Ejemplo de Configuración de Autenticación de Varios Dominios IEEE 802.1x en Switches de Configuración Fija de Capa 3 de Cisco Catalyst

Contenido

Introducción

La autenticación multidominio permite que un teléfono IP y un PC se autentiquen en el mismo puerto del switch mientras los coloca en las VLAN de voz y datos adecuadas. Este documento explica cómo configurar la autenticación de varios dominios (MDA) IEEE 802.1x en los switches de configuración fija de capa 3 de Cisco Catalyst.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- ¿Cómo funciona RADIUS?
- Guía de implementación de Catalyst Switching y ACS
- Guía del usuario de Cisco Secure Access Control Server 4.1
- Descripción general del teléfono IP de Cisco Unified

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switch Catalyst de Cisco serie 3560 que ejecuta Cisco IOS® Software Release 12.2(37)SE1**Nota:** El soporte de autenticación multidominio está disponible solamente en Cisco IOS Software Release 12.2(35)SE y posterior.
- Este ejemplo utiliza Cisco Secure Access Control Server (ACS) 4.1 como servidor RADIUS.**Nota:** Se debe especificar un servidor RADIUS antes de habilitar 802.1x en el switch.
- Clientes de PC que admiten autenticación 802.1x**Nota:** Este ejemplo utiliza clientes de Microsoft Windows XP.
- Teléfono IP 7970G de Cisco Unified con firmware SCCP versión 8.2(1)
- Teléfono IP 7961G de Cisco Unified con firmware SCCP versión 8.2(2)
- Media Covergence Server (MCS) con 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.

Productos Relacionados

Esta configuración también se puede utilizar con estos hardware:

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

Nota: El switch Catalyst de Cisco serie 3550 no admite la autenticación de varios dominios 802.1x.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

El estándar IEEE 802.1x define un protocolo de autenticación y control de acceso basado en cliente-servidor que restringe la conexión de dispositivos no autorizados a una LAN a través de puertos de acceso público. 802.1x controla el acceso a la red mediante la creación de dos puntos de acceso virtuales distintos en cada puerto. Un punto de acceso es un puerto no controlado; el otro es un puerto controlado. Todo el tráfico a través del puerto único está disponible para ambos

puntos de acceso. 802.1x autentica cada dispositivo de usuario que está conectado a un puerto de switch y asigna el puerto a una VLAN antes de que ponga a disposición cualquier servicio ofrecido por el switch o la LAN. Hasta que se autentique el dispositivo, el control de acceso 802.1x sólo permite el tráfico de protocolo de autenticación extensible sobre LAN (EAPOL) a través del puerto al que está conectado el dispositivo. Una vez que la autenticación se realiza correctamente, el tráfico normal puede pasar a través del puerto.

802.1x consta de tres componentes principales. Cada una de ellas se denomina entidad de acceso a puertos (PAE).

- Suplicante: dispositivo cliente que solicita acceso a la red, por ejemplo, teléfonos IP y PC conectados
- Authenticator: dispositivo de red que facilita las solicitudes de autorización del solicitante, por ejemplo, Cisco Catalyst 3560
- Servidor de autenticación: servidor de usuario de acceso telefónico de autenticación remota (RADIUS), que proporciona el servicio de autenticación, por ejemplo, Cisco Secure Access Control Server

Los teléfonos IP de Cisco Unified también contienen un suplicante 802.1X. Este suplicante permite a los administradores de red controlar la conectividad de los teléfonos IP a los puertos del switch LAN. La versión inicial del suplicante 802.1X del teléfono IP implementa la opción EAP-MD5 para la autenticación 802.1X. En una configuración de varios dominios, el teléfono IP y el PC conectado deben solicitar de forma independiente acceso a la red mediante la especificación de un nombre de usuario y una contraseña. El dispositivo Authenticator puede requerir información de los atributos RADIUS llamados. Los atributos especifican información de autorización adicional como si se permite el acceso a una VLAN determinada para un solicitante. Estos atributos pueden ser específicos del proveedor. Cisco utiliza el atributo RADIUS `cisco-av-pair` para decirle al autenticador (Cisco Catalyst 3560) que se permite un suplicante (teléfono IP) en la VLAN de voz.

Configurar

En esta sección, se le presenta la información para configurar la función de autenticación multidominio 802.1x descrita en este documento.

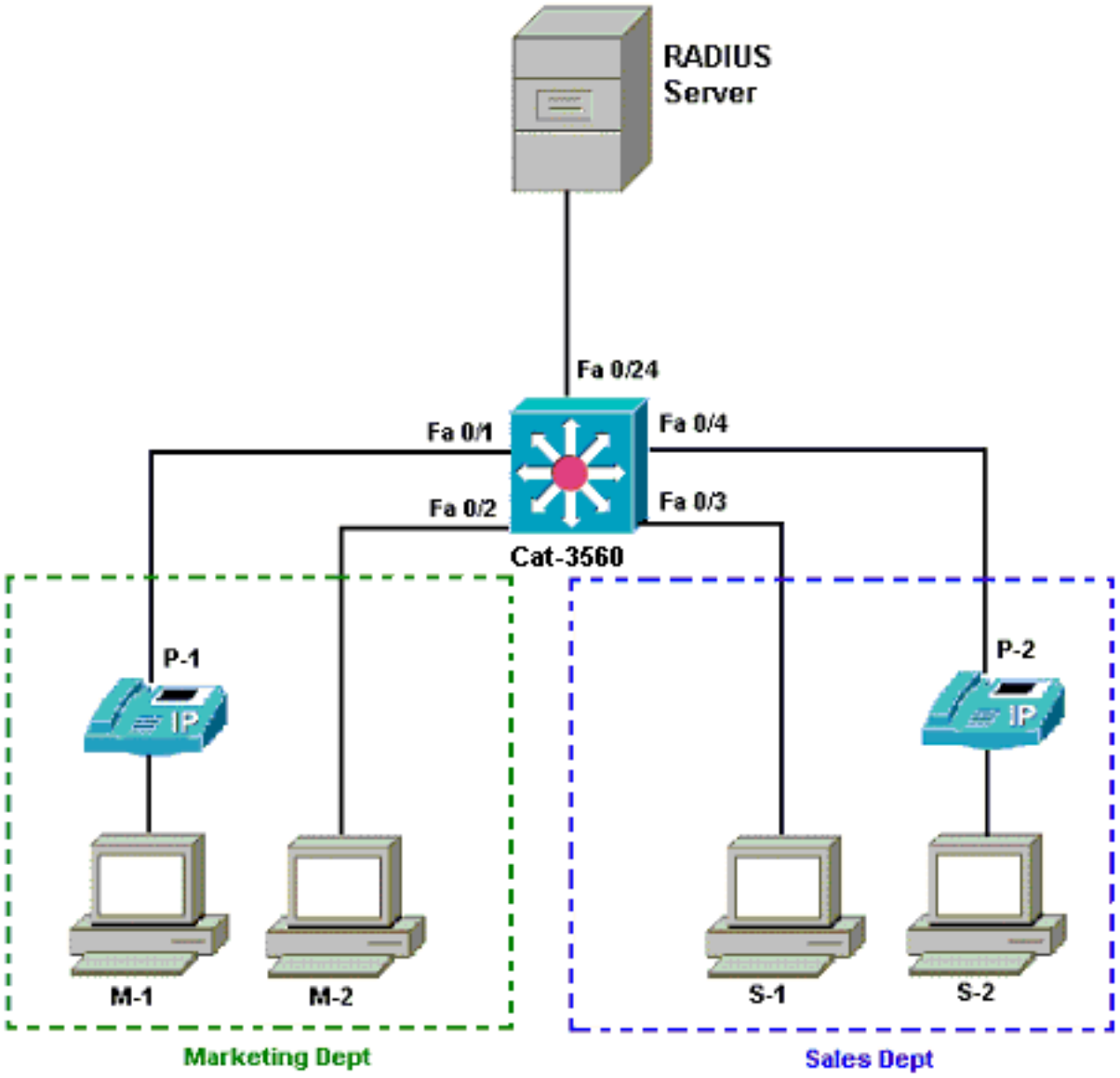
La configuración requiere estos pasos:

- Configure el Switch Catalyst para la Autenticación de Varios Dominios 802.1x.
- Configure el servidor RADIUS.
- Configure los clientes de PC para utilizar la autenticación 802.1x.
- Configure los teléfonos IP para utilizar la autenticación 802.1x.

Nota: Use la Command Lookup Tool (sólo para clientes registrados) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



- Servidor RADIUS: realiza la autenticación real del cliente. El servidor RADIUS valida la identidad del cliente y notifica al switch si el cliente está autorizado o no para acceder a la LAN y los servicios del switch. Aquí, el Cisco ACS se instala y configura en un Media Covergence Server (MCS) para la autenticación y la asignación de VLAN. El MCS también es el servidor TFTP y Cisco Unified Communications Manager (Cisco CallManager) para los teléfonos IP.
- Switch: controla el acceso físico a la red en función del estado de autenticación del cliente. El switch actúa como intermediario (proxy) entre el cliente y el servidor RADIUS. Solicita información de identidad del cliente, verifica esa información con el servidor RADIUS y retransmite una respuesta al cliente. Aquí, el switch Catalyst 3560 también se configura como servidor DHCP. El soporte de autenticación 802.1x para el protocolo de configuración dinámica de host (DHCP) permite al servidor DHCP asignar las direcciones IP a las diferentes clases de usuarios finales. Para hacer esto, agrega la identidad de usuario autenticada al proceso de detección de DHCP. Los puertos FastEthernet 0/1 y 0/4 son los únicos puertos configurados para la autenticación multidominio 802.1x. Los puertos FastEthernet 0/2 y 0/3 se encuentran en el modo de host único 802.1x predeterminado. El puerto FastEthernet 0/24 se conecta al servidor RADIUS.**Nota:** Si utiliza un servidor DHCP externo, no olvide agregar el comando **ip helper-address** en la interfaz SVI (vlan), en la que reside el cliente, que apunta al servidor DHCP.

- Clientes: se trata de dispositivos, por ejemplo, teléfonos IP o estaciones de trabajo, que solicitan acceso a los servicios LAN y de switch y responden a las solicitudes del switch. Aquí, los clientes se configuran para obtener la dirección IP de un servidor DHCP. Los dispositivos M-1, M-2, S-1 y S-2 son los clientes de estación de trabajo que solicitan acceso a la red. P-1 y P-2 son los clientes del teléfono IP que solicitan acceso a la red. M-1, M-2 y P-1 son dispositivos cliente en el departamento de marketing. S-1, S-2 y P-2 son dispositivos cliente en el departamento de ventas. Los teléfonos IP P-1 y P-2 están configurados para estar en la misma VLAN de voz (VLAN 3). Las estaciones de trabajo M-1 y M-2 se configuran para que estén en la misma VLAN de datos (VLAN 4) después de una autenticación exitosa. Las estaciones de trabajo S-1 y S-2 también están configuradas para que estén en la misma VLAN de datos (VLAN 5) después de una autenticación exitosa.**Nota:** Sólo puede utilizar la asignación de VLAN dinámica desde un servidor RADIUS para los dispositivos de datos.

Configuración del switch Catalyst para la autenticación multidominio 802.1x

Esta configuración de switch de ejemplo incluye:

- Cómo habilitar la autenticación multidominio 802.1x en los puertos del switch
- configuración relacionada con el servidor RADIUS
- Configuración del servidor DHCP para la asignación de dirección IP
- Routing entre VLAN para tener conectividad entre clientes después de la autenticación

Refiérase a Uso de la Autenticación Multidominio para obtener más información sobre las pautas sobre cómo configurar MDA.

Nota: Asegúrese de que el servidor RADIUS siempre se conecte detrás de un puerto autorizado.

Nota: Aquí sólo se muestra la configuración 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
```

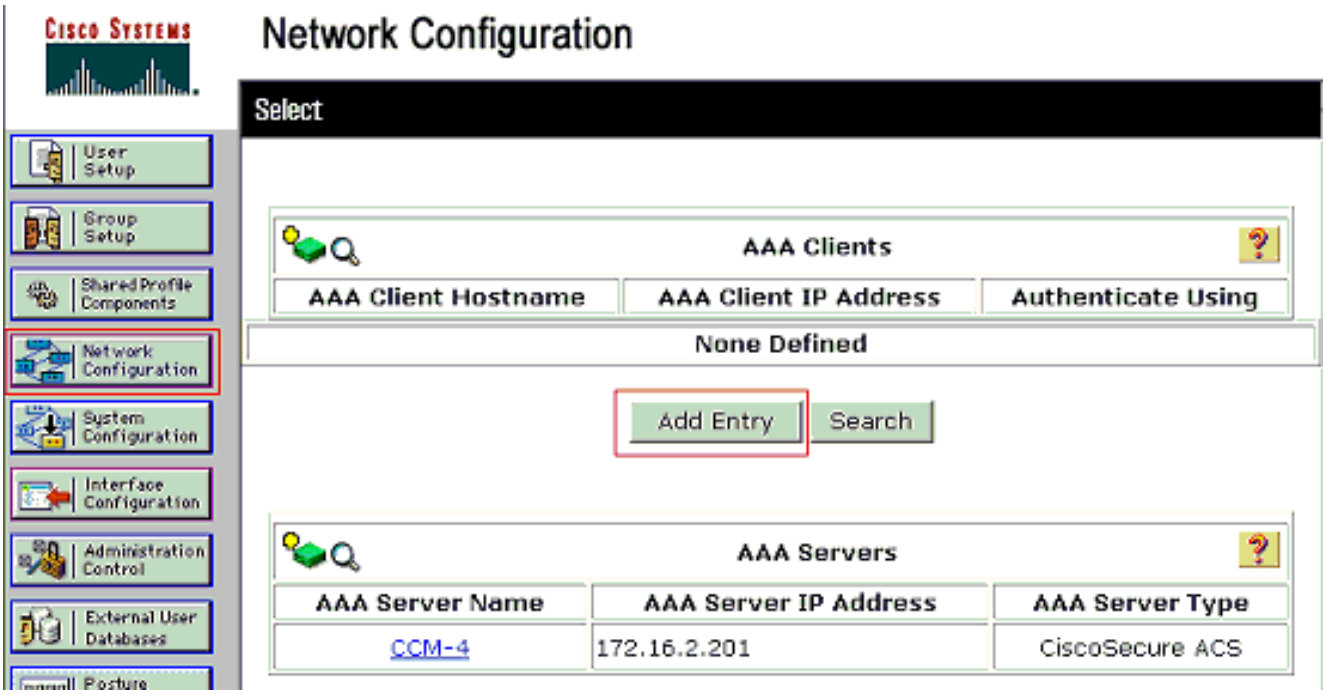
Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Configuración del servidor RADIUS

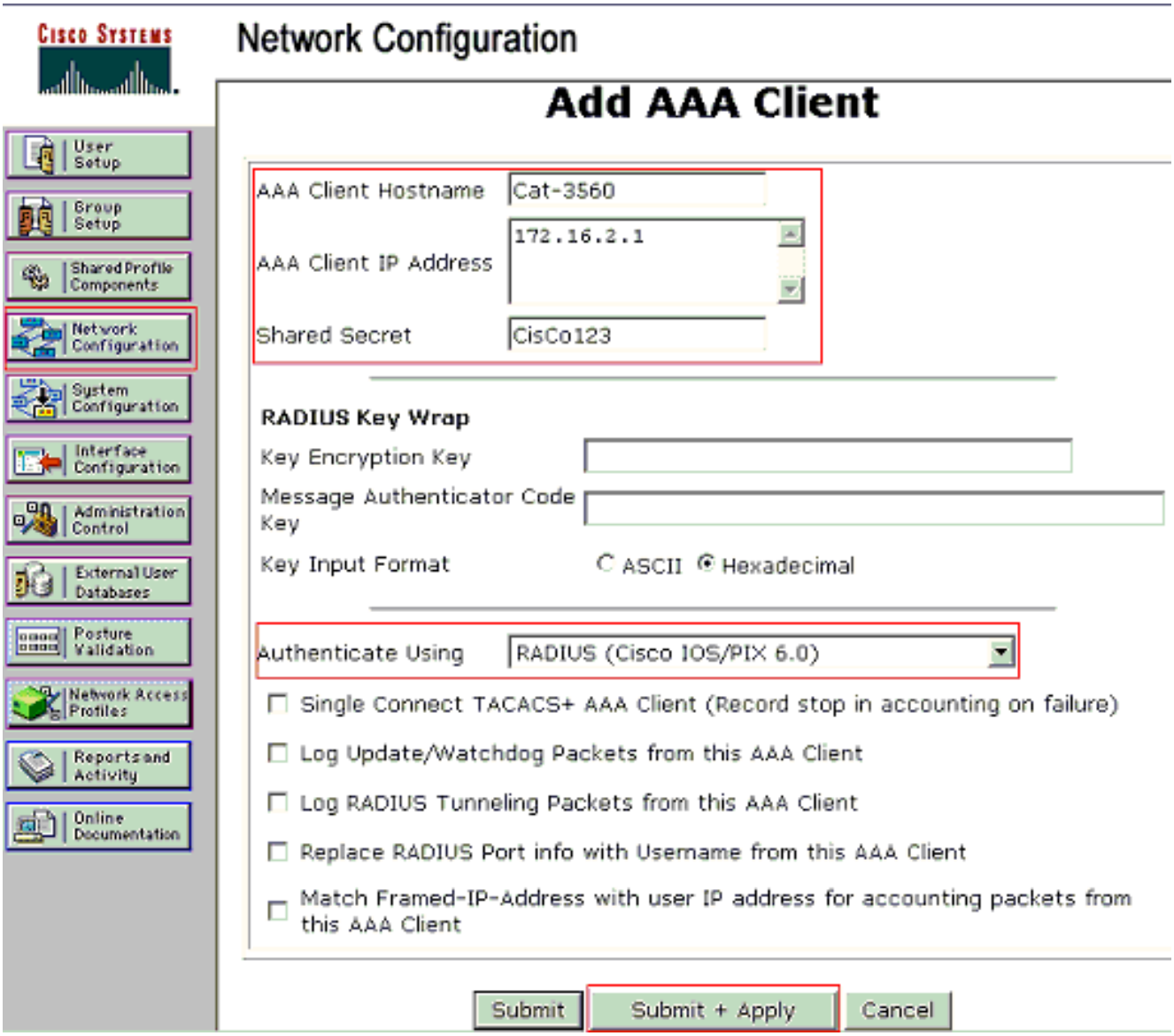
El servidor RADIUS se configura con una dirección IP estática de 172.16.2.201/24. Complete

estos pasos para configurar el servidor RADIUS para un cliente AAA:

1. Haga clic en **Configuración de Red** en la ventana de administración de ACS para configurar un cliente AAA.
2. Haga clic en **Agregar entrada** en la sección Clientes AAA.



3. Configure el nombre de host del cliente AAA, la dirección IP, la clave secreta compartida y el tipo de autenticación como:Nombre de host del cliente AAA = Nombre de host del switch (**Cat-3560**).Dirección IP del cliente AAA = Dirección IP de la interfaz de administración del switch (**172.16.2.1**).Secreto compartido = clave RADIUS configurada en el switch (**CisCo123**).**Nota:** Para un funcionamiento correcto, la clave secreta compartida debe ser idéntica en el cliente AAA y ACS. Las claves distinguen entre mayúsculas y minúsculas.Autentique Usando = **RADIUS (Cisco IOS/PIX 6.0)**.**Nota:** El atributo del par de Cisco Attribute-Value (AV) está disponible en esta opción.
4. Haga clic en **Enviar + Aplicar** para que estos cambios sean efectivos, como muestra este ejemplo:



Configuración de grupo

Consulte esta tabla para configurar el servidor RADIUS para la autenticación.

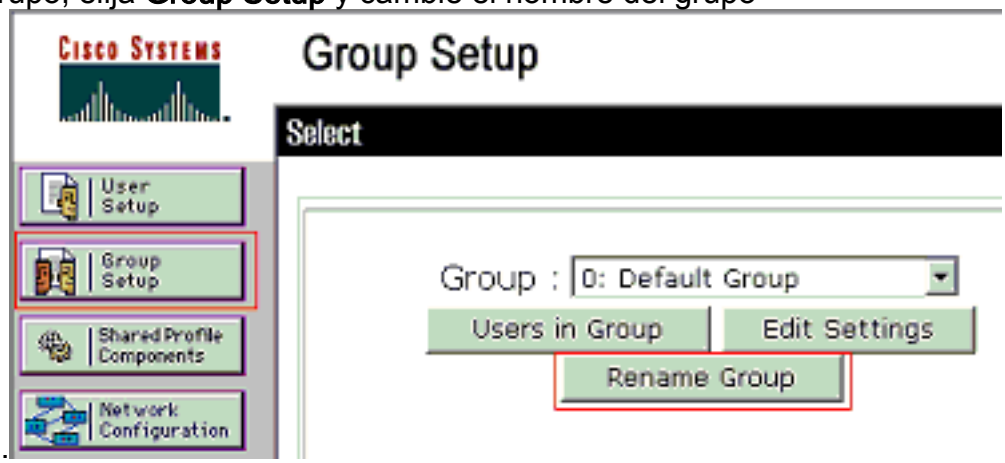
Dispositivo	Dept	Grupo	Usuario	Contraseña	VLAN	Conjunto DHCP
M-1	Marketing	Marketing	mkt-manager	Cisco	MARKETING	Marketing
M-2	Marketing	Marketing	mkt-staff	MScisco	MARKETING	Marketing
S-2	Ventas	Ventas	gerente de ventas	SMcisco	VENTAS	Ventas
S-1	Ventas	Ventas	person	Cisco	VENTA	Vent

			al de ventas		S	as
P-1	Marketing	Teléfonos IP	CP-7970G-SEP001759E7492C	P1cisco	VOICE	Teléfonos IP
P-2	Ventas	Teléfonos IP	CP-7961G-SEP001A2F80381F	P2cisco	VOICE	Teléfonos IP

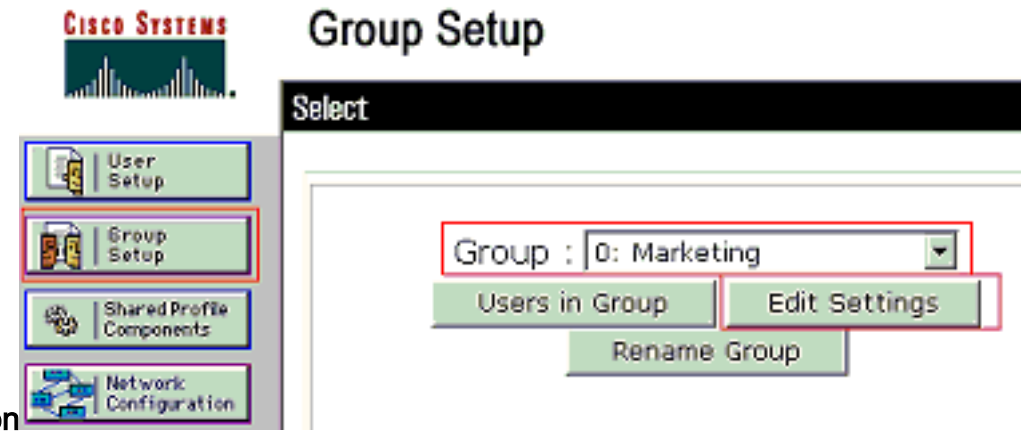
Cree grupos para clientes que se conectan a VLAN 3 (VOZ), 4 (MARKETING) y 5 (VENTAS). Aquí, se crean grupos de **teléfonos IP**, **marketing** y **ventas** con este fin.

Nota: Esta es la configuración de los grupos **Marketing** y **Teléfonos IP**. Para la configuración del grupo **Ventas**, complete los pasos para el grupo **Marketing**.

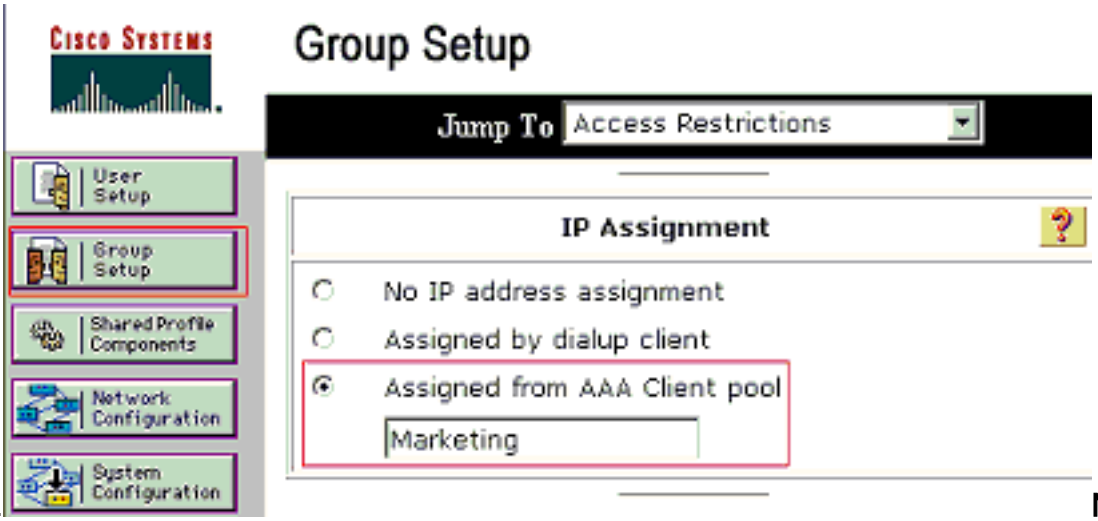
1. Para crear un grupo, elija **Group Setup** y cambie el nombre del grupo predeterminado.



2. Para configurar un grupo, elija el grupo de la lista y haga clic en **Editar configuración**

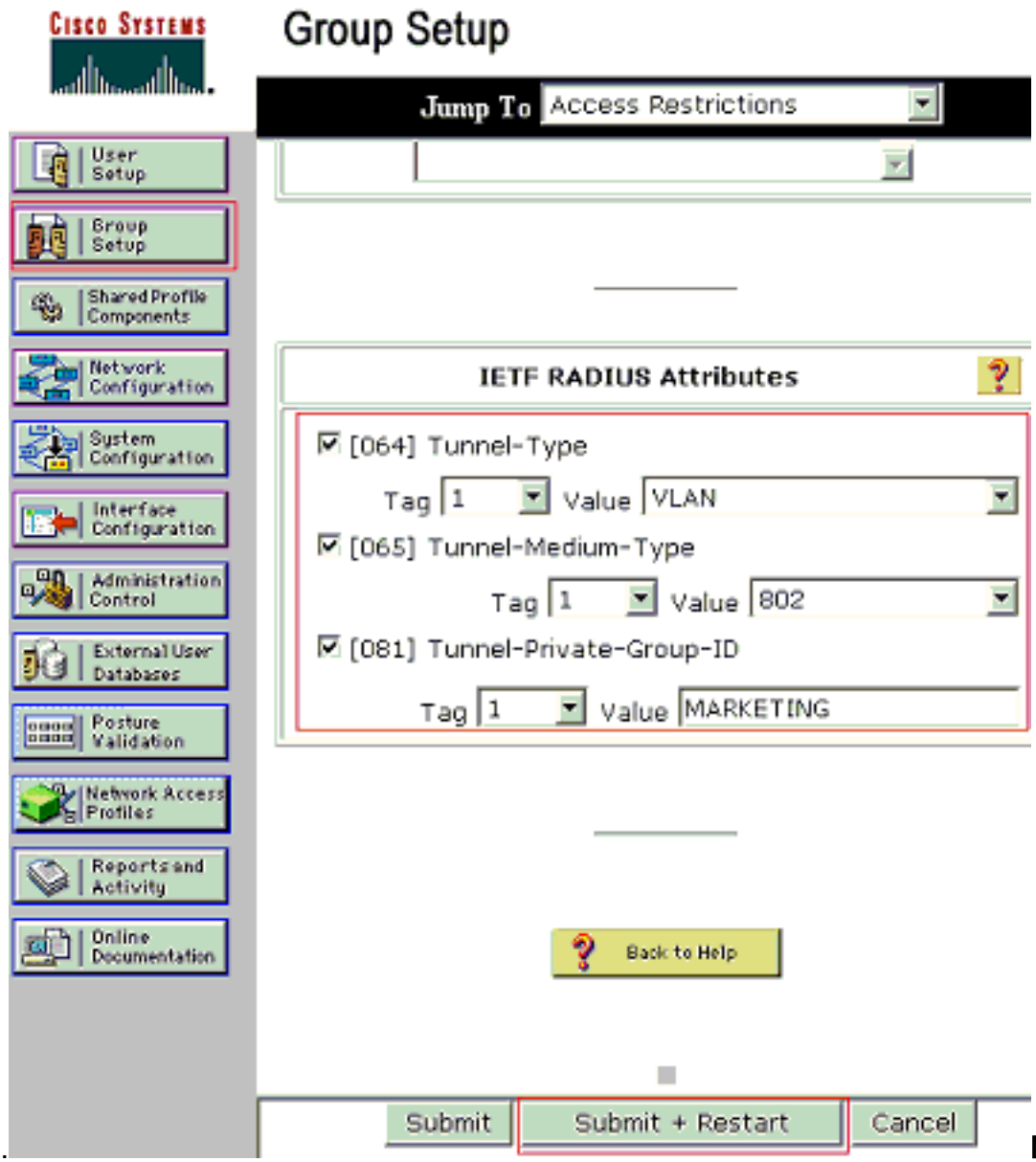


3. Defina la asignación de dirección IP del cliente como **Asignado por el conjunto de clientes AAA**. Introduzca el nombre del conjunto de direcciones IP configurado en el switch para estos clientes de



grupo. **Nota:** Elija esta opción y escriba el nombre del conjunto IP del cliente AAA en el cuadro, sólo si este usuario va a tener la dirección IP asignada por un conjunto de direcciones IP configurado en el cliente AAA.**Nota:** Para la configuración del grupo de **teléfonos IP** solo, omita el paso siguiente, paso 4, y vaya al paso 5.

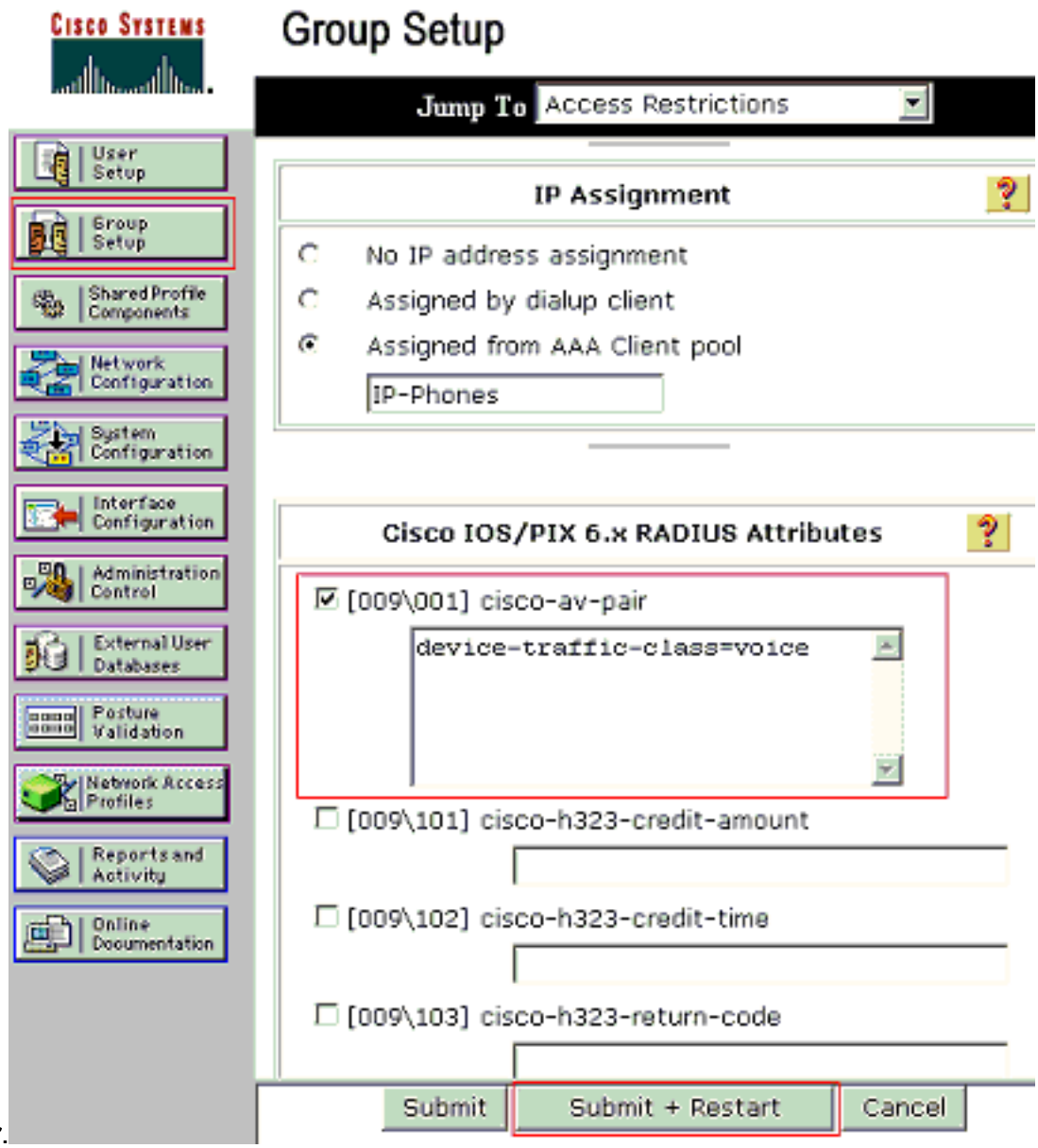
4. Defina los atributos **64**, **65** y **81** de Internet Engineering Task Force (IETF) y, a continuación, haga clic en **Enviar + Reiniciar**.Asegúrese de que las Etiquetas de los Valores estén configuradas en **1**, como muestra este ejemplo. Catalyst ignora cualquier etiqueta que no sea 1. Para asignar un usuario a una VLAN específica, también debe definir el atributo **81** con un *nombre de* VLAN o *número* de VLAN que corresponda.**Nota:** Si utiliza el *nombre* de VLAN, debe ser exactamente igual al configurado en el



switch. **Nota:** Consulte RFC 2868: Atributos RADIUS para el Soporte del Protocolo de Túnel para obtener más información sobre estos atributos IETF.**Nota:** En la configuración inicial del servidor ACS, los atributos RADIUS de IETF pueden no mostrarse en la **Configuración de usuario**. Para habilitar los atributos IETF en las pantallas de configuración de usuario, elija **Configuración de interfaz > RADIUS (IETF)**. Luego, verifique los atributos 64, 65 y 81 en las columnas Usuario y Grupo.**Nota:** Si no define el atributo IETF **81** y el puerto es un puerto de switch en modo de acceso, el cliente se asigna a la VLAN de acceso del puerto. Si ha definido el atributo **81** para la asignación de VLAN dinámica y el puerto es un puerto de switch en el modo de acceso, debe ejecutar el comando **aaa authorization network default group radius** en el switch. Este comando asigna el puerto a la VLAN que el servidor RADIUS provee. De lo contrario, 802.1x mueve el puerto al estado AUTORIZADO después de la autenticación del usuario; pero el puerto aún se encuentra en la VLAN predeterminada del puerto y la conectividad puede fallar.**Nota:** El siguiente paso sólo se aplica al grupo **de teléfonos IP**.

5. Configure el servidor RADIUS para que envíe un atributo de par Cisco Attribute-Value (AV) para autorizar un dispositivo de voz. Sin esto, el switch trata al dispositivo de voz como un dispositivo de datos. Defina el atributo de par de Cisco Attribute-Value (AV) con un valor de *device-traffic-class=voice* y haga clic en **Enviar +**

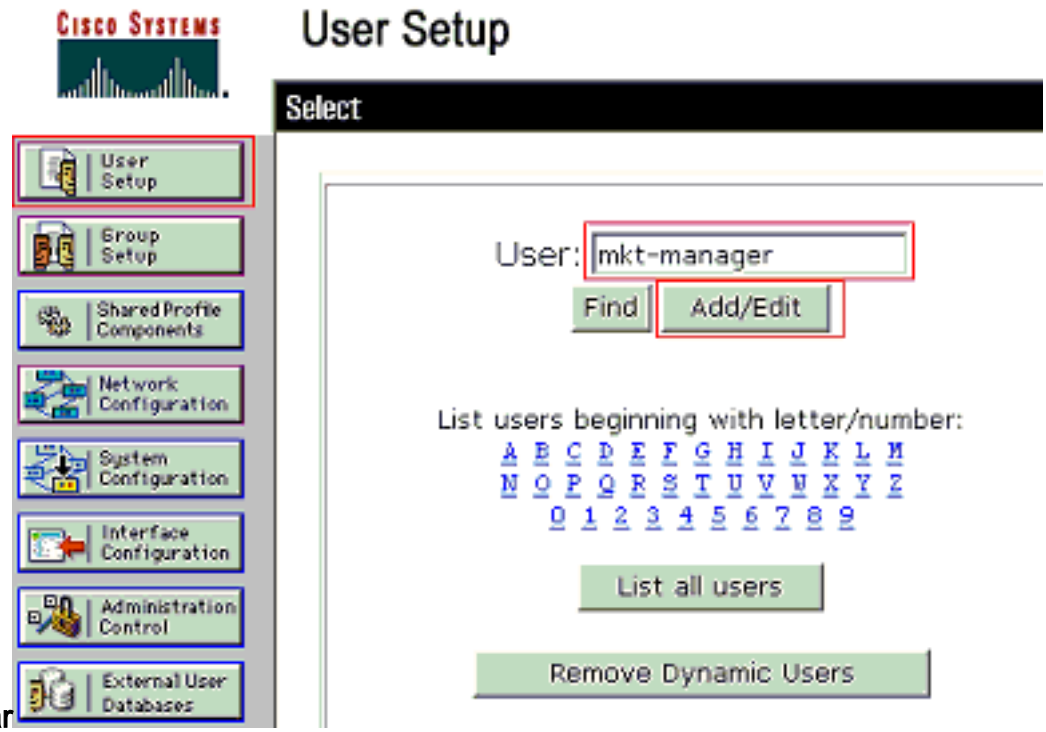
Reiniciar.



Configuración de usuario

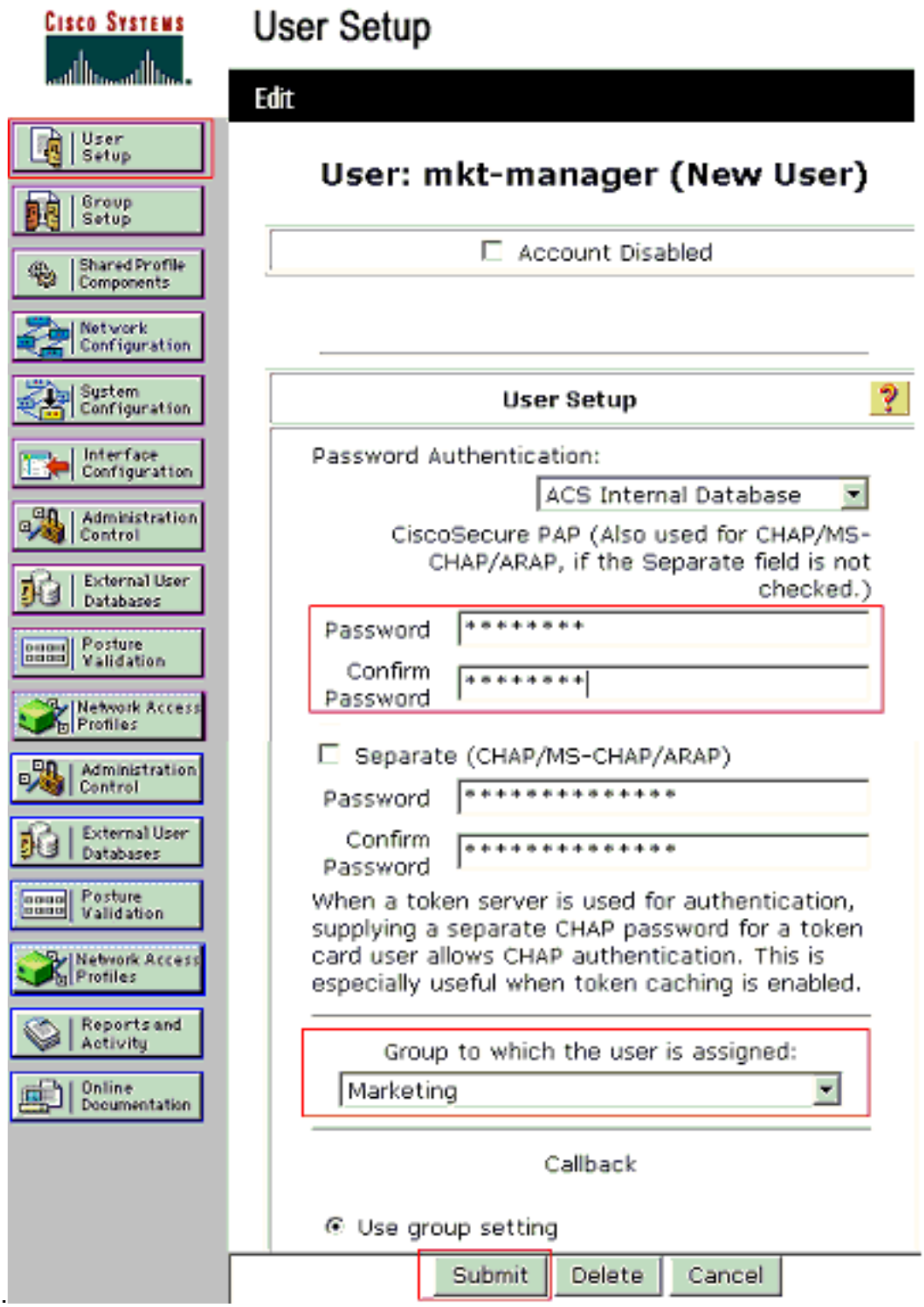
Complete estos pasos para agregar y configurar un usuario.

1. Para agregar y configurar usuarios, elija **User Setup**. Introduzca el nombre de usuario y haga clic en



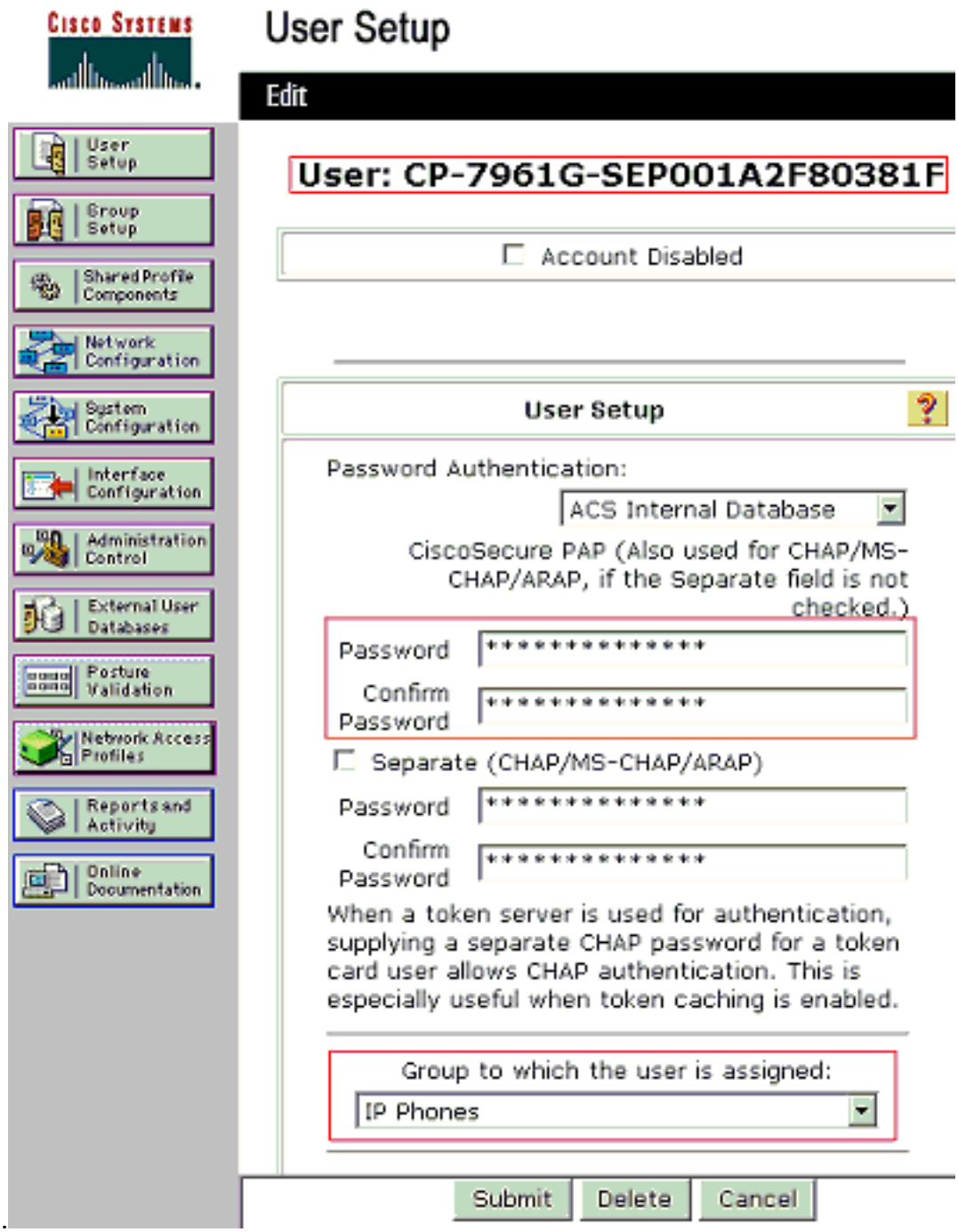
Agregar/Editar

2. Defina el nombre de usuario, la contraseña y el grupo para el



usuario.

3. El teléfono IP utiliza su ID de dispositivo como nombre de usuario y secreto compartido como contraseña para la autenticación. Estos valores deben coincidir en el servidor RADIUS. Para los teléfonos IP P-1 y P-2, cree nombres de usuario iguales a su ID de dispositivo y contraseña que el secreto compartido configurado. Consulte la sección Configuración de los Teléfonos IP para Utilizar la Autenticación 802.1x para obtener más información sobre el ID de dispositivo y el Secreto compartido en un Teléfono



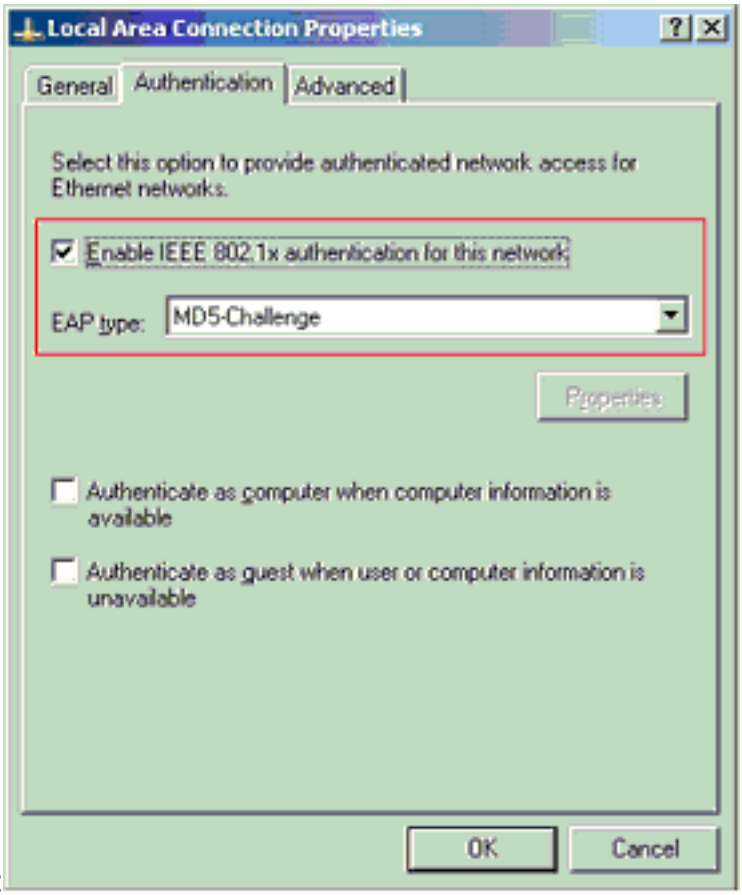
IP.

Configuración de los clientes de PC para utilizar la autenticación 802.1x

Este ejemplo es específico del cliente de protocolo de autenticación extensible (EAP) sobre LAN (EAPOL) de Microsoft Windows XP:

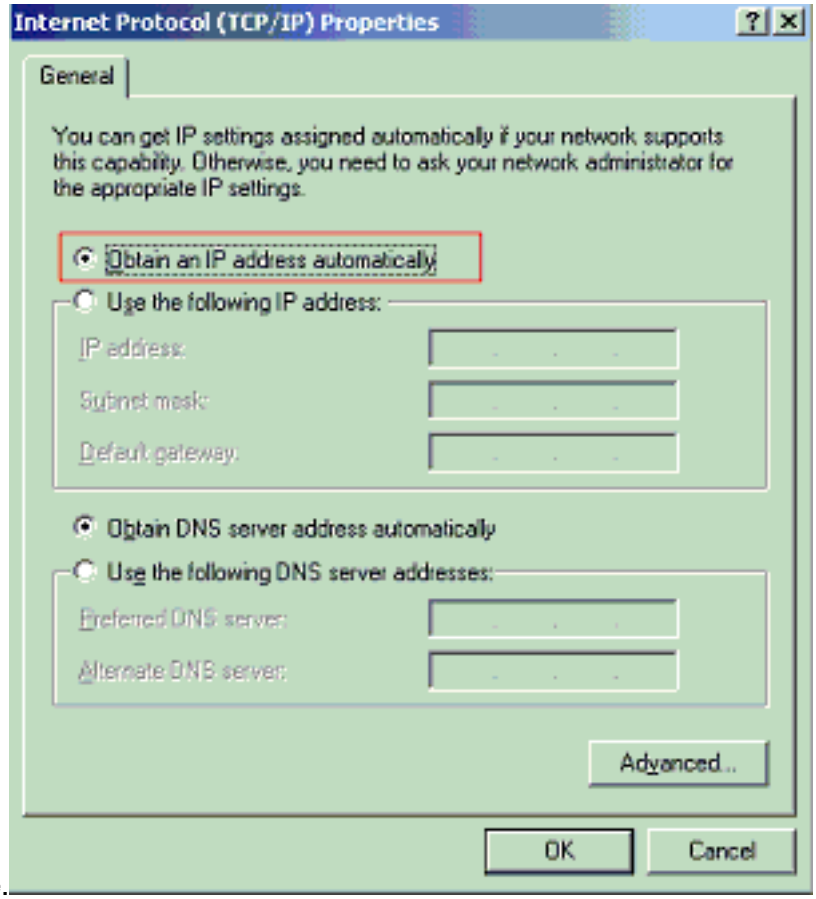
1. Elija **Inicio > Panel de control > Conexiones de red**, luego haga clic con el botón derecho en su **Conexión de área local** y elija **Propiedades**.
2. Marque **Mostrar icono en el área de notificación cuando esté conectado** en la ficha General.
3. En la ficha Authentication (Autenticación), marque Enable IEEE 802.1x authentication para habilitar la autenticación en esta red.
4. Establezca el tipo EAP en MD5-Challenge tal como se muestra en el

ejemplo:



Complete estos pasos para configurar los clientes para obtener la dirección IP de un servidor DHCP.

1. Elija **Inicio > Panel de control > Conexiones de red**, luego haga clic con el botón derecho en su **Conexión de área local** y elija **Propiedades**.
2. En la ficha General, haga clic en **Internet Protocol (TCP/IP)** y, a continuación, **Properties**.
3. Elija **Obtener una dirección IP**

automáticamente. 

Configuración de los Teléfonos IP para Utilizar la Autenticación 802.1x

Complete estos pasos para configurar los teléfonos IP para la autenticación 802.1x.

1. Presione el botón **Settings** para acceder a la configuración de **Autenticación 802.1X** y elija **Configuración de Seguridad > Autenticación 802.1X > Autenticación de Dispositivo**.
2. Establezca la opción **Device Authentication** en **Enabled**.
3. Presione la tecla programable **Save.**
4. Elija **802.1X Authentication > EAP-MD5 > Shared Secret** para establecer una contraseña en el teléfono.
5. Introduzca el secreto compartido y pulse **Guardar**.**Nota:** La contraseña debe tener entre seis y 32 caracteres, que constan de cualquier combinación de números o letras. `Esa clave no está activa aquí` se muestra el mensaje y la contraseña no se guarda si no se cumple esta condición.**Nota:** Si desactiva la autenticación 802.1X o realiza un restablecimiento de fábrica en el teléfono, se elimina el secreto compartido MD5 configurado previamente.**Nota:** No se pueden configurar las otras opciones, ID de dispositivo y rango. El ID de dispositivo se utiliza como nombre de usuario para la autenticación 802.1x. Se trata de una derivación del número de modelo del teléfono y la dirección MAC única que se muestra en este formato: CP-<model>-SEP-<MAC>. Por ejemplo, **CP-7970G-SEP001759E7492C**. Refiérase a Configuración de Autenticación 802.1X para obtener más información.

Complete estos pasos para configurar el teléfono IP para obtener la dirección IP de un servidor DHCP.

1. Presione el botón **Settings** para acceder a la configuración de **Network Configuration** y elija **Network Configuration**.
2. Desbloquee las opciones **de configuración de red**. Para desbloquear, presione **#.**Nota:** No

presione **# para desbloquear opciones y luego presione inmediatamente **# de nuevo para bloquear opciones. El teléfono interpreta esta secuencia como **#**, que restablece el teléfono. Para bloquear las opciones después de desbloquearlas, espere al menos 10 segundos antes de presionar **# otra vez.

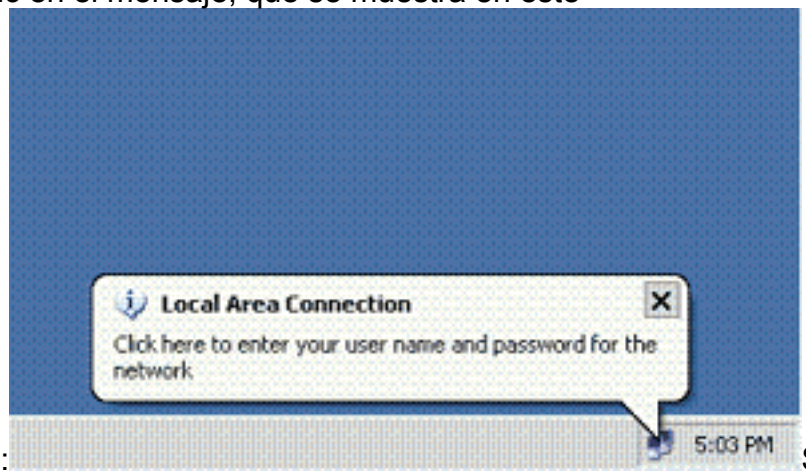
3. Desplácese hasta la opción DHCP Enabled y presione la tecla programada **Yes** para habilitar DHCP.
4. Presione la tecla programable **Save.**

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

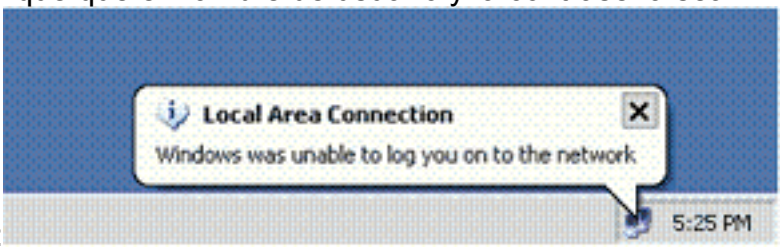
Clientes de PC

Si ha completado correctamente la configuración, los clientes de PC mostrarán un mensaje emergente para introducir un nombre de usuario y una contraseña.

1. Haga clic en el mensaje, que se muestra en este ejemplo: 

Se muestra una ventana de entrada de nombre de usuario y contraseña.**Nota:** MDA no aplica el orden de autenticación del dispositivo. Sin embargo, para obtener mejores resultados, Cisco recomienda que un dispositivo de voz se autentique antes que un dispositivo de datos en un puerto habilitado para MDA.
2. Introduzca el nombre de usuario y la

contraseña. 

3. Si no aparece ningún mensaje de error, verifique la conectividad con los métodos habituales, por ejemplo, a través del acceso a los recursos de red y con **ping**.**Nota:** Si aparece este error, verifique que el nombre de usuario y la contraseña sean correctos: 

Teléfonos IP

El menú 802.1X Authentication Status (Estado de autenticación) en los teléfonos IP permite supervisar el estado de autenticación.

1. Presione el botón **Settings** para acceder a las Estadísticas en Tiempo Real de Autenticación 802.1X y elija **Security Configuration > 802.1X Authentication Status**.
2. El **estado de la transacción** debe **autenticarse**. Refiérase a 802.1X Authentication Real-Time Status para obtener más información.**Nota:** El estado de autenticación también se puede verificar desde **Settings > Status > Status Messages**.

Switch de capa 3

Si la contraseña y el nombre de usuario parecen ser correctos, verifique el estado del puerto 802.1x en el switch.

1. Busque un estado de puerto que indique `AUTHORIZED`.

```
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
```

Verifique el estado de VLAN después de la autenticación exitosa.

```
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. Verifique el estado de enlace DHCP después de una autenticación exitosa.

```
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
```

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilize el OIT para ver una análisis de la salida del comando show.

Troubleshoot

Error de autenticación del teléfono IP

El estado del teléfono IP muestra `Configuración de IP` o `Registro` si falla la autenticación 802.1x. Complete estos pasos para resolver estos problemas:

- Confirme que el 802.1x esté activado en el teléfono IP.
- Compruebe que ha introducido el ID de dispositivo en el servidor de autenticación (RADIUS) como nombre de usuario.
- Confirme que el secreto compartido esté configurado en el teléfono IP.
- Si el secreto compartido está configurado, verifique que se haya especificado el mismo secreto compartido en el servidor de autenticación.
- Verifique que haya configurado correctamente los otros dispositivos requeridos, por ejemplo, el switch y el servidor de autenticación.

Información Relacionada

- Configuración de la Autenticación Basada en Puertos IEEE 802.1x
- Configuración del teléfono IP para utilizar la autenticación 802.1x
- Pautas para la implementación de Cisco Secure ACS para servidores Windows NT/2000 en un entorno de switch Catalyst de Cisco
- RFC 2868: Atributos de RADIUS para soporte a protocolo de túnel
- Ejemplo de Configuración de Autenticación IEEE 802.1x con Catalyst 6500/6000 que Ejecuta Cisco IOS Software
- Ejemplo de Configuración de Autenticación IEEE 802.1x con Catalyst 6500/6000 que Ejecuta el Software CatOS
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems