Autenticación del Multi-dominio del IEEE 802.1X en el ejemplo de configuración de los switches de configuración fija de la capa 3 del Cisco Catalyst

Contenido

Introducción

La autenticación del Multi-dominio permite que un teléfono del IP y un PC autentiquen en el mismo puerto del switch mientras que los coloca en la Voz y los VLAN de datos apropiados. Este documento explica cómo configurar la autenticación del Multi-dominio del IEEE 802.1X (MDA) en los switches de configuración fija de la capa 3 del Cisco Catalyst.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- ¿Cómo el RADIUS trabaja?
- Transferencia del Catalyst y Guía de despliegue ACS
- Guía del usuario para el Cisco Secure Access Control Server 4.1
- Una descripción de Cisco unificó el teléfono del IP

Componentes Utilizados

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

- Cisco Catalyst 3560 Series Switch que funciona con la versión 12.2(37)SE1 del Cisco IOS ® Software**Nota:** El soporte de la autenticación del Multi-dominio está disponible solamente del Cisco IOS Software Release 12.2(35)SE y Posterior.
- Este ejemplo utiliza el Cisco Secure Access Control Server (ACS) 4.1 como el servidor de RADIUS.**Nota:** Un servidor de RADIUS debe ser especificado antes de que usted habilite el 802.1x en el Switch.
- PC cliente que soporta la autenticación del 802.1x**Nota:** Este ejemplo utiliza a los clientes del Microsoft Windows XP.
- Cisco Unified IP Phone 7970G con la versión 8.2(1) del firmware de SCCP
- Cisco Unified IP Phone 7961G con la versión 8.2(2) del firmware de SCCP
- Servidor de Covergence de los media (MCS) con el administrador de las Comunicaciones unificadas de Cisco (Cisco CallManager) 4.1(3)sr2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Productos Relacionados

Esta configuración se puede también utilizar con estos hardwares:

- Cisco Catalyst 3560-E Series Switch
- Cisco Catalyst 3750 Series Switch
- Cisco Catalyst 3750-E Series Switch

Nota: El Cisco Catalyst 3550 Series Switch no soporta la autenticación del Multi-dominio del 802.1x.

Convenciones

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

Antecedentes

El estándar del IEEE 802.1X define un protocolo basado servidor del cliente del control de acceso y de autenticación que restrinja los dispositivos desautorizados de la conexión con un LAN a

través de los puertos público accesibles. el 802.1x controla el acceso a la red por la creación de dos puntas de acceso virtual distintas en cada puerto. Un Punto de acceso es un puerto incontrolado; el otro es un puerto controlado. Todo el tráfico a través del puerto único está disponible para ambos Puntos de acceso. el 802.1x autentica cada dispositivo del usuario que esté conectado con un puerto del switch y asigna el puerto a un VLA N antes de que haga disponible cualquier servicio que sea ofrecido por el Switch o el LAN. Hasta que se autentique el dispositivo, el control de acceso del 802.1x permite solamente el protocolo extensible authentication sobre el tráfico LAN (EAPOL) a través del puerto con el cual el dispositivo está conectado. Después de que la autenticación sea acertada, el tráfico normal puede pasar a través del puerto.

el 802.1x se comprende de tres componentes primarios. Se refiere cada uno como una entidad del acceso del puerto (PAE).

- Supplicant — Dispositivo del cliente que pide el acceso a la red, por ejemplo, los Teléfonos IP y los PC asociados
- Authenticator — Dispositivo de red que facilita los pedidos de autorización del supplicant, por ejemplo, el Cisco Catalyst 3560
- Servidor de autenticación — Un Remote Authentication Dial-In User Server (RADIUS), que proporciona el servicio de autenticación, por ejemplo, Cisco Secure Access Control Server

Los Teléfonos IP unificados Cisco también contienen un supplicant del 802.1x. Este supplicant permite que los administradores de la red controlen la Conectividad de los Teléfonos IP a los puertos del switch LAN. La versión inicial del supplicant del 802.1x del teléfono del IP implementa la opción del EAP-MD5 para la autenticación del 802.1x. En una configuración del multi-dominio, el teléfono del IP y el PC asociado deben pedir independientemente el acceso a la red por la especificación de un nombre de usuario y contraseña. El dispositivo del authenticator puede requerir la información de los atributos llamados RADIUS. Los atributos especifican la información de autorización adicional por ejemplo si el acceso a un VLAN determinado está permitido para un supplicant. Estos atributos pueden ser específico del vendedor. Cisco utiliza el `Cisco-av-pair del` atributo de RADIUS para decir el authenticator (Cisco Catalyst 3560) que un supplicant (teléfono del IP) no se prohibe en el VLA N de la Voz.

Configurar

En esta sección, le presentan con la información para configurar la característica de autenticación del multi-dominio del 802.1x descrita en este documento.

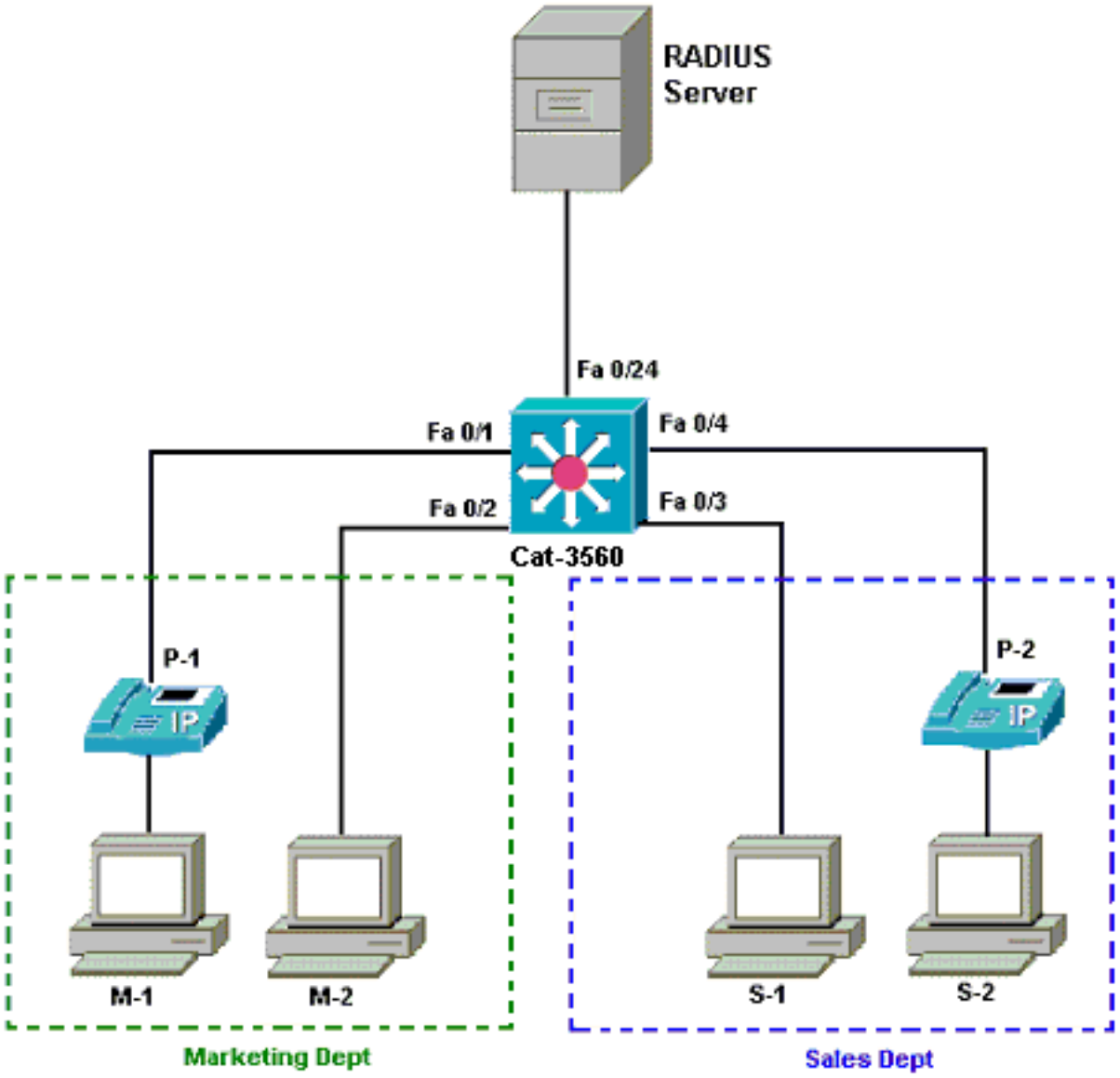
La configuración requiere estos pasos:

- Configure el switch de Catalyst para la autenticación del Multi-dominio del 802.1x.
- Configure al servidor de RADIUS.
- Configure a los PC cliente para utilizar la autenticación del 802.1x.
- Configure los Teléfonos IP para utilizar la autenticación del 802.1x.

Nota: Utilice la herramienta de búsqueda de comandos (clientes registrados solamente) 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 de RADIUS — Esto realiza la autenticación real del cliente. El servidor de RADIUS valida la identidad del cliente y notifica el Switch independientemente de si autorizan al cliente a acceder el LAN y a conmutar los servicios. Aquí, Cisco ACS está instalado y configurado en un servidor de Covergence de los media (MCS) para la autenticación y la asignación VLAN. El MCS es también el servidor TFTP y el administrador de las Comunicaciones unificadas de Cisco (Cisco CallManager) para los Teléfonos IP.
- Switch — Esto controla el acceso físico a la red basada en el estado de autenticación del cliente. El Switch actúa como intermediario (proxy) entre el cliente y el servidor de RADIUS. Pide la información de identidad del cliente, verifica esa información con el servidor de RADIUS, y retransmite una respuesta al cliente. Aquí, el Catalyst 3560 Switch también se configura como servidor DHCP. El soporte de la autenticación del 802.1x para el Protocolo de configuración dinámica de host (DHCP) permite que el servidor DHCP asigne los IP Addresses a las diversas clases de usuarios finales. Para hacer esto, agrega la identidad del usuario autenticado en el proceso de detección del DHCP. El FastEthernet0/1 y 0/4 de los puertos son los únicos puertos configurados para la autenticación del multi-dominio del 802.1x. El FastEthernet 0/2 y 0/3 de los puertos está en el modo predeterminado del solo host del 802.1x. El FastEthernet0/24 del puerto conecta con el servidor de RADIUS.**Nota:** Si usted utiliza a un servidor DHCP externo, no olvide agregar el **comando ip helper-address** en la interfaz (vlan) SVI, en la cual el cliente reside, que señala al servidor DHCP.

- Clientes — Éstos son dispositivos, por ejemplo, los Teléfonos IP o los puestos de trabajo, ese acceso de la petición a los servicios LAN y del Switch y responden a las peticiones del Switch. Aquí, configuran a los clientes para lograr la dirección IP de un servidor DHCP. Los dispositivos M-1, M-2, S1 y S-2 son los clientes del puesto de trabajo que piden el acceso a la red. P-1 y P-2 son los clientes del teléfono del IP que piden el acceso a la red. El M-1, los M-2 y P-1 son dispositivos del cliente en el departamento del márketing. El S1, S-2 y P-2 son dispositivos del cliente en el Departamento de ventas. Los Teléfonos IP P-1 y P-2 se configuran para estar en el mismo VLA N de la Voz (VLA N 3). Los puestos de trabajo M-1 y M-2 se configuran para estar en el mismo VLAN de dato (VLA N 4) después de una autenticación satisfactoria. Los puestos de trabajo S1 y S-2 también se configuran para estar en el mismo VLAN de dato (VLA N 5) después de una autenticación satisfactoria.**Nota:** Usted puede utilizar la asignación del VLAN dinámico de un servidor de RADIUS solamente para los dispositivos de datos.

Configure el switch de Catalyst para la autenticación del Multi-dominio del 802.1x

Esta configuración del switch de la muestra incluye:

- Cómo habilitar la autenticación del multi-dominio del 802.1x en los puertos del switch
- Configuración relacionada del servidor de RADIUS
- Configuración del servidor DHCP para la asignación de la dirección IP
- Routing entre VLAN para tener Conectividad entre los clientes después de la autenticación

Refiérase con la autenticación de Multidomain para más información sobre las guías de consulta en cómo configurar MDA.

Nota: Aseegurese que el servidor de RADIUS conecta siempre detrás de un puerto autorizado.

Nota: Solamente la configuración pertinente se muestra aquí.

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
```

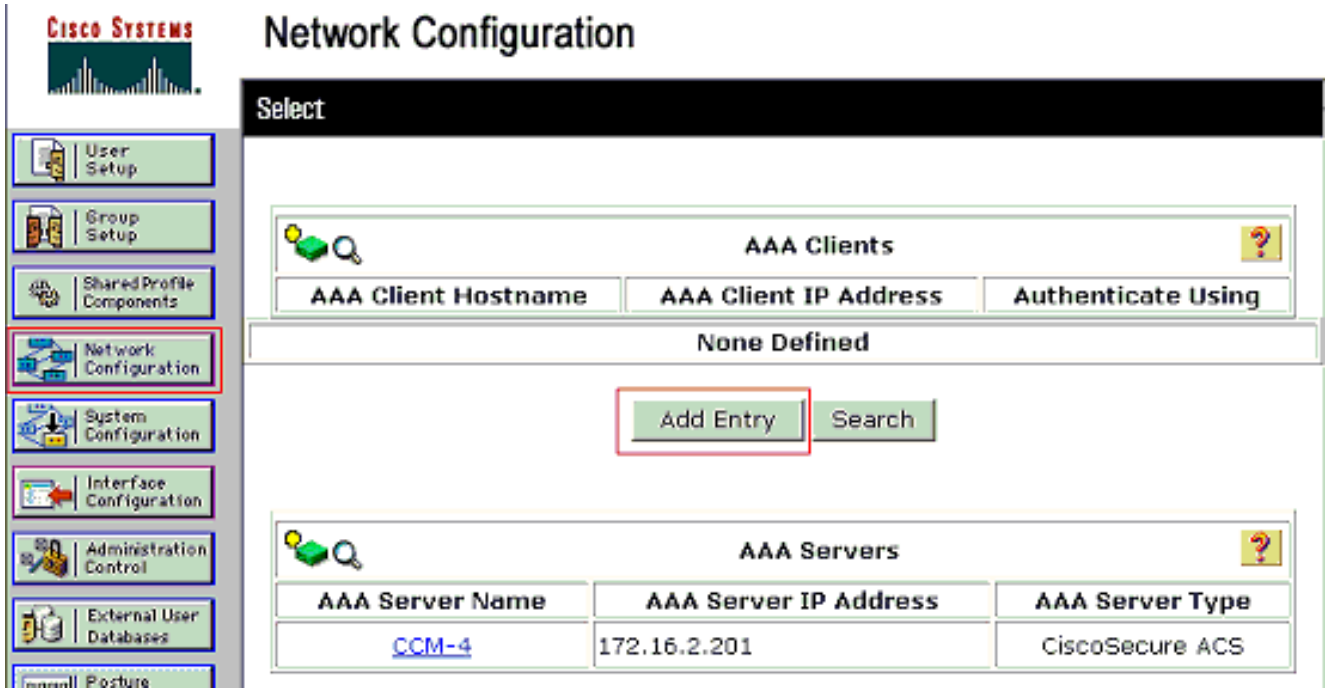
```
radius !--- You need authorization for dynamic VLAN
assignment to work with RADIUS. Cat-3560(config)#radius-
server host 172.16.2.201 key CisCo123 !--- The key must
match the key used on the RADIUS server. Cat-
3560(config)#dot1x system-auth-control !--- Globally
enables 802.1x. Cat-3560(config)#interface 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 la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Configure al servidor de RADIUS

