Ejemplo de Configuración de Autenticación IEEE 802.1x con Catalyst 6500/6000 que Ejecuta el Software CatOS

Contenido

Introducción

Este documento explica cómo configurar IEEE 802.1x en un Catalyst 6500/6000 que se ejecuta en modo híbrido (CatOS en la Supervisor Engine y Cisco IOS® Software en MSFC) y un servidor de Servicio de Autenticación Remota Telefónica de Usuario (RADIUS) para la autenticación y asignación VLAN.

Prerequisites

Requirements

Quienes lean este documento deben tener conocimiento de los siguientes temas:

- Guía de instalación de Cisco Secure ACS para Windows 4.1
- Guía del usuario de Cisco Secure Access Control Server 4.1
- ¿Cómo funciona RADIUS?
- Guía de implementación de Catalyst Switching y ACS

Componentes Utilizados

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

- Catalyst 6500 que ejecuta CatOS Software Release 8.5(6) en Supervisor Engine y Cisco IOS Software Release 12.2(18)SXF en MSFC**Nota:** Necesita CatOS Release 6.2 o posterior para soportar la autenticación basada en puerto 802.1x.**Nota:** Antes de la versión de software 7.2(2), una vez que se autentica el host 802.1x, se une a una VLAN configurada con NVRAM. Con la versión de software 7.2(2) y posteriores, después de la autenticación, un host 802.1x puede recibir su asignación de VLAN del servidor RADIUS.
- 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.

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.

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 servidor de cliente 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 poner a disposición cualquier servicio ofrecido por el switch o la LAN. Hasta que se autentique el dispositivo, el control de acceso 802.1x solo permite el tráfico de protocolo de autenticación extensible (EAP) 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.

Configurar

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

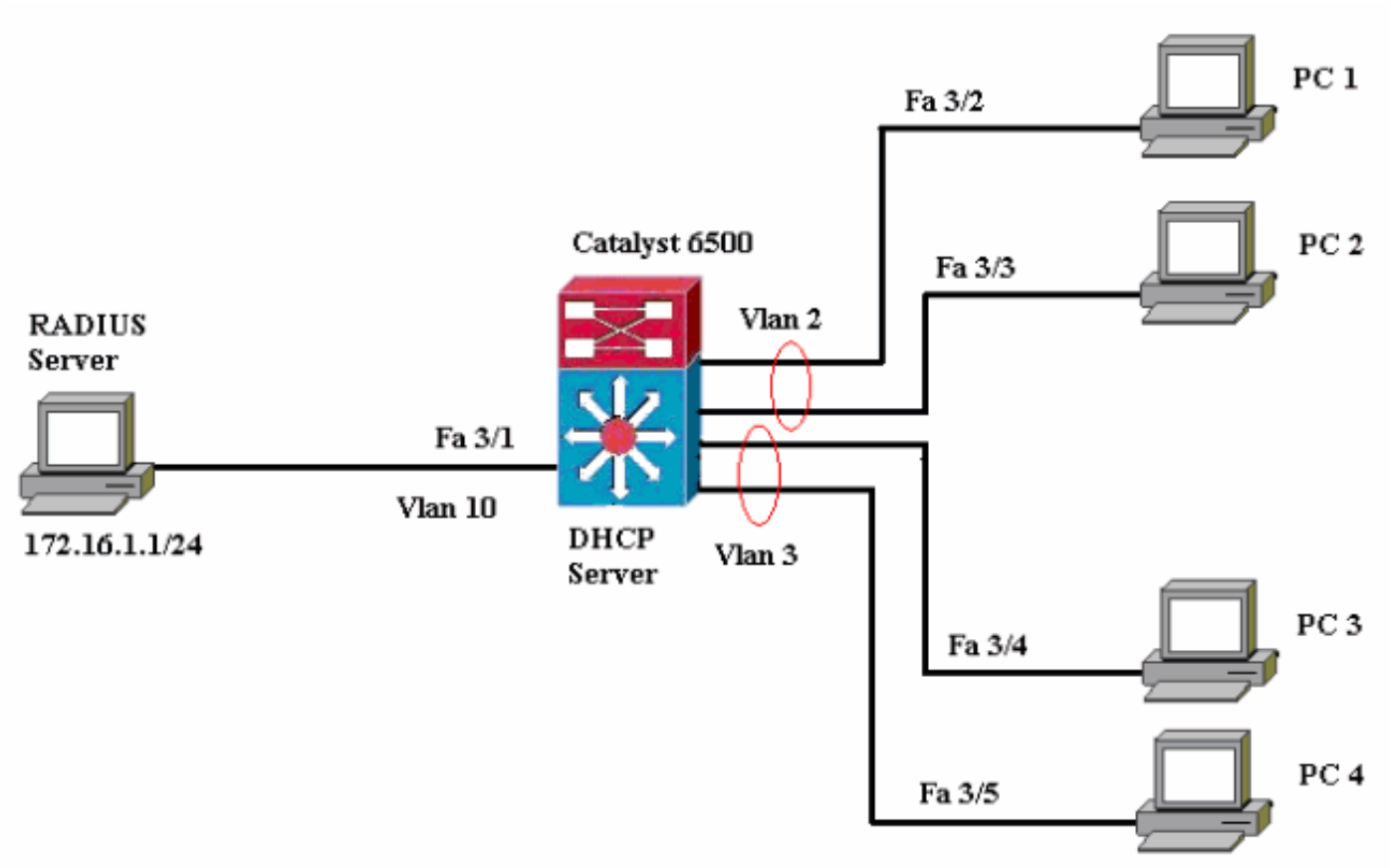
Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

La configuración requiere estos pasos:

- Configuración del switch Catalyst para la autenticación 802.1x
- Configuración del servidor RADIUS
- Configuración de los clientes de PC para utilizar la autenticación 802.1x

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 servidor RADIUS se configura para la autenticación y la asignación de VLAN.
- 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, solicitando información de identidad del cliente, verificando esa información con el servidor RADIUS y reenviando una respuesta al cliente. Aquí, el switch Catalyst 6500 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 mediante la adición de la identidad de usuario autenticada en el proceso de detección de DHCP.
- Clientes: los dispositivos (estaciones de trabajo) que solicitan acceso a los servicios LAN y de switch y responden a las solicitudes del switch. Aquí, los PC 1 a 4 son los clientes que solicitan un acceso de red autenticado. Los PC 1 y 2 utilizarán la misma credencial de inicio de sesión para estar en la VLAN 2. De manera similar, los PC 3 y 4 utilizarán una credencial de inicio de sesión para la VLAN 3. Los clientes PC se configuran para obtener la dirección IP de un servidor DHCP.**Nota:** En esta configuración, a cualquier cliente que falle la autenticación o a cualquier cliente que no sea compatible con 802.1x que se conecte al

switch se le niega el acceso a la red al moverlos a una VLAN no utilizada (VLAN 4 o 5) usando la falla de autenticación y las funciones de VLAN de invitado.

Configuración del switch Catalyst para la autenticación 802.1x

Esta configuración de switch de ejemplo incluye:

- Habilite la autenticación 802.1x y las funciones asociadas en los puertos FastEthernet.
- Conecte el servidor RADIUS a la VLAN 10 detrás del puerto FastEthernet 3/1.
- Configuración del servidor DHCP para dos grupos IP, uno para clientes en VLAN 2 y otro para clientes en VLAN 3.
- Routing entre VLAN para tener conectividad entre clientes después de la autenticación.

Refiérase a Pautas de Configuración de Autenticación para ver las pautas sobre cómo configurar la autenticación 802.1x.

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

Catalyst 6500

```
Console (enable) set system name Cat6K
System name set.
!--- Sets the hostname for the switch. Cat6K> (enable)
set localuser user admin password cisco
Added local user admin.
Cat6K> (enable) set localuser authentication enable
LocalUser authentication enabled
!--- Uses local user authentication to access the
switch. Cat6K> (enable) set vtp domain cisco
VTP domain cisco modified
!--- Domain name must be configured for VLAN
configuration. Cat6K> (enable) set vlan 2 name VLAN2
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 2 configuration successful
!--- VLAN should be existing in the switch !--- for a
successful authentication. Cat6K> (enable) set vlan 3
name VLAN3
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 3 configuration successful
!--- VLAN names will be used in RADIUS server for VLAN
assignment. Cat6K> (enable) set vlan 4 name
AUTHFAIL_VLAN
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 4 configuration successful
!--- A VLAN for non-802.1x capable hosts. Cat6K>
(enable) set vlan 5 name GUEST_VLAN
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 4 configuration successful
!--- A VLAN for failed authentication hosts. Cat6K>
(enable) set vlan 10 name RADIUS_SERVER
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 10 configuration successful
!--- This is a dedicated VLAN for the RADIUS Server.
Cat6K> (enable) set interface sc0 10 172.16.1.2
```

```
255.255.255.0
Interface sc0 vlan set, IP address and netmask set.
!--- Note: 802.1x authentication always uses the !---
sc0 interface as the identifier for the authenticator !-
-- when communicating with the RADIUS server.

Cat6K> (enable) set vlan 10 3/1
VLAN 10 modified.
VLAN 1 modified.
VLAN  Mod/Ports
---- ----------------------
10    3/1
!--- Assigns port connecting to RADIUS server to VLAN
10. Cat6K> (enable) set radius server 172.16.1.1 primary
172.16.1.1 with auth-port 1812 acct-port 1813
added to radius server table as primary server.
!--- Sets the IP address of the RADIUS server. Cat6K>
(enable) set radius key cisco
Radius key set to cisco
!--- The key must match the key used on the RADIUS
server. Cat6K> (enable) set dot1x system-auth-control
enable
dot1x system-auth-control enabled.
Configured RADIUS servers will be used for dot1x
authentication.
!--- Globally enables 802.1x. !--- You must specify at
least one RADIUS server before !--- you can enable
802.1x authentication on the switch. Cat6K> (enable) set
port dot1x 3/2-48 port-control auto
Port 3/2-48 dot1x port-control is set to auto.
Trunking disabled for port 3/2-48 due to Dot1x feature.
Spantree port fast start option enabled for port 3/2-48.
!--- Enables 802.1x on all FastEthernet ports. !--- This
disables trunking and enables portfast automatically.
Cat6K> (enable) set port dot1x 3/2-48 auth-fail-vlan 4
Port 3/2-48 Auth Fail Vlan is set to 4
!--- Ports will be put in VLAN 4 after three !--- failed
authentication attempts. Cat6K> (enable) set port dot1x
3/2-48 guest-vlan 5
Ports 3/2-48 Guest Vlan is set to 5
!--- Any non-802.1x capable host connecting or 802.1x !-
-- capable host failing to respond to the username and
password !--- authentication requests from the
Authenticator is placed in the !--- guest VLAN after 60
seconds. !--- Note: An authentication failure VLAN is
independent !--- of the guest VLAN. However, the guest
VLAN can be the same !--- VLAN as the authentication
failure VLAN. If you do not want to !--- differentiate
between the non-802.1x capable hosts and the !---
authentication failed hosts, you can configure both
hosts to !--- the same VLAN (either a guest VLAN or an
authentication failure VLAN). !--- For more information,
refer to !--- Understanding How 802.1x Authentication
for the Guest VLAN Works. Cat6K> (enable) switch console
Trying Router-16...
Connected to Router-16.
Type ^C^C^C to switch back...
!--- Transfers control to the routing module (MSFC).
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#interface vlan 10
Router(config-if)#ip address 172.16.1.3 255.255.255.0
```

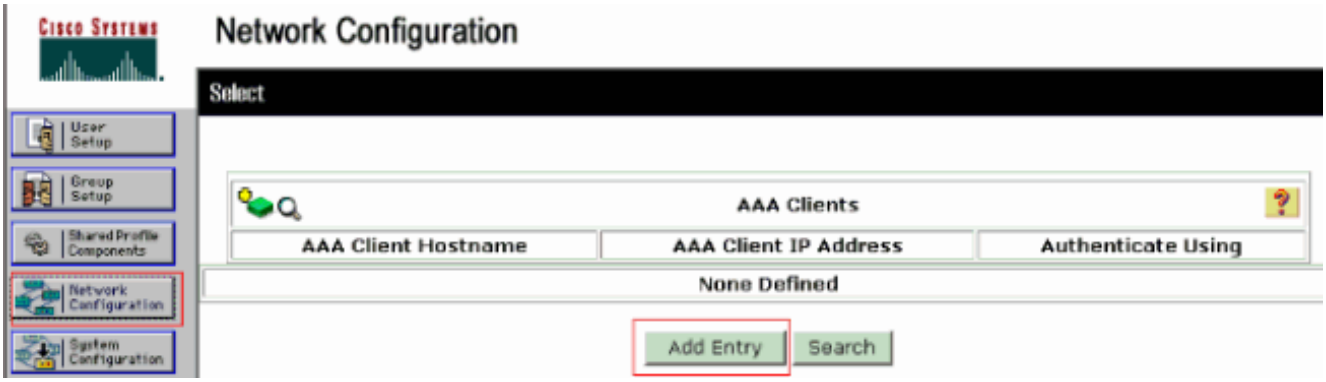
```
!--- This is used as the gateway address in RADIUS
server. Router(config-if)#no shut
Router(config-if)#interface vlan 2
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Router(config-if)#interface vlan 3
Router(config-if)#ip address 172.16.3.1 255.255.255.0
Router(config-if)#no shut
!--- This is the gateway address for clients in VLAN 3.
Router(config-if)#exit
Router(config)#ip dhcp pool vlan2_clients
Router(dhcp-config)#network 172.16.2.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.2.1
!--- This pool assigns ip address for clients in VLAN 2.
Router(dhcp-config)#ip dhcp pool vlan3_clients
Router(dhcp-config)#network 172.16.3.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.3.1
!--- This pool assigns ip address for clients in VLAN 3.
Router(dhcp-config)#exit
Router(config)#ip dhcp excluded-address 172.16.2.1
Router(config)#ip dhcp excluded-address 172.16.3.1
!--- In order to go back to the Switching module, !---
enter Ctrl-C three times. Router# Router#^C Cat6K>
(enable) Cat6K> (enable) show vlan VLAN Name Status
IfIndex Mod/Ports, Vlans ---- ------------------ -------
-- ------- ------------------------ 1    default
active    6       2/1-2

3/2-48
2    VLAN2                            active    83
3    VLAN3                            active    84
4    AUTHFAIL_VLAN                    active    85
5    GUEST_VLAN                       active    86
10   RADIUS_SERVER                    active    87
3/1
1002 fddi-default                     active    78
1003 token-ring-default               active    81
1004 fddinet-default                  active    79
1005 trnet-default                    active    80
!--- Output suppressed. !--- All active ports will be in
VLAN 1 (except 3/1) before authentication. Cat6K>
(enable) show dot1x
PAE Capability             Authenticator Only
Protocol Version           1
system-auth-control        enabled
max-req                    2
quiet-period               60 seconds
re-authperiod              3600 seconds
server-timeout             30 seconds
shutdown-timeout           300 seconds
supp-timeout               30 seconds
tx-period                  30 seconds
!--- Verifies dot1x status before authentication. Cat6K>
(enable)
```

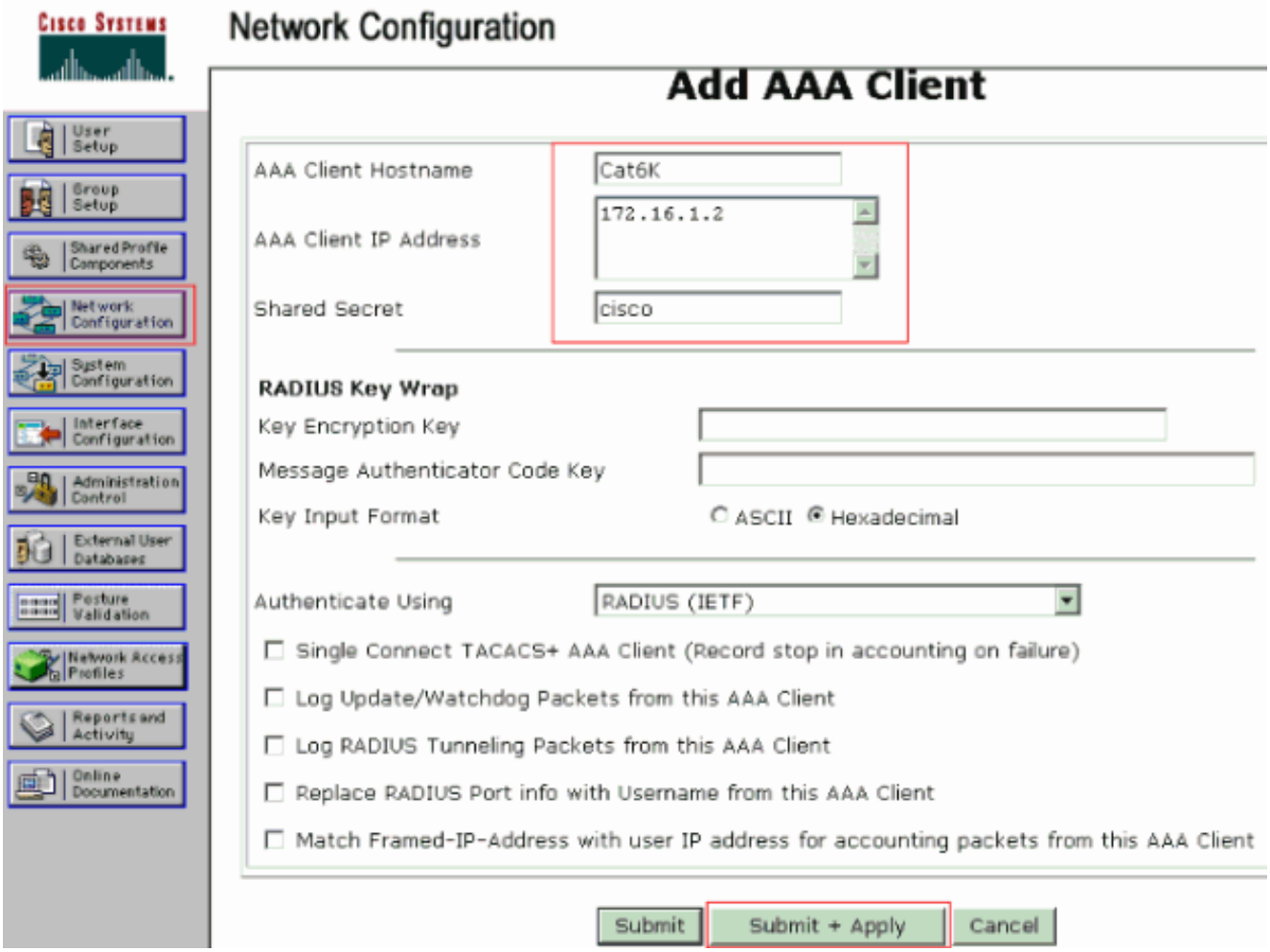
Configuración del servidor RADIUS

El servidor RADIUS se configura con una dirección IP estática de 172.16.1.1/24. Complete estos pasos para configurar el servidor RADIUS para un cliente AAA:

1. Para configurar un cliente AAA, haga clic en **Configuración de Red** en la ventana de administración ACS.
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 (**Cat6K**).Dirección IP del cliente AAA = Dirección IP de la interfaz de administración (sc0)del switch (**172.16.1.2**).Secreto compartido = Clave RADIUS configurada en el switch (**cisco**).Autentique Usando = **RADIUS IETF**.**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.
4. Haga clic en **Enviar + Aplicar** para que estos cambios sean efectivos, como muestra este ejemplo:

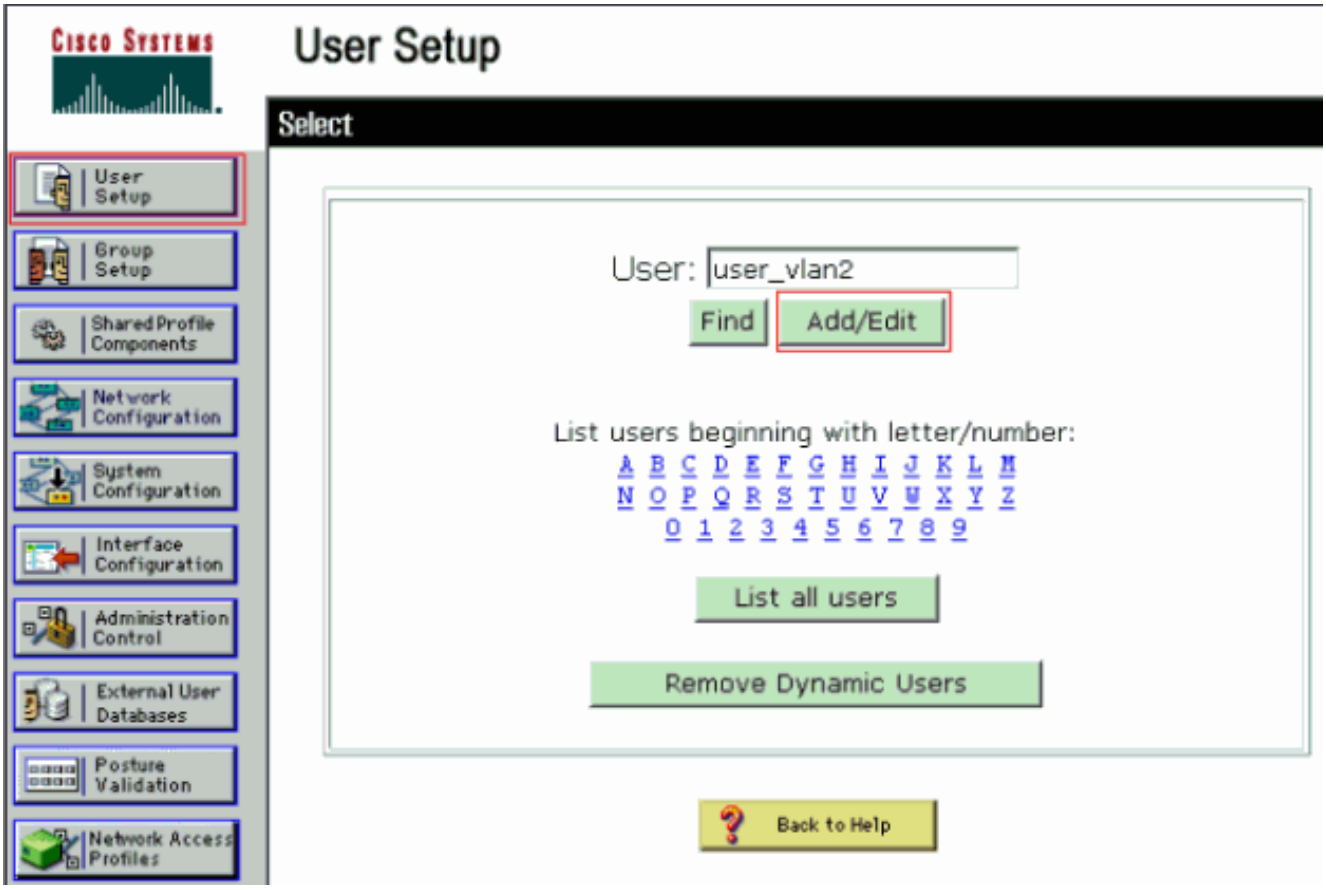


