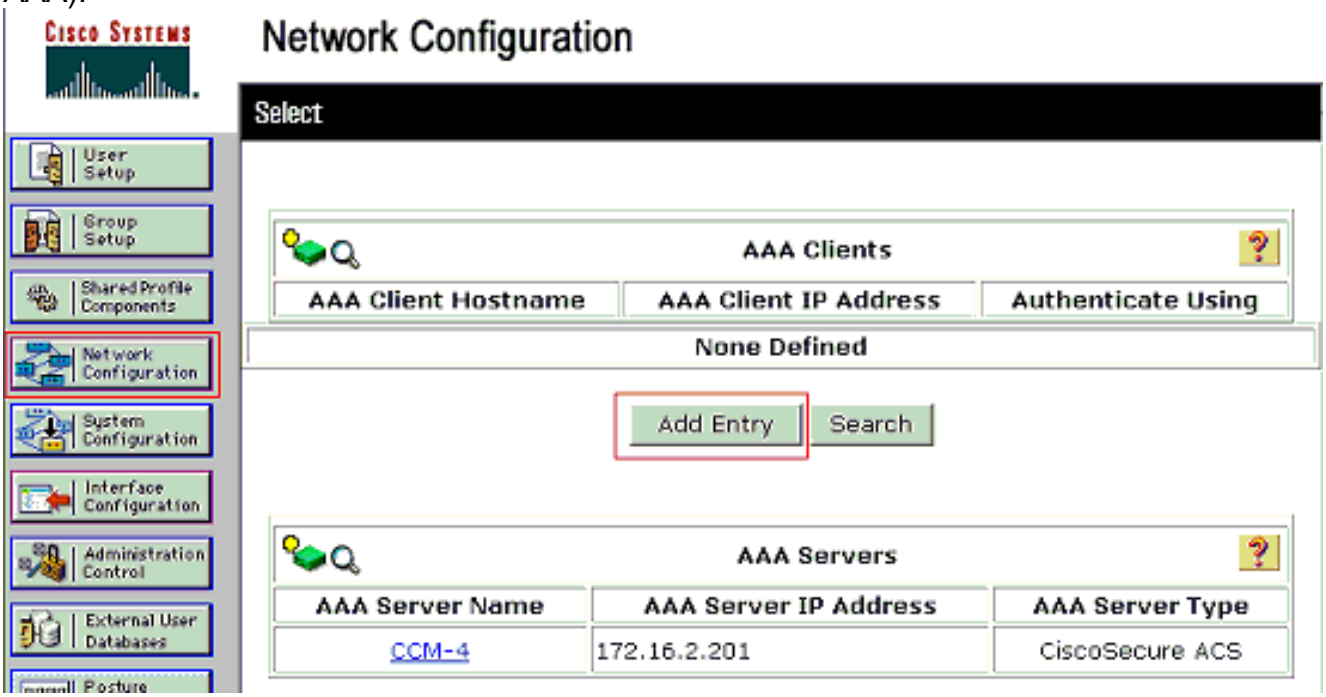
Configurazione del server RADIUS

Il server RADIUS è configurato con un indirizzo IP statico di 172.16.2.201/24. Per configurare il server RADIUS per un client AAA, attenersi alla seguente procedura:

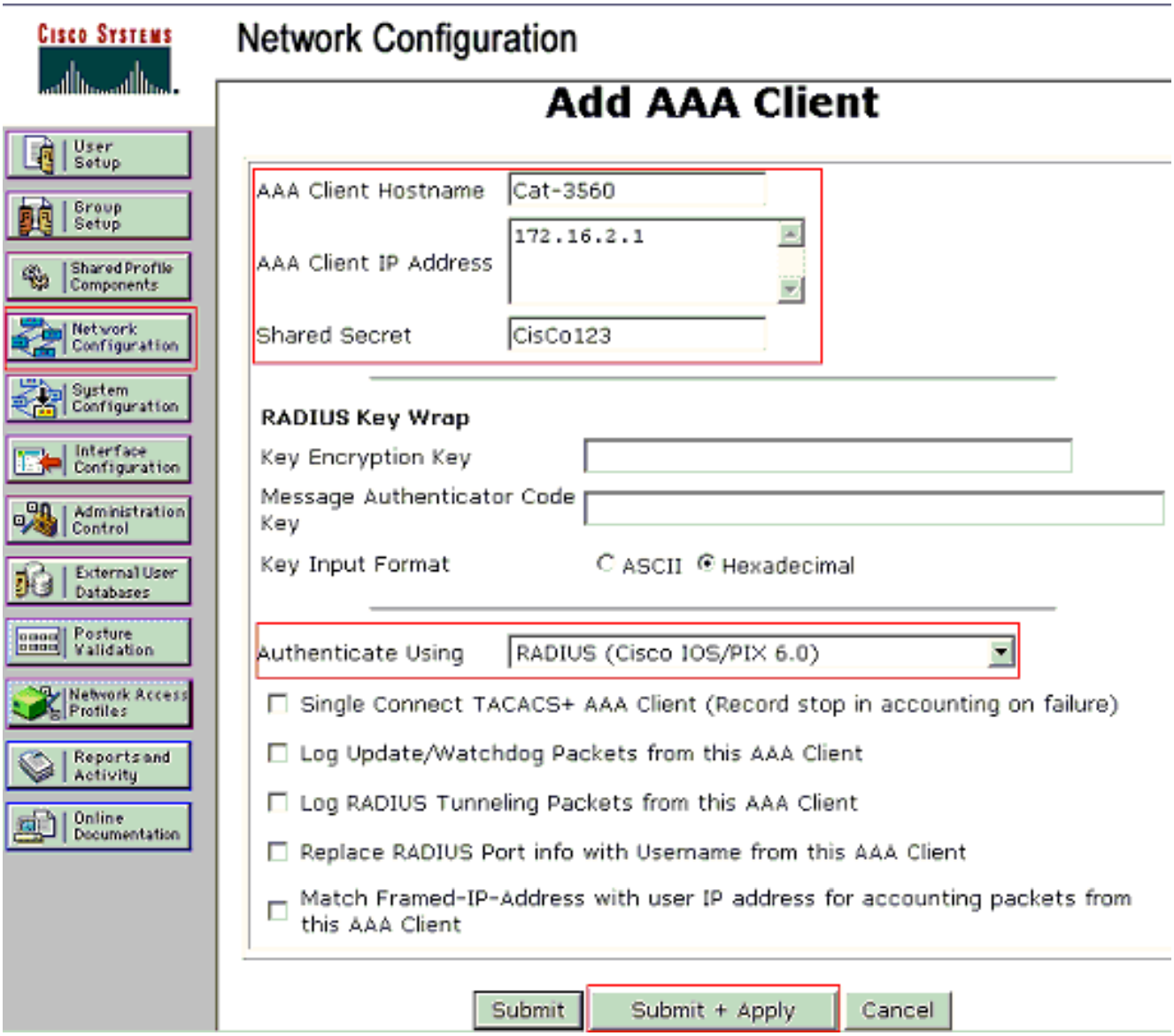
1. Per configurare un client AAA, fare clic su **Configurazione di rete** nella finestra di

amministrazione di ACS.

2. Fare clic su **Add Entry** (Aggiungi voce) nella sezione AAA Client (Client AAA).



3. Configurare il nome host del client AAA, l'indirizzo IP, la chiave segreta condivisa e il tipo di autenticazione come:Nome host client AAA = Nome host switch (**Cat-3560**).Indirizzo IP client AAA = Indirizzo IP dell'interfaccia di gestione dello switch (**172.16.2.1**).Shared Secret = Chiave RADIUS configurata sullo switch (**CisCo123**).**Nota:** per un corretto funzionamento, la chiave privata condivisa deve essere identica sul client AAA e su ACS. Le chiavi distinguono tra maiuscole e minuscole.Autenticazione tramite = **RADIUS (Cisco IOS/PIX 6.0)**.**Nota:** in questa opzione è disponibile l'attributo di coppia Cisco Attribute-Value (AV).
4. Per rendere effettive le modifiche, fare clic su **Submit + Apply** (Invia + Applica), come mostrato
nell'esempio:



Impostazione gruppo

Per configurare il server RADIUS per l'autenticazione, fare riferimento a questa tabella.

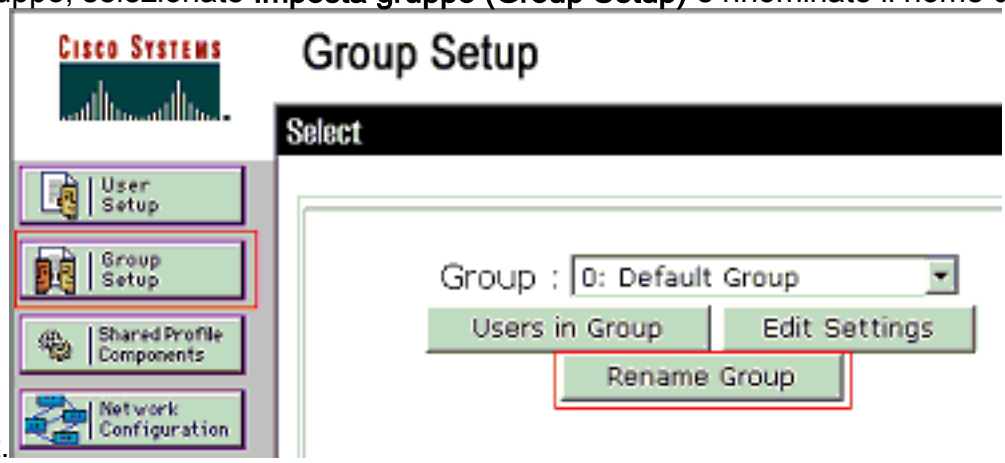
Sul dispositivo bootflash o slot0:	Reparto	Group	Utente	Password	VLAN	Pool DHCP
M-1	Marketing	Marketing	responsabile del marketing	Cisco	MARKETING	Marketing
M-2	Marketing	Marketing	personale di mercato	MScisco	MARKETING	Marketing
S-2	Vendit	Vendit	respon	SMcisc	VENDI	Ven

	e	e	sabile vendite	o	TE	dite
S-1	Vendite	Vendite	addetto alle vendite	Cisco	VENDITE	Vendite
P-1	Marketing	Telefoni IP	CP-7970G-SEP001759E7492C	P1cisco	VOCE	IP-Phone
P-2	Vendite	Telefoni IP	CP-7961G-SEP001A2F80381F	P2cisco	VOCE	IP-Phone

Creare gruppi per i client che si connettono alle VLAN 3 (VOICE), 4 (MARKETING) e 5 (SALES). In questo caso, vengono creati i gruppi **IP Phone**, **Marketing** e **Sales**.

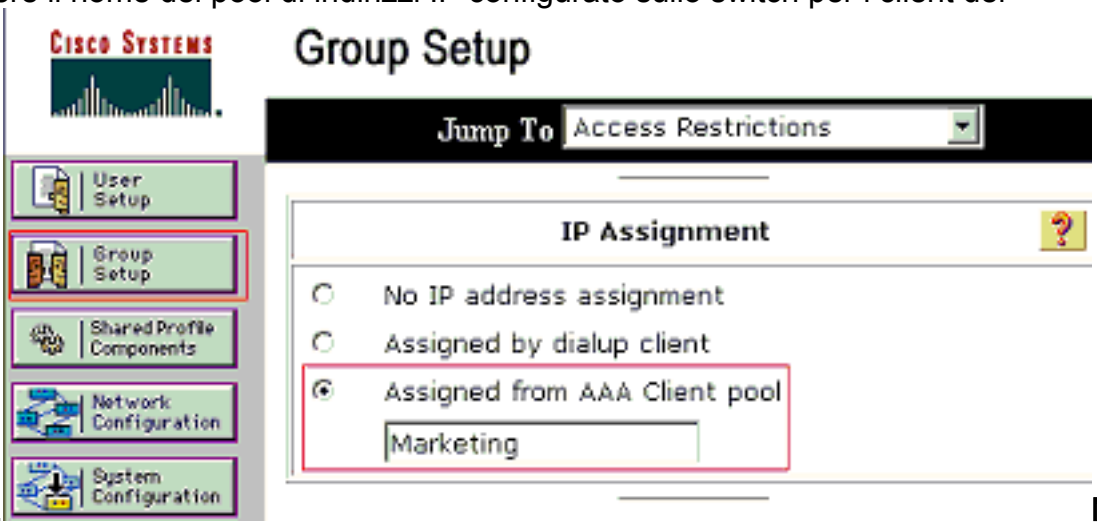
Nota: questa è la configurazione dei gruppi **Marketing** e **Telefoni IP**. Per la configurazione del gruppo **Vendite**, completare i passaggi per il gruppo **Marketing**.

1. Per creare un gruppo, selezionate **Imposta gruppo (Group Setup)** e rinominate il nome del gruppo di default.



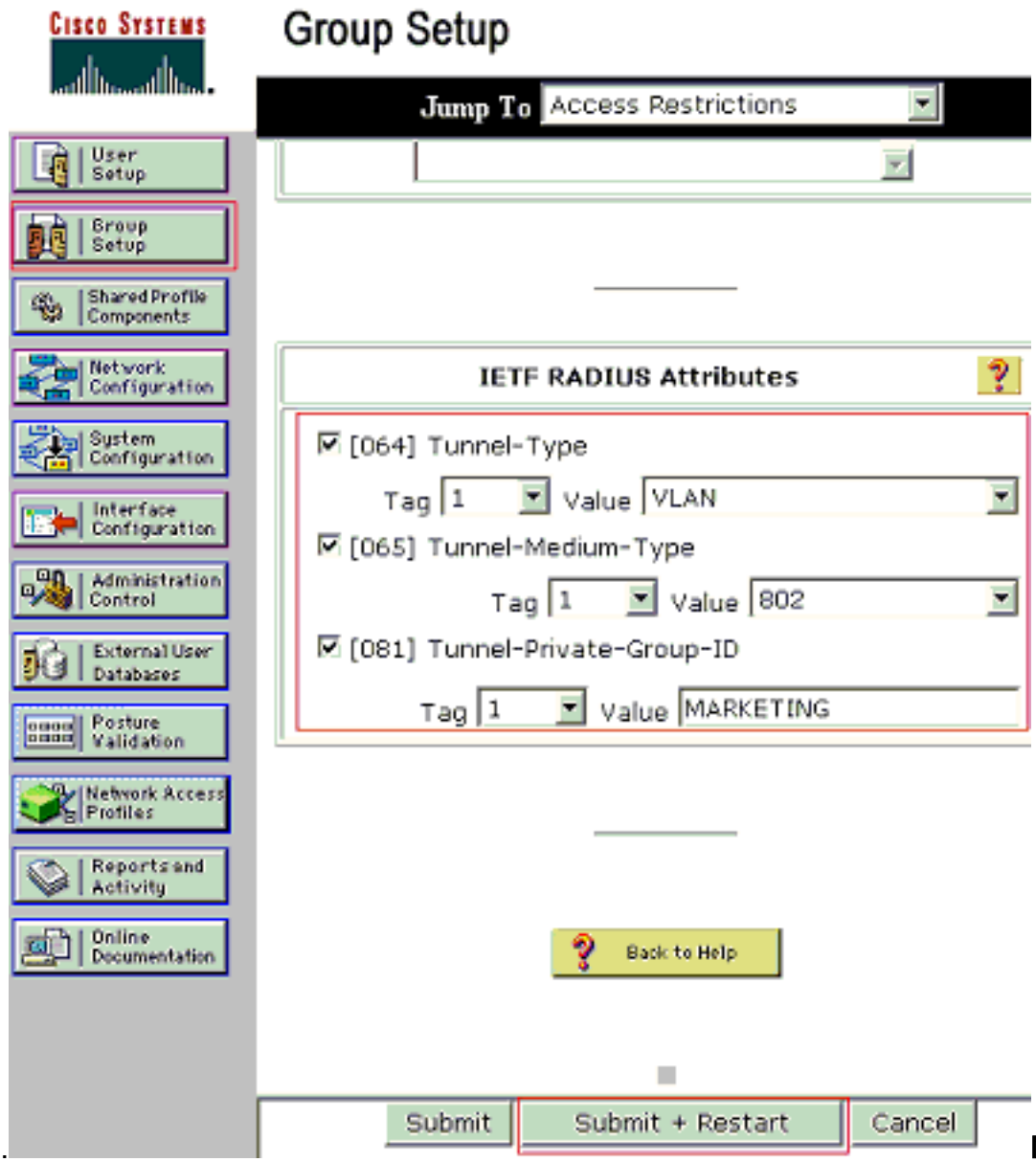
2. Per configurare un gruppo, selezionarlo dall'elenco e fare clic su **Modifica impostazioni**

3. Definire l'assegnazione dell'indirizzo IP del client come **assegnato dal pool di client AAA**.

Immettere il nome del pool di indirizzi IP configurato sullo switch per i client del gruppo. 

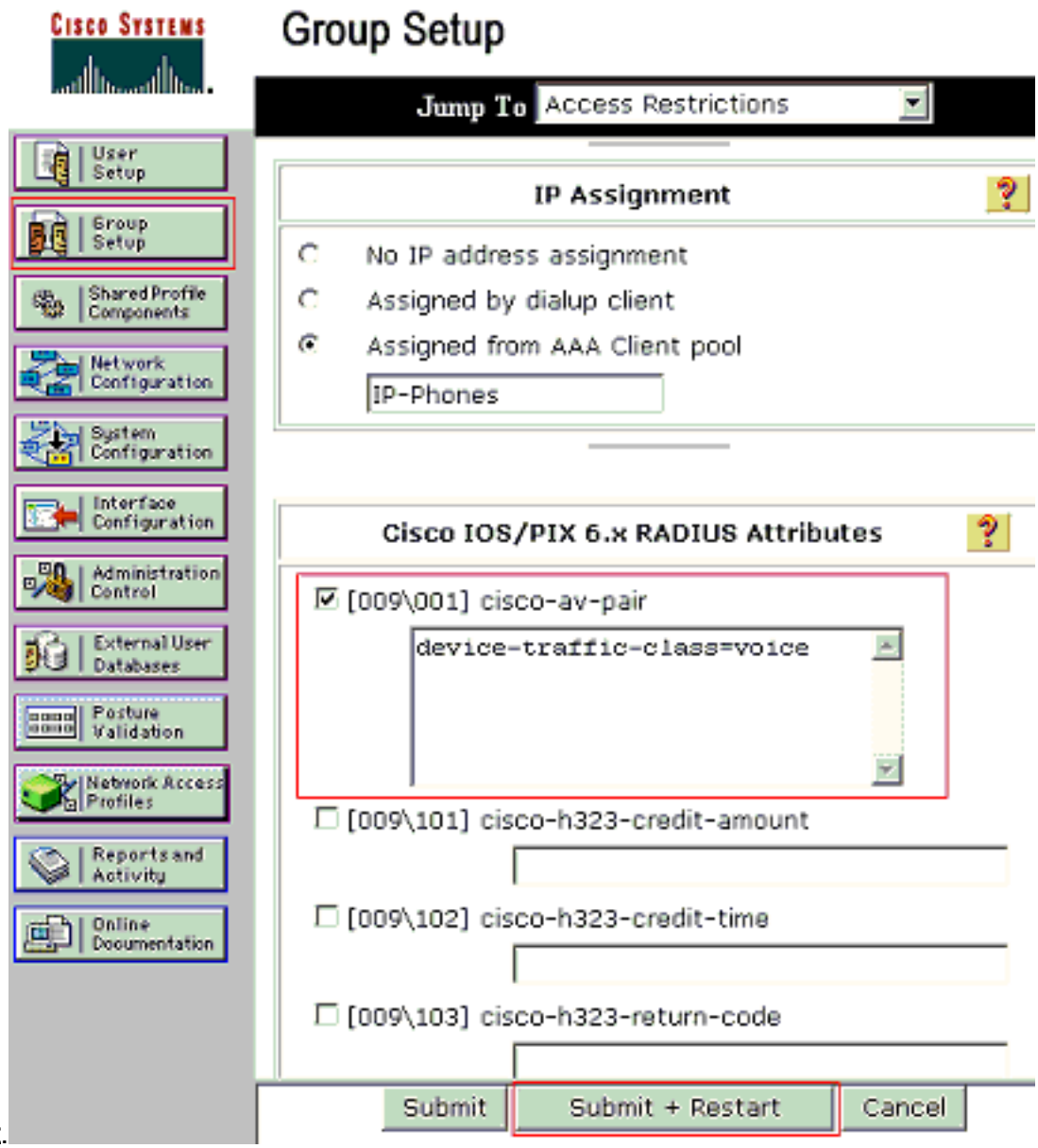
Nota: selezionare questa opzione e digitare il nome del pool IP del client AAA nella casella, solo se l'indirizzo IP deve essere assegnato da un pool di indirizzi IP configurato sul client AAA.**Nota:** per la sola configurazione del gruppo **IP Phone**, saltare il passaggio successivo, il passaggio 4, e andare al passaggio 5.

4. Definire gli attributi **64**, **65** e **81 di** Internet Engineering Task Force (IETF) e fare clic su **Invia + Riavvia**.Assicurarsi che le etichette dei valori siano impostate su **1**, come illustrato nell'esempio. Catalyst ignora i tag diversi da 1. Per assegnare un utente a una VLAN specifica, è necessario definire anche l'attributo **81** con un *nome di* VLAN o un *numero di* VLAN corrispondente.**Nota:** se si usa il *nome* VLAN, deve essere esattamente lo stesso di quello configurato nello



switch. **Nota:** Per ulteriori informazioni, fare riferimento alla RFC 2868: per ulteriori informazioni sugli attributi IETF, consultare la sezione Attributi RADIUS per il supporto del protocollo tunnel.**Nota:** nella configurazione iniziale del server ACS, gli attributi RADIUS IETF potrebbero non essere visualizzati in **Impostazione utente**. Per abilitare gli attributi IETF nelle schermate di configurazione utente, scegliere **Configurazione interfaccia > RADIUS (IETF)**. Verificare quindi gli attributi **64**, **65** e **81** nelle colonne Utente e Gruppo.**Nota:** se non si definisce l'attributo IETF **81** e la porta è una porta dello switch in modalità di accesso, il client viene assegnato alla VLAN di accesso della porta. Se è stato definito l'attributo **81** per l'assegnazione dinamica della VLAN e la porta è una porta dello switch in modalità di accesso, è necessario usare il comando **aaa authorization network default group radius** sullo switch. Con questo comando la porta viene assegnata alla VLAN fornita dal server RADIUS. In caso contrario, 802.1x sposta la porta allo stato AUTORIZZATO dopo l'autenticazione dell'utente; tuttavia, la porta si trova ancora nella VLAN predefinita e la connettività potrebbe non riuscire.**Nota: il** passaggio successivo è applicabile solo al gruppo **Telefoni IP**.

5. Configurare il server RADIUS in modo che invii un attributo di coppia Cisco Attribute-Value (AV) per autorizzare un dispositivo voce. In caso contrario, lo switch considera il dispositivo voce come un dispositivo dati. Definire l'attributo della coppia Cisco Attribute-Value (AV) con il valore *device-traffic-class=voice* e fare clic su **Submit +**

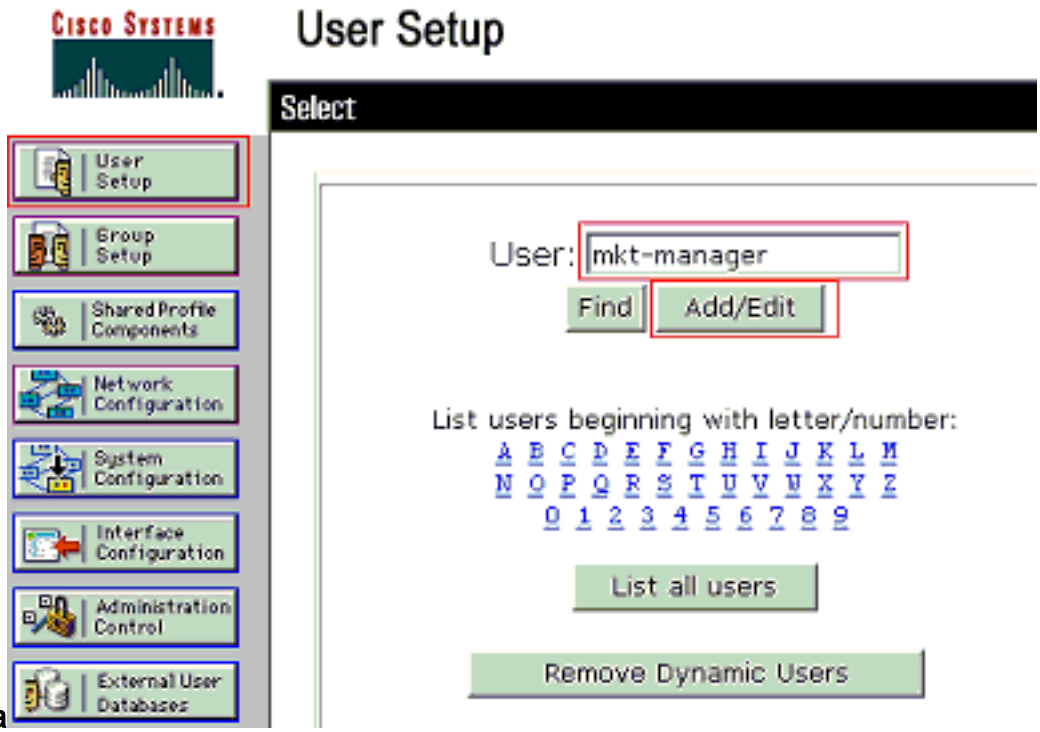


Restart.

Impostazione utente

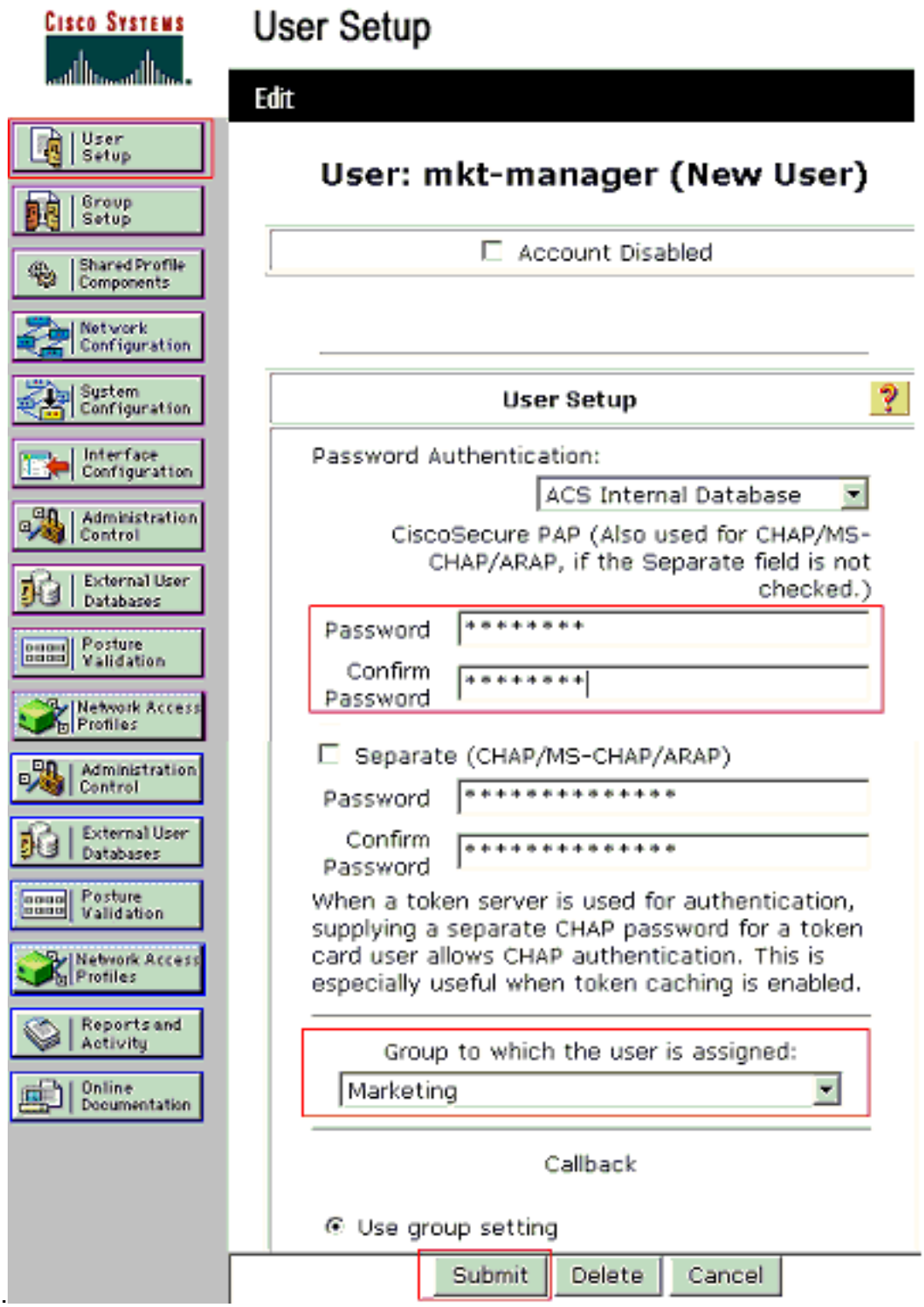
Completare questa procedura per aggiungere e configurare un utente.

1. Per aggiungere e configurare gli utenti, scegliere **Configurazione utente**. Immettere il nome utente e fare clic su



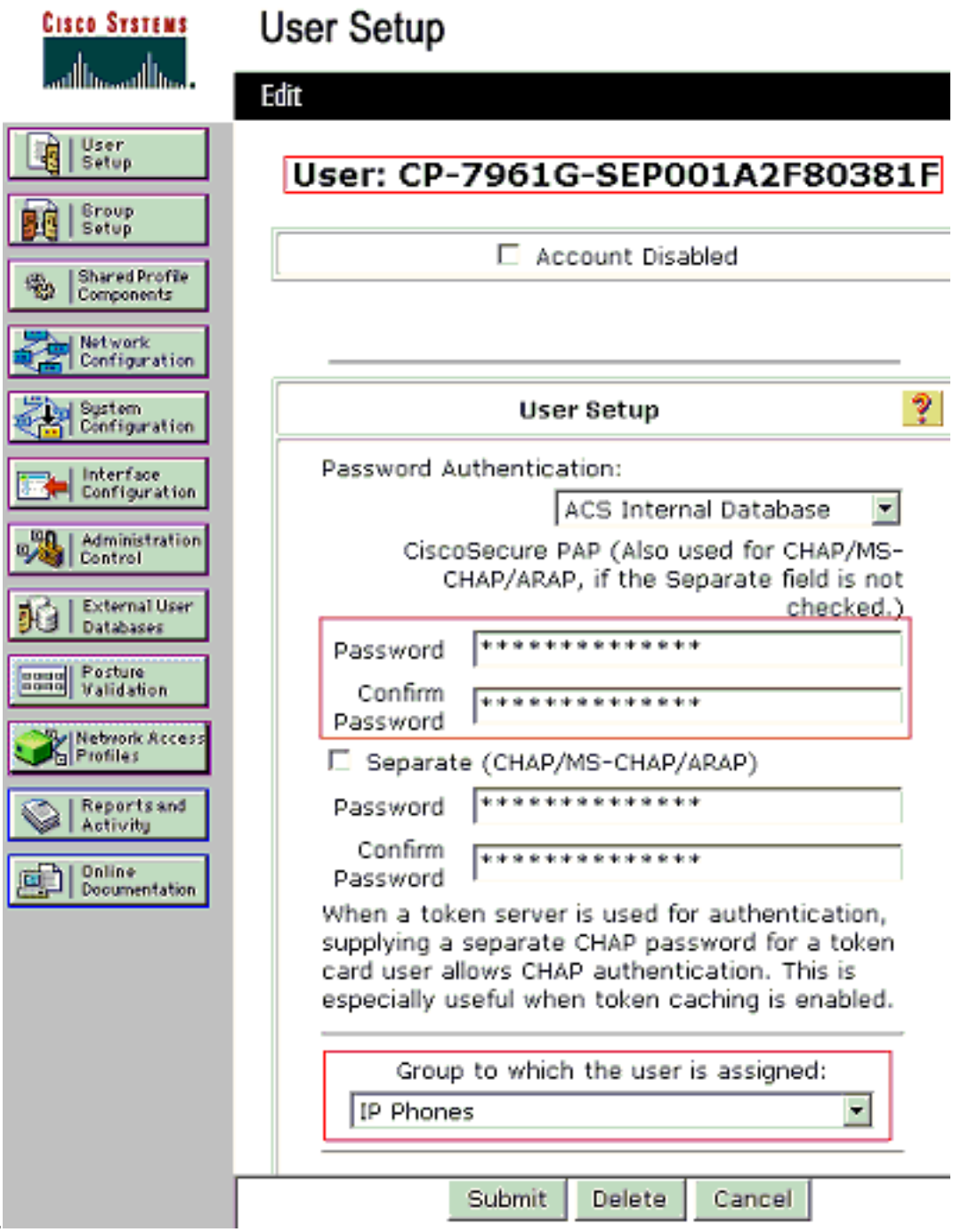
Aggiungi/Modifica

2. Definire il nome utente, la password e il gruppo per



l'utente.

3. IP Phone utilizza il proprio ID dispositivo come nome utente e il segreto condiviso come password per l'autenticazione. Questi valori devono corrispondere sul server RADIUS. Per i telefoni IP P-1 e P-2 creare nomi utente identici all'ID e alla password del dispositivo, come il segreto condiviso configurato. Per ulteriori informazioni sull'ID dispositivo e sul segreto condiviso di un telefono IP, vedere la sezione Configurazione dei telefoni IP per l'autenticazione



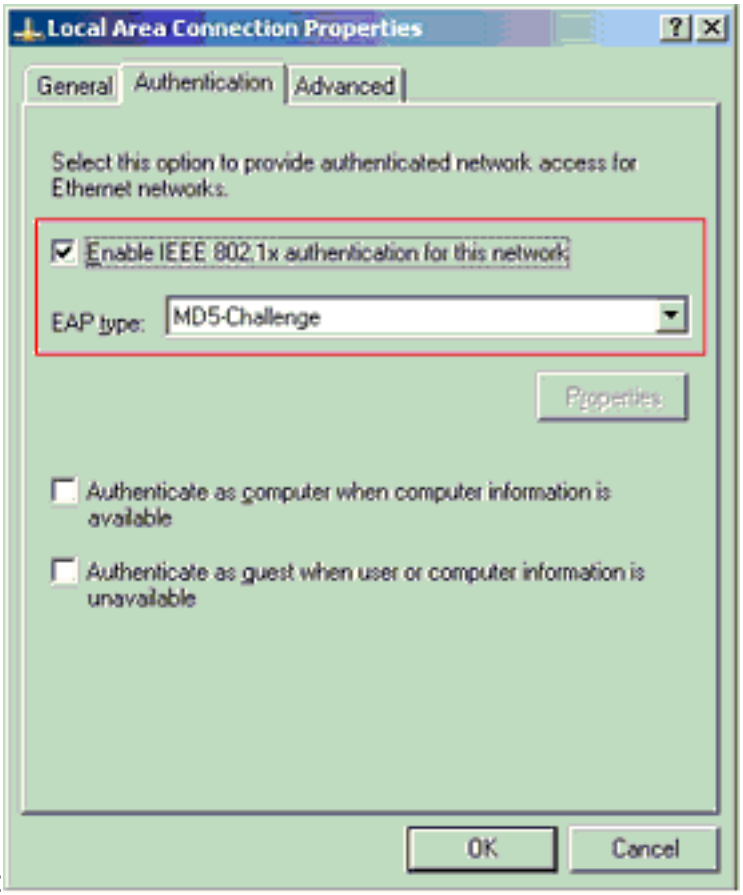
802.1x.

Configurazione dei client PC per l'utilizzo dell'autenticazione 802.1x

Questo esempio è specifico del client Microsoft Windows XP Extensible Authentication Protocol (EAP) over LAN (EAPOL):

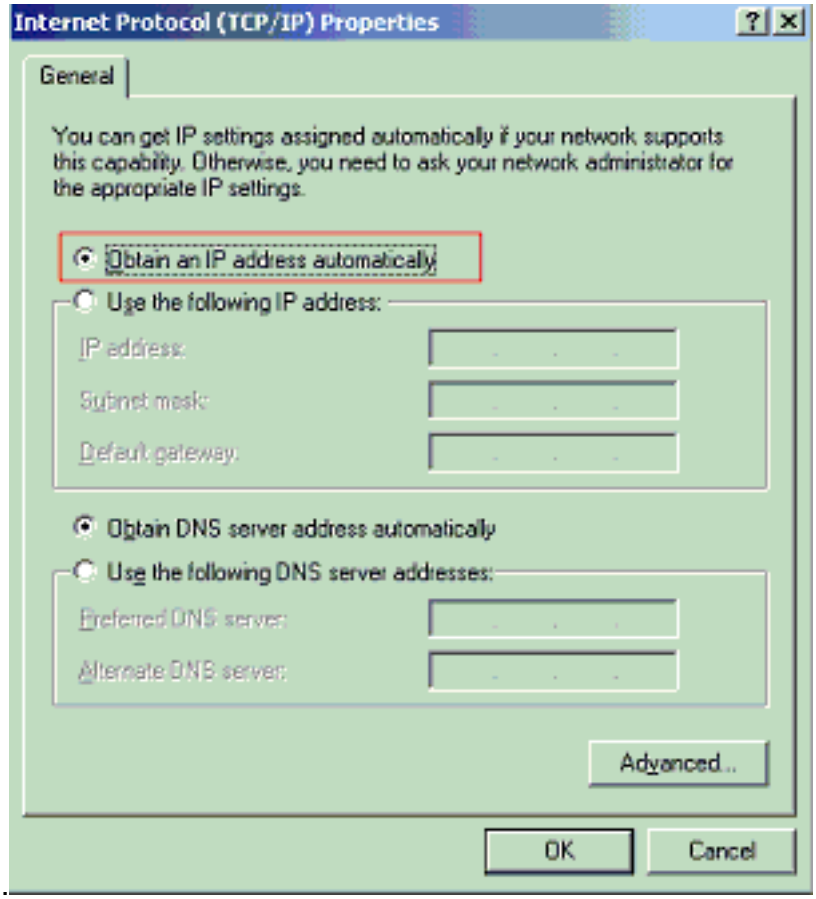
1. Scegliere **Start > Pannello di controllo > Connessioni di rete**, fare clic con il pulsante destro del mouse su **Connessione alla rete locale** e scegliere **Proprietà**.
2. Selezionare **Mostra icona nell'area di notifica quando si è connessi** nella scheda Generale.
3. Nella scheda Autenticazione selezionare **Attiva autenticazione IEEE 802.1x per la rete**.
4. Impostare il tipo EAP su **MD5-Challenge**, come mostrato

nell'esempio:



Completare questa procedura per configurare i client in modo che ottengano l'indirizzo IP da un server DHCP.

1. Scegliere **Start > Pannello di controllo > Connessioni di rete**, fare clic con il pulsante destro del mouse su **Connessione alla rete locale** e scegliere **Proprietà**.
2. Nella scheda Generale fare clic su **Protocollo Internet (TCP/IP)** e quindi su **Proprietà**.
3. Scegliere **Ottieni automaticamente un indirizzo**

IP. 

Configurazione dei telefoni IP per l'autenticazione 802.1x

Completare questa procedura per configurare i telefoni IP per l'autenticazione 802.1x.

1. Premere il pulsante **Settings** (Impostazioni) per accedere alle impostazioni di **autenticazione 802.1X** e scegliere **Security Configuration (Configurazione protezione) > 802.1X Authentication (Autenticazione 802.1X) > Device Authentication (Autenticazione dispositivo)**.
2. Impostare l'opzione **Device Authentication** su **Enabled**.
3. Premere il tasto softkey **Save**.
4. Scegliere **Autenticazione 802.1X > EAP-MD5 > Segreto condiviso** per impostare una password sul telefono.
5. Immettere il segreto condiviso e scegliere **Salva**.**Nota:** la password deve contenere da sei a 32 caratteri, costituiti da qualsiasi combinazione di numeri o lettere. `La chiave non è attiva.` Se questa condizione non viene soddisfatta, viene visualizzato un messaggio e la password non viene salvata.**Nota:** se si disabilita l'autenticazione 802.1X o si esegue un ripristino del telefono, il segreto condiviso MD5 precedentemente configurato viene eliminato.**Nota:** non è possibile configurare le altre opzioni ID dispositivo e Realm. L'ID dispositivo viene utilizzato come nome utente per l'autenticazione 802.1x. Questo è un derivato del numero di modello del telefono e dell'indirizzo MAC univoco visualizzato in questo formato: CP-<modello>-SEP-<MAC>. Ad esempio, **CP-7970G-SEP001759E7492C**. per ulteriori informazioni, fare riferimento a Impostazioni autenticazione 802.1X.

Completare la procedura descritta di seguito per configurare il telefono IP in modo da ottenere l'indirizzo IP da un server DHCP.

1. Premere il pulsante **Settings** (Impostazioni) per accedere alle impostazioni **Network Configuration** (Configurazione di rete) e scegliere **Network Configuration** (Configurazione di

rete).

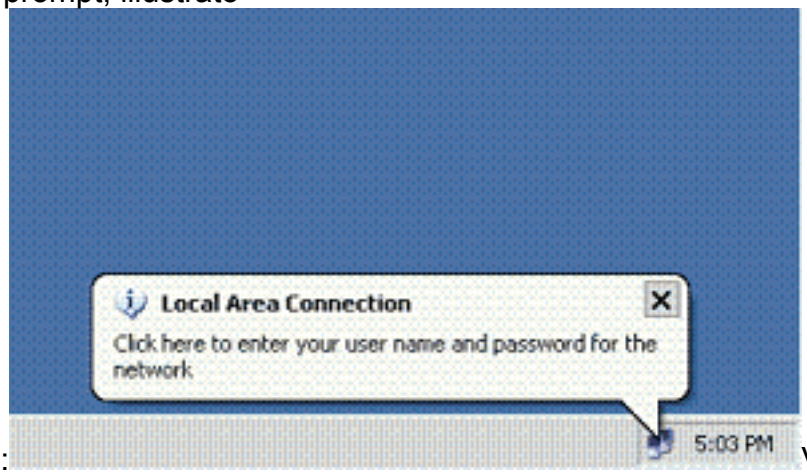
2. Sbloccare le opzioni **di Configurazione rete**. Per sbloccare, premere **#.**Nota:** Non premere **# per sbloccare le opzioni, quindi premere **# nuovamente per bloccarle. Il telefono interpreta questa sequenza come **#**, che ripristina il telefono. Per bloccare le opzioni dopo averle sbloccate, attendere almeno 10 secondi prima di premere di nuovo **#.
3. Scorrere l'opzione DHCP Enabled (DHCP abilitato) e premere il tasto softkey **Yes** per abilitare il protocollo DHCP.
4. Premere il tasto softkey **Save**.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

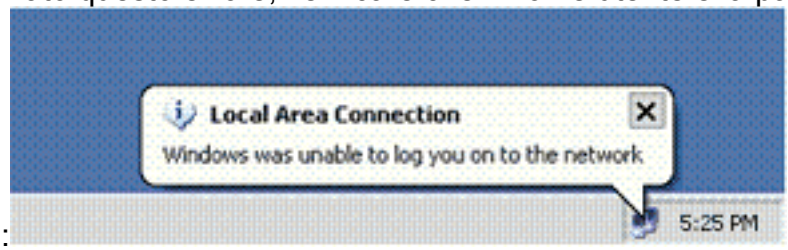
Client PC

Se la configurazione è stata completata correttamente, i client del PC visualizzeranno una richiesta di immissione di un nome utente e di una password.

1. Fare clic sul prompt, illustrato nell'esempio: 

Viene visualizzata una finestra per l'immissione del nome utente e della password.**Nota:** MDA non applica l'ordine di autenticazione del dispositivo. Tuttavia, per risultati ottimali, Cisco consiglia di autenticare un dispositivo voce prima di un dispositivo dati su una porta abilitata per MDA.

2. Immettere il nome utente e la password. 

3. Se non viene visualizzato alcun messaggio di errore, verificare la connettività con i metodi tradizionali, ad esempio tramite l'accesso alle risorse di rete e con **ping**.**Nota:** se viene visualizzato questo errore, verificare che il nome utente e la password siano corretti: 

Telefoni IP

Il menu dello stato di autenticazione 802.1X nei telefoni IP consente di monitorare lo stato di autenticazione.

1. Premere il pulsante **Settings** (Impostazioni) per accedere agli stati in tempo reale dell'autenticazione 802.1X e scegliere **Security Configuration (Configurazione sicurezza) > 802.1X Authentication Status** (Stato autenticazione 802.1X).
2. **Lo stato** della **transazione** deve essere **Autenticato**. per ulteriori informazioni, fare riferimento a Stato in tempo reale dell'autenticazione 802.1X.**Nota:** lo stato di autenticazione può essere verificato anche da **Impostazioni > Stato > Messaggi di stato**.

Switch Layer 3

Se la password e il nome utente sembrano corretti, verificare lo stato della porta 802.1x sullo switch.

1. Cercare uno stato della porta che indichi AUTORIZZATO.

```
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
```

Verificare lo stato della VLAN dopo aver completato l'autenticazione.

```
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. Verificare lo stato del binding DHCP dopo un'autenticazione riuscita.

```
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
```

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Autenticazione telefono IP non riuscita

Nel campo Stato telefono IP viene visualizzato `Configurazione IP` o `Registrazione` in caso di errore dell'autenticazione 802.1x. Per risolvere questo problema, completare i seguenti passaggi:

- Verificare che 802.1x sia abilitato sul telefono IP.
- Verificare di avere immesso l'ID dispositivo nel server di autenticazione (RADIUS) come nome utente.
- Confermare che il segreto condiviso sia configurato sul telefono IP.
- Se è stato configurato il segreto condiviso, verificare che nel server di autenticazione sia stato immesso lo stesso segreto condiviso.
- Verificare di aver configurato correttamente gli altri dispositivi richiesti, ad esempio lo switch e il server di autenticazione.

Informazioni correlate

- Configurazione dell'autenticazione basata sulla porta IEEE 802.1x
- Configurazione del telefono IP per l'utilizzo dell'autenticazione 802.1x
- Linee guida per la distribuzione di Cisco Secure ACS per server Windows NT/2000 in un ambiente switch Cisco Catalyst
- RFC 2868: Attributi RADIUS per il supporto del protocollo tunnel
- Esempio di autenticazione IEEE 802.1x con Catalyst 6500/6000 con software Cisco IOS
- Esempio di autenticazione IEEE 802.1x con Catalyst 6500/6000 con software CatOS
- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico – Cisco Systems