Configuran al servidor de RADIUS con un IP Address estático de 172.16.2.201/24. Complete estos pasos para configurar al servidor de RADIUS para un cliente AAA:

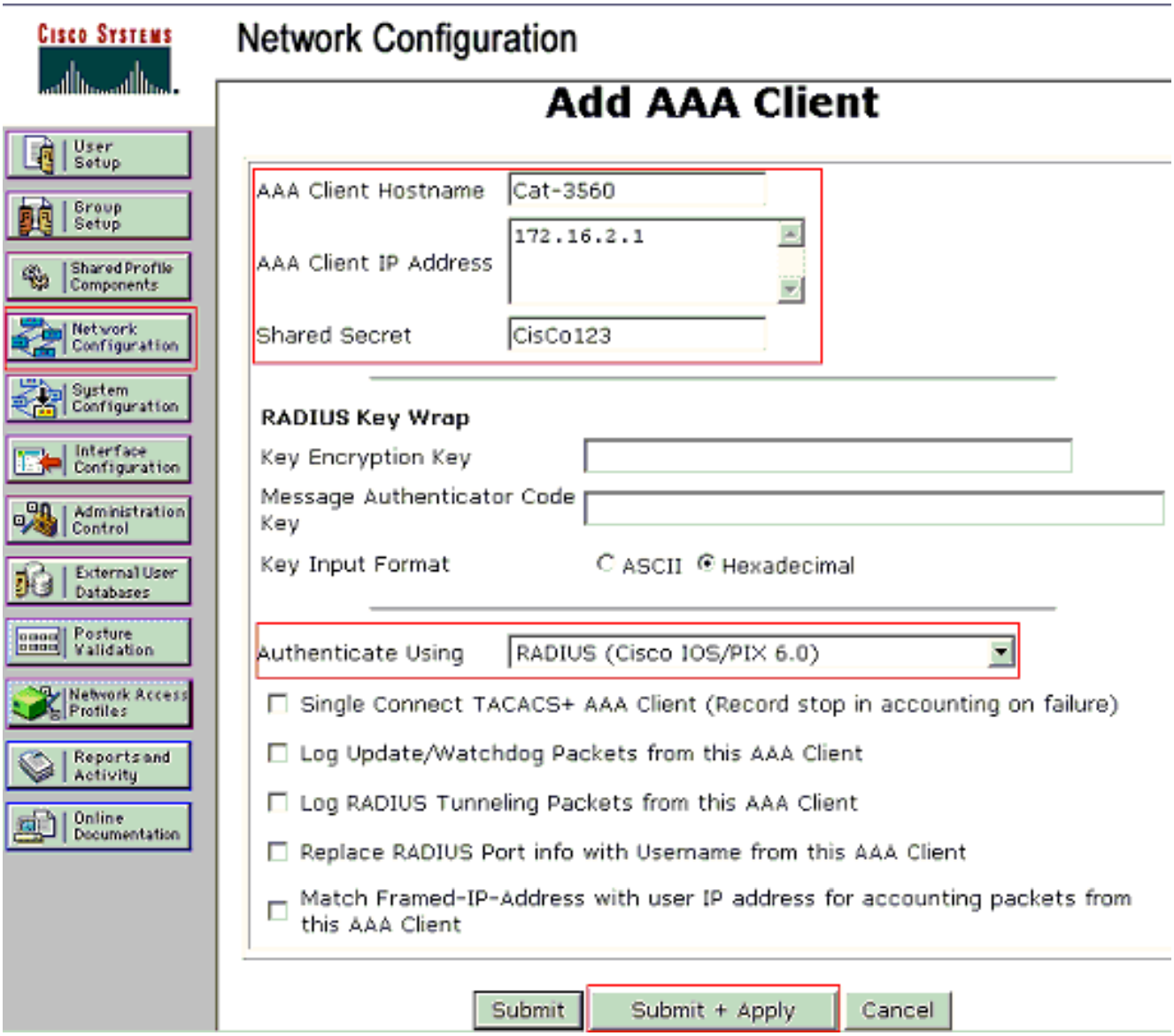
1. Haga clic la **configuración de red** en la ventana de administración ACS para configurar a un cliente AAA.
2. El tecleo **agrega la entrada** bajo sección de los clientes AAA.



3. Configure Nombre del host del cliente AAA, la dirección IP, la clave secreta compartida y el tipo de autenticación como:Nombre del 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 la operación correcta, la clave secreta compartida debe ser idéntica

en el cliente AAA y el ACS. Las claves son con diferenciación entre mayúsculas y minúsculas.Autentique usando = **RADIUS (Cisco IOS/PIX 6.0)**.**Nota:** El atributo de los pares del valor de atributo de Cisco (AV) está disponible bajo esta opción.

4. El tecleo **somete + se aplica** para realizar estos cambios eficaces, pues este ejemplo muestra:



Configuración de grupo

Refiera a esta tabla para configurar al servidor de RADIUS para la autenticación.

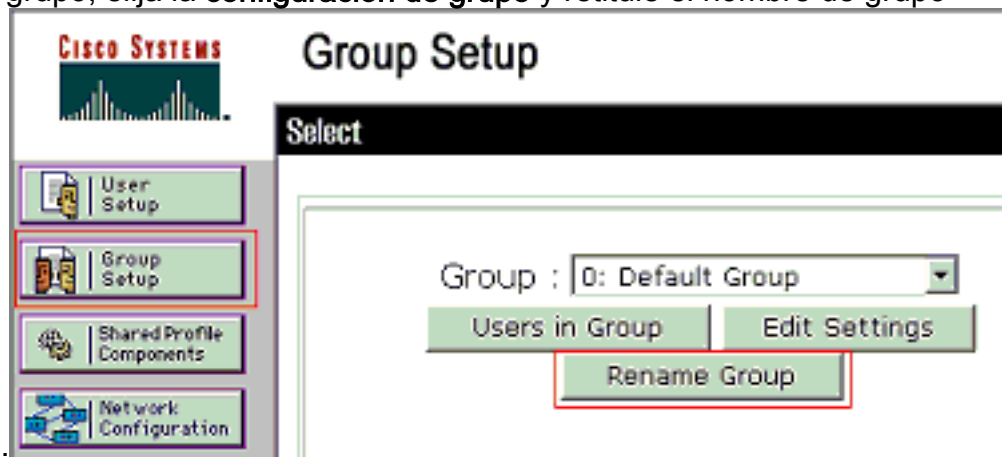
Dispositivo	Departamento	Grupo	Usuario	Contraseña	VLAN	Agrupamiento DHCP
M-1	Comercialización	Comercialización	mkt-administrador	MMcisco	COMERCIALIZACIÓN	Comercialización

M-2	Comercialización	Comercialización	mkt-personal	MScisco	COMERCIALIZACIÓN	Comercialización
S-2	Ventas	Ventas	venta-administrador	SMcisco	VENTAS	Ventas
S1	Ventas	Ventas	venta-personal	SScisco	VENTAS	Ventas
P-1	Comercialización	Teléfonos IP	CP-7970G-SEP001759E7492C	P1cisco	VOICE	Teléfonos IP
P-2	Ventas	Teléfonos IP	CP-7961G-SEP001A2F80381F	P2cisco	VOICE	Teléfonos IP

Cree a los grupos para los clientes que conectan con los VLA N 3 (VOZ), 4 (MÁRKETING) y 5 (las VENTAS). Aquí, los **Teléfonos IP de los** grupos, el **márketing** y las **ventas** son para este propósito creado.

Nota: Ésta es la configuración de los grupos del **márketing** y de los **Teléfonos IP**. Para las **ventas** configuración de grupo, complete los pasos para el **Grupo de comercialización**.

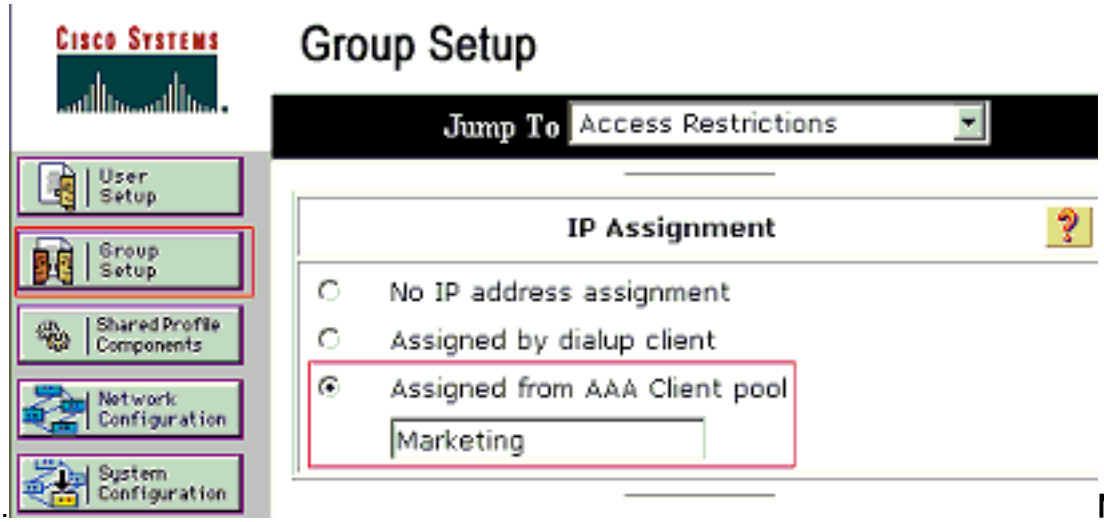
1. Para crear a un grupo, elija la **configuración de grupo** y retitule el nombre de grupo predeterminado.



2. Para configurar a un grupo, elegir al grupo de la lista y del tecleo **edite las**

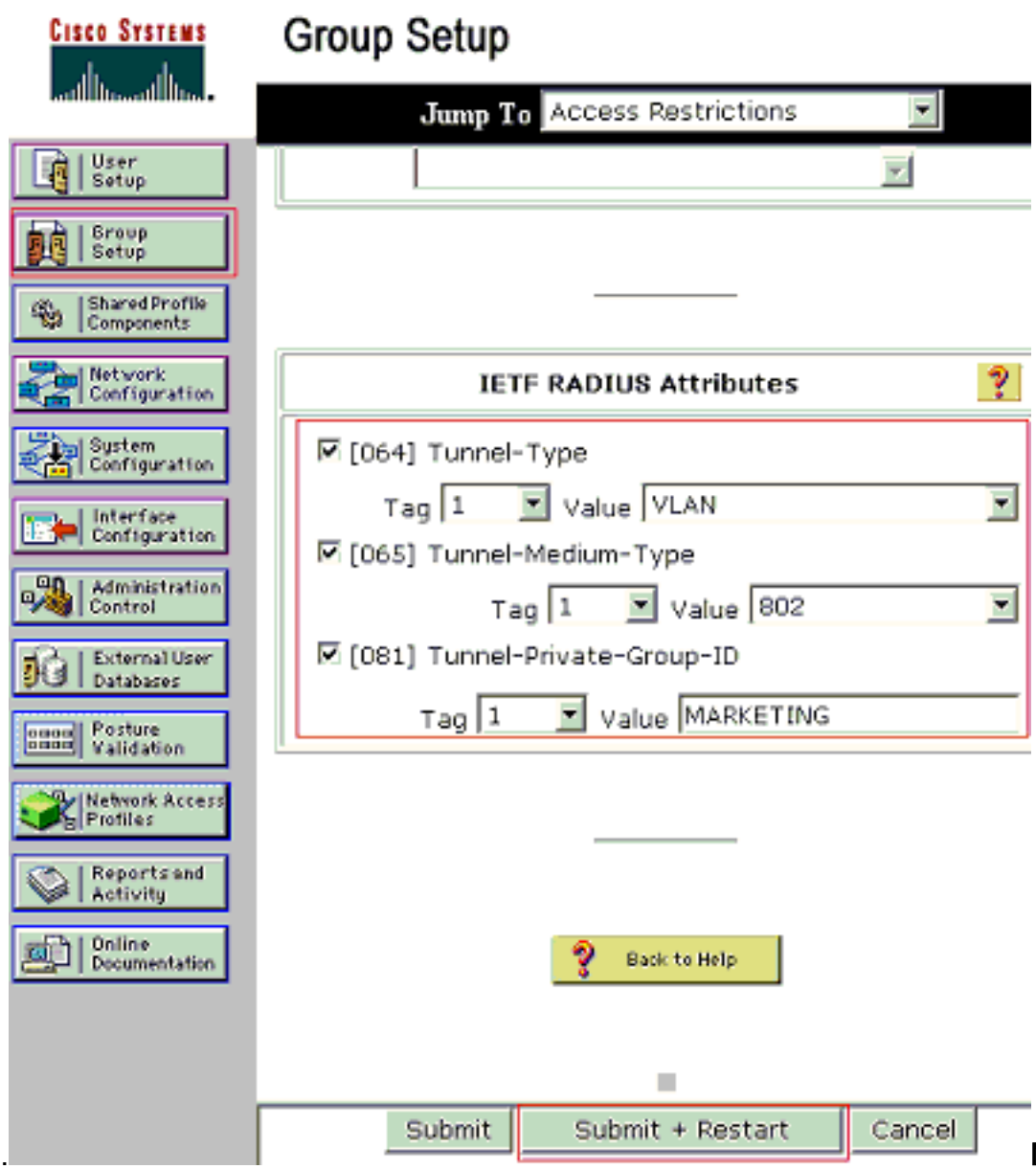
configuraciones

3. Defina la asignación de dirección IP del cliente según lo **asignado por el pool del cliente AAA**. Ingrese el nombre del pool del IP Address configurado en el Switch para los clientes de este



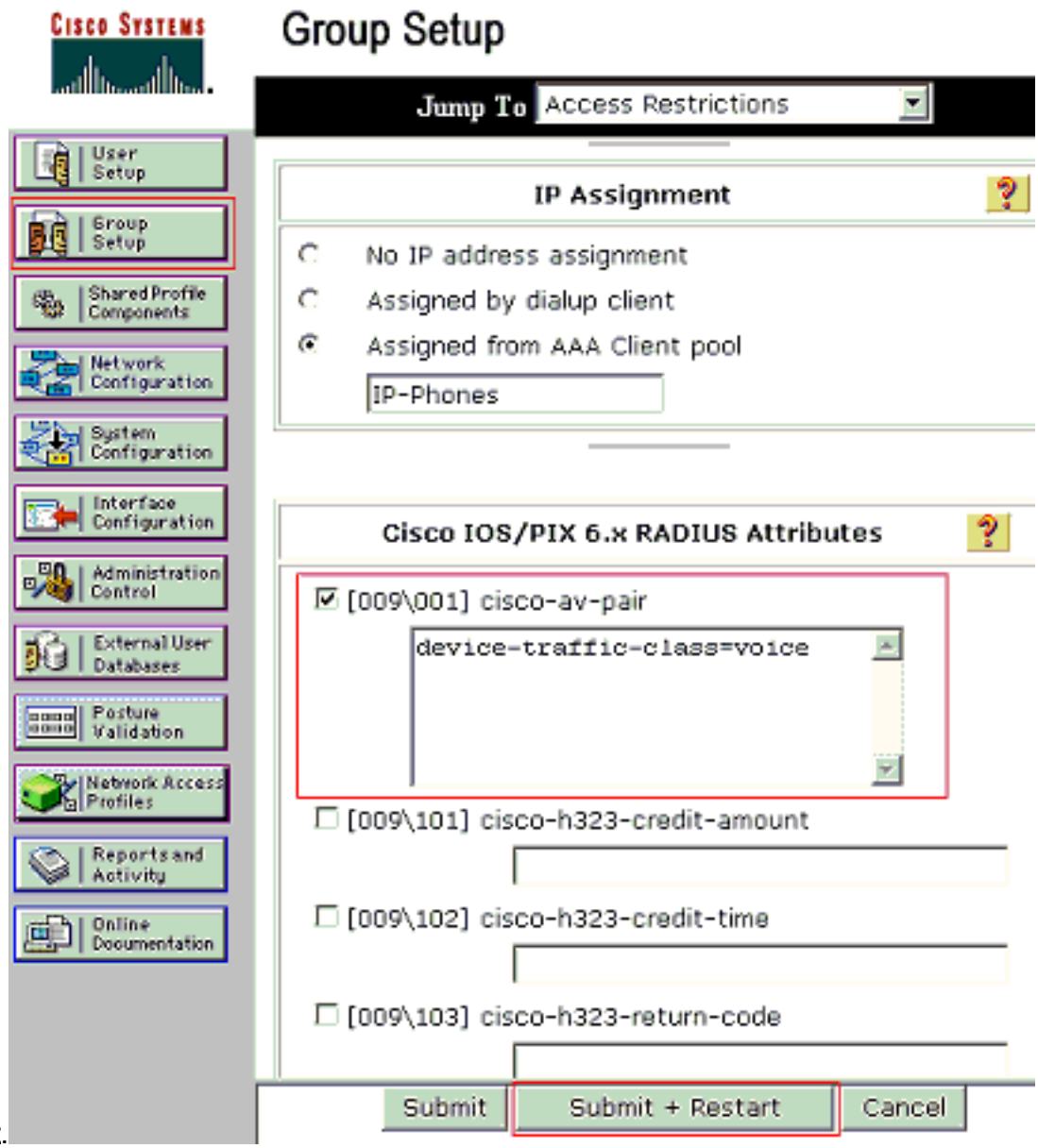
grupo. **Nota:** Elij a esta opción y teclee el nombre de la agrupación IP del cliente AAA en el cuadro, sólo si este usuario debe hacer la dirección IP asignar por un pool de la dirección IP configurado en el cliente AAA.**Nota:** Para la configuración de grupo de los **Teléfonos IP** solamente, salte el siguiente paso, el paso 4, y vaya al paso 5.

4. Defina los atributos **64**, **65** y **81 de la** Fuerza de tareas de ingeniería en Internet (IETF) (IETF) y después haga clic **Submit + Restart**.Aseegurese que las etiquetas de los valores están fijadas a **1**, pues este ejemplo muestra. El Catalyst ignora cualquier etiqueta con excepción de 1. para asignar a un usuario a un VLA N específico, usted debe también definir el atributo **81** con un *nombre* o un número VLAN del VLA N que corresponda.**Nota:** Si usted utiliza el *nombre del* VLA N, debe ser exactamente lo mismo que el que está configurado en



el Switch. **Nota:** Refiera al RFC 2868: Atributos de RADIUS para el soporte del Tunnel Protocol para más información sobre estos atributos IETF.**Nota:** En la configuración inicial del servidor ACS, los atributos IETF RADIUS pueden no poder visualizar en **configuración de usuario**. Para habilitar los atributos IETF en las pantallas de la configuración de usuario, elija la **configuración de la interfaz > RADIUS (IETF)**. Luego, verifique los atributos 64, 65 y 81 en las columnas Usuario y Grupo.**Nota:** Si usted no define el atributo **81** IETF y el puerto es un puerto del switch en el modo de acceso, asignan el cliente al VLA N del acceso del puerto. Si usted ha definido el atributo **81** para la asignación del VLAN dinámico y el puerto es un puerto del switch en el modo de acceso, usted necesita publicar el **comando radius del grupo predeterminado de la autorización de red AAA** en el Switch. Este comando asigna el puerto a la VLAN que el servidor RADIUS provee. Si no, el 802.1x mueve el puerto al estado AUTORIZADO después de la autenticación del usuario; pero el puerto todavía está en el VLAN predeterminado del puerto, y la Conectividad puede fallar.**Nota:** El siguiente paso es solamente aplicable al grupo de los **Teléfonos IP**.

5. Configure al servidor de RADIUS para enviar un atributo de los pares del valor de atributo de Cisco (AV) para autorizar un dispositivo de la Voz. Sin esto, el Switch trata el dispositivo de la Voz como dispositivo de datos. Defina el atributo de los pares del valor de atributo de Cisco (AV) con un valor del *device-traffic-class=voice* y haga clic **Submit +**

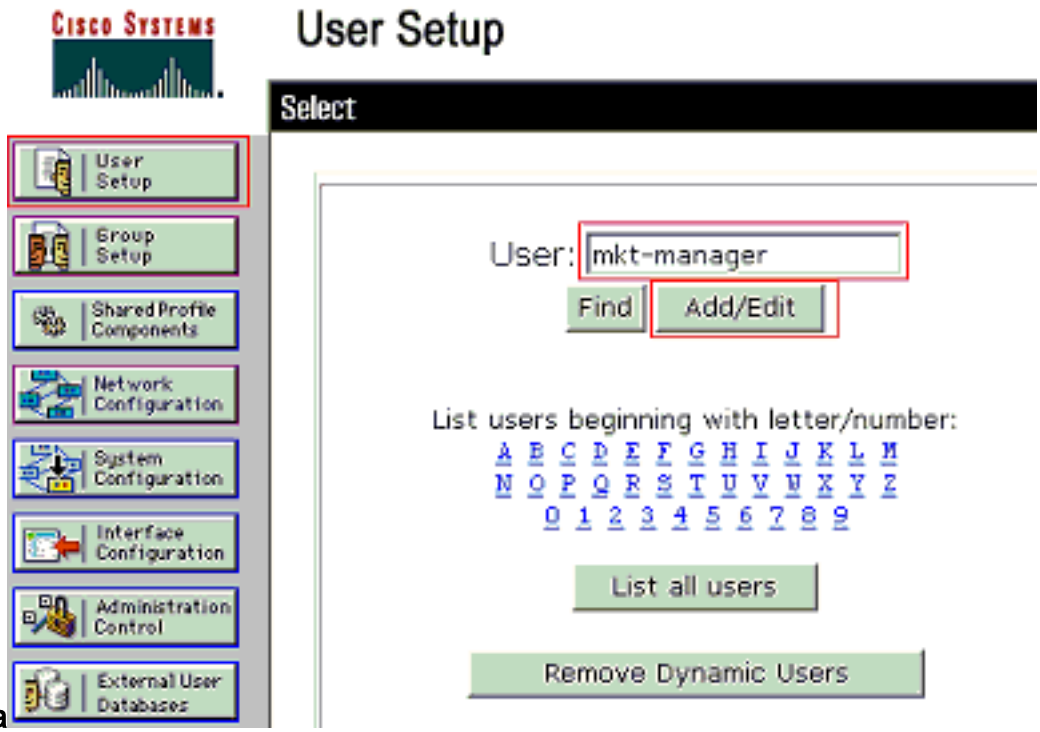


Restart.

Configuración de usuario

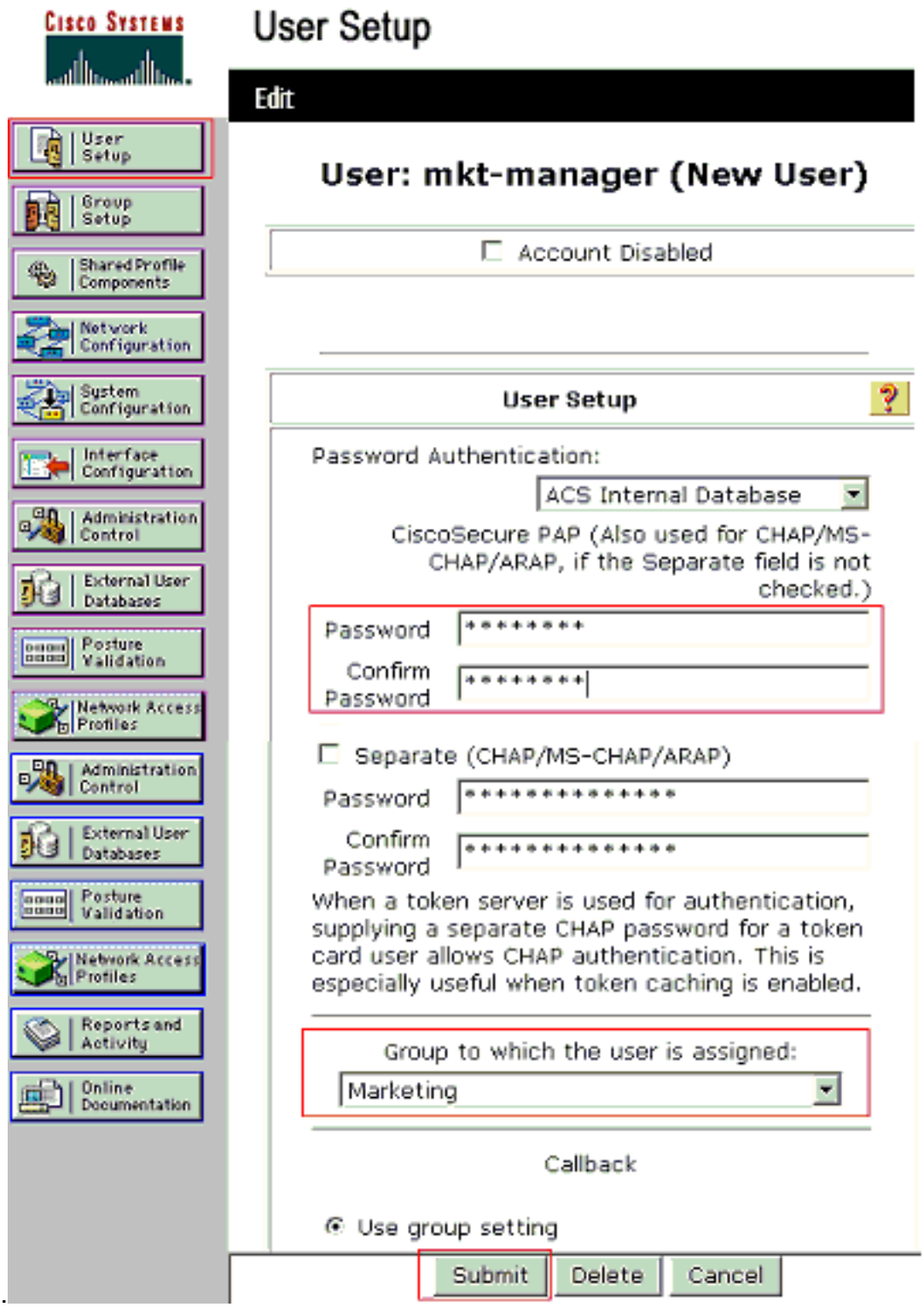
Complete estos pasos para agregar y configurar a un usuario.

1. Para agregar y configurar a los usuarios, elija la **configuración de usuario**. Ingrese el nombre de usuario y el tecleo



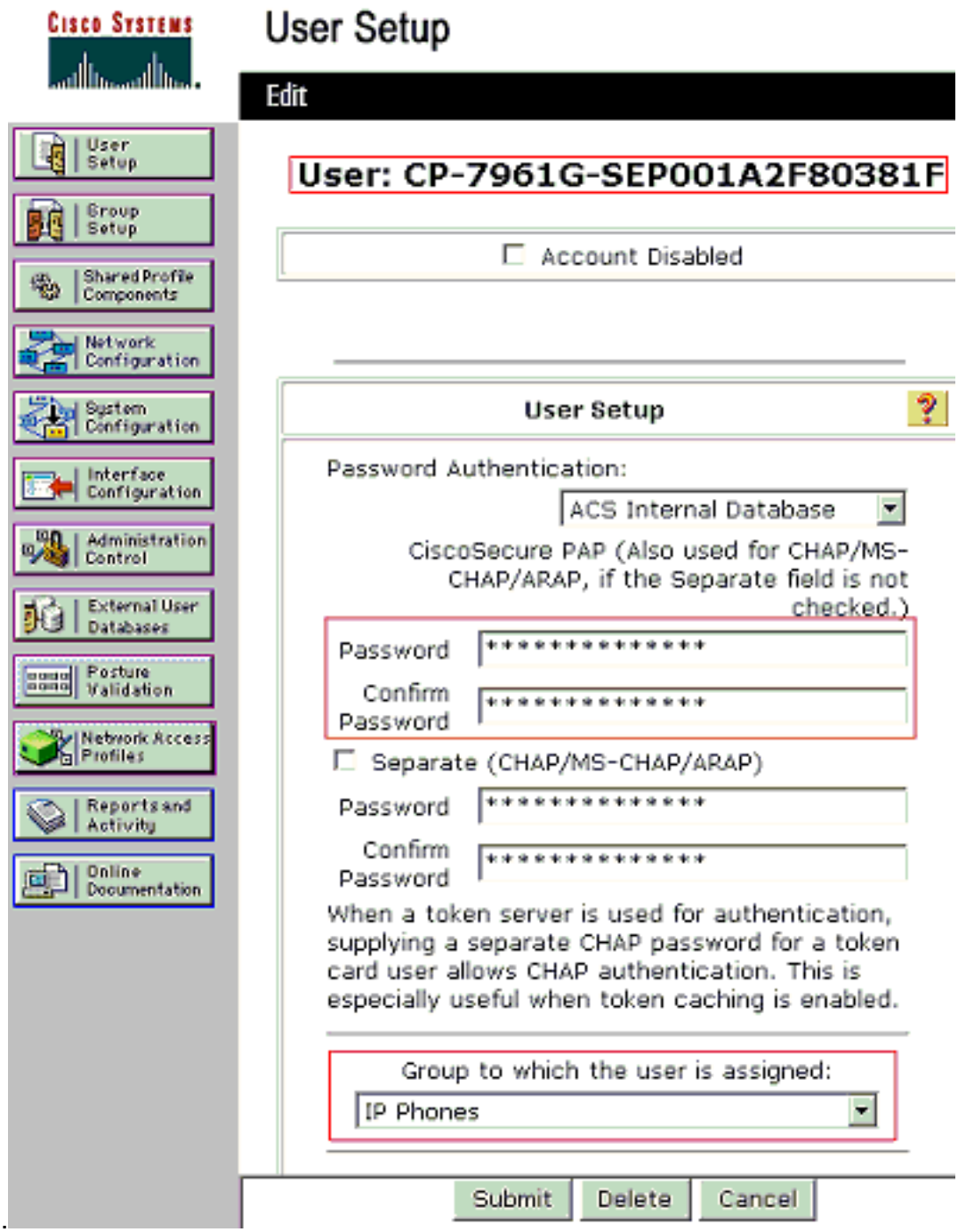
agrega/edita

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



usuario.

3. El teléfono del IP utiliza su ID del dispositivo como el nombre de usuario y el secreto compartido como la contraseña para autenticación. Estos valores deben hacer juego en el servidor de RADIUS. Para los Teléfonos IP P-1 y P-2 cree los nombres de usuario lo mismo que su ID del dispositivo y contraseña lo mismo que el secreto compartido configurado. Vea la configuración los Teléfonos IP para utilizar la sección de la autenticación del 802.1x para más información sobre el ID del dispositivo y el secreto compartido en un teléfono del

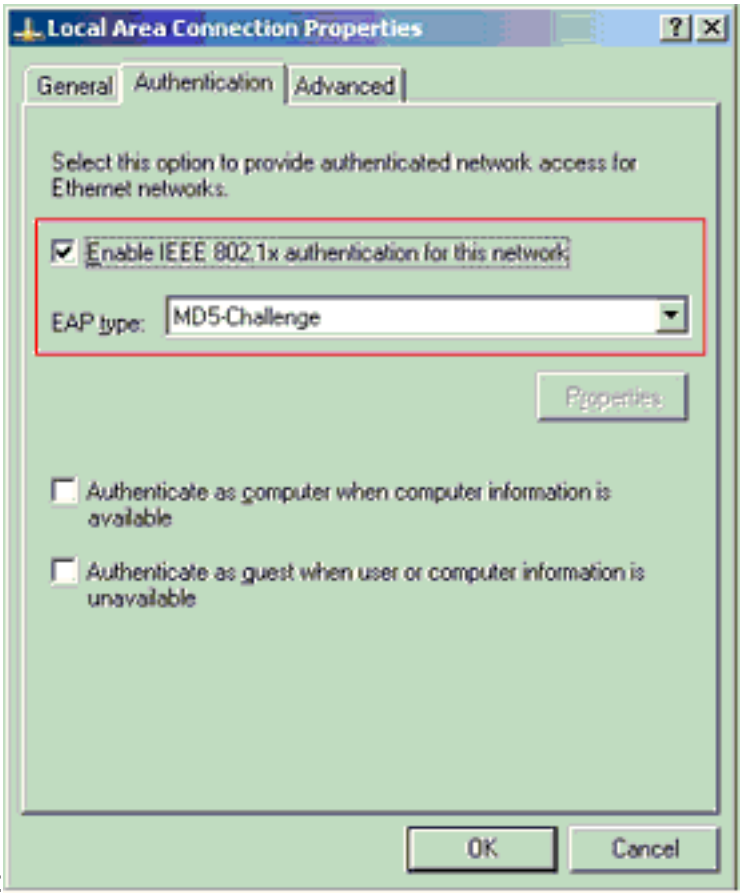


IP.

Configure a los PC cliente para utilizar la autenticación del 802.1x

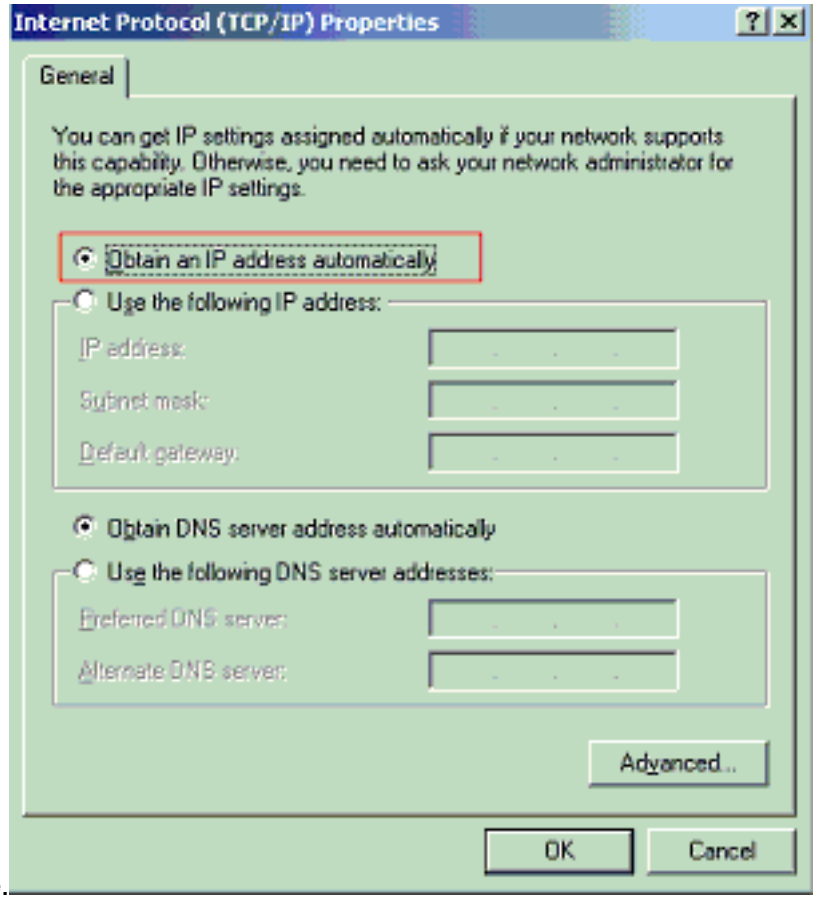
Este ejemplo es específico al Protocolo de Autenticación Extensible (EAP) del Microsoft Windows XP sobre el cliente LAN (EAPOL):

1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**, después haga clic con el botón derecho del ratón en su **conexión de área local** y elija las **propiedades**.
2. Marque el **icono de la demostración en la área de notificación cuando está conectado** conforme a 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 a los clientes para obtener la dirección IP de un servidor DHCP.

1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**, después haga clic con el botón derecho del ratón en su **conexión de área local** y elija las **propiedades**.
2. Conforme a la ficha general, haga clic el **protocolo de Internet (TCP/IP)** y entonces las **propiedades**.
3. Elija **obtienen una dirección IP**

automáticamente. 

Configure los Teléfonos IP para utilizar la autenticación del 802.1x

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

1. Presione el **botón Settings Button** para acceder las configuraciones de la **autenticación del 802.1x** y elegir la **Configuración de seguridad > la autenticación > la autenticación del dispositivo del 802.1x**.
2. Fije la opción de la **autenticación del dispositivo a habilitado**.
3. Presione la tecla programable **Save**.
4. Elija la **autenticación > el EAP-MD5 > el secreto compartido del 802.1x** para fijar una contraseña en el teléfono.
5. Ingrese el secreto compartido y presione la **salvaguardia**.**Nota:** La contraseña debe estar entre seis y 32 caracteres, que consisten en cualquier combinación de números o de cartas. `Que la clave no es aquí` mensaje `activo` se muestra y la contraseña no se guarda si esta condición no se satisface.**Nota:** Si usted inhabilita la autenticación del 802.1x o realiza una fábrica reajustada en el teléfono, se borra el secreto compartido previamente configurado MD5.**Nota:** Las otras opciones, el ID del dispositivo y el reino no pueden ser configurados. El ID del dispositivo se utiliza como el nombre de usuario para la autenticación del 802.1x. Esto es un derivado del número de modelo y de la dirección MAC única del teléfono visualizados en este formato: CP-<model>-SEP-<MAC>. Por ejemplo, **CP-7970G-SEP001759E7492C**. Refiera a las configuraciones de la autenticación del 802.1x para más información.

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

1. Presione el **botón Settings Button** para acceder las configuraciones de la **configuración de red** y elegir la **configuración de red**.

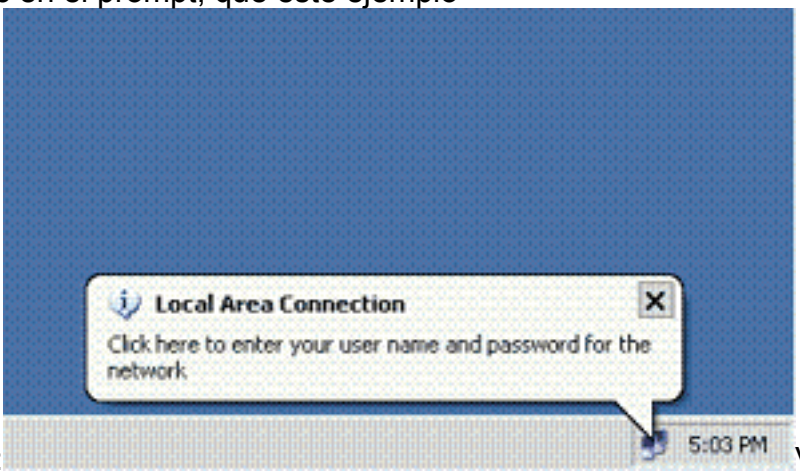
2. Desbloquee las opciones de **configuración de red**. Para desbloquear, presionar **** #.**Nota:** No presione **** # para desbloquear las opciones y después presionar inmediatamente **** # otra vez para las opciones de bloqueo. El teléfono interpreta esta secuencia como **** # ****, que reajusta el teléfono. Para opciones de bloqueo después de que usted los desbloquee, espera por lo menos 10 segundos antes de que usted presiona **** # otra vez.
3. Navegue a la opción habilitada DHCP y pulse la tecla suave del **sí** para habilitar el DHCP.
4. Presione la tecla programable **Save**.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

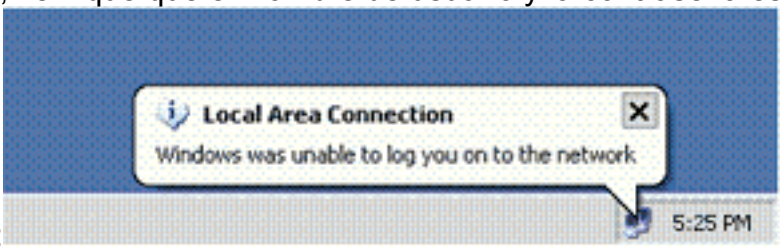
PC cliente

Si usted tiene terminado correctamente la configuración, los PC cliente visualizan un prompt del popup para ingresar un Nombre de usuario y una contraseña.

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

Visualizaciones de la ventana de un Nombre de usuario y de la entrada de contraseña.**Nota:** MDA no aplica la orden de la autenticación del dispositivo. Pero, para los mejores resultados, Cisco recomienda que un dispositivo de la Voz está autenticado antes de un dispositivo de datos en un puerto habilitado MDA.
2. Ingrese el Nombre de usuario y la

contraseña. 

3. Si aparecen ningunos mensajes de error, verifique la Conectividad con los métodos habituales, tales como acceso directo de los recursos de red y con el **ping**.**Nota:** Si aparece este error, verifique que el Nombre de usuario y la contraseña estén correctos: 

Teléfonos IP

el menú del estado de autenticación del 802.1x en los Teléfonos IP permite monitorear el estado de autenticación.

1. Presione el **botón Settings Button** para acceder el Stats en tiempo real de la autenticación del 802.1x y elegir el **estado de autenticación de la Configuración de seguridad > del 802.1x**.
2. **El estatus de transacción** debe **ser autenticado**. Refiera al estatus en tiempo real de la autenticación del 802.1x para más información.**Nota:** El estado de autenticación puede también ser verificado de las **configuraciones > del estatus > de los mensajes de estado**.

Switch de la capa 3

Si la contraseña y el Nombre de usuario aparecen estar correctos, verifique al estado de puerto del 802.1x en el Switch.

1. Busque un estado del puerto que indique `AUTORIZADO.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 satisfactoria.`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 DHCP que ata el estatus después de una autenticación satisfactoria.`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.

Troubleshooting

La autenticación del teléfono del IP falla

Se muestra el estados del teléfono del IP `que configuran el IP` o `que se registran` si la autenticación del 802.1x falla. Complete estos pasos para resolver problemas esto publica:

- Confirme que el 802.1x está habilitado en el teléfono del IP.
- Verifique que usted tenga el ID del dispositivo ingresado en el servidor de la autenticación (RADIO) como el nombre de usuario.
- Confirme que el secreto compartido está configurado en el teléfono del IP.
- Si se configura el secreto compartido, verifique que usted tenga el mismo secreto compartido ingresado en el servidor de autenticación.
- Verifique que usted haya configurado correctamente los otros dispositivos requeridos, por ejemplo, el Switch y al servidor de autenticación.

Información Relacionada

- Configurar la autenticación del acceso basado del IEEE 802.1X
- Configure el teléfono del IP para utilizar la autenticación del 802.1x
- Guías de consulta para el despliegue del Cisco Secure ACS para los servidores de Windows Nt/2000 en un entorno del Switch del Cisco Catalyst
- RFC 2868: Atributos de RADIUS para soporte a protocolo de túnel
- Autenticación del IEEE 802.1X con el Catalyst 6500/6000 que funciona con el ejemplo de configuración del Cisco IOS Software
- Autenticación del IEEE 802.1X con el Catalyst 6500/6000 que funciona con el ejemplo de

configuración del software CatOS
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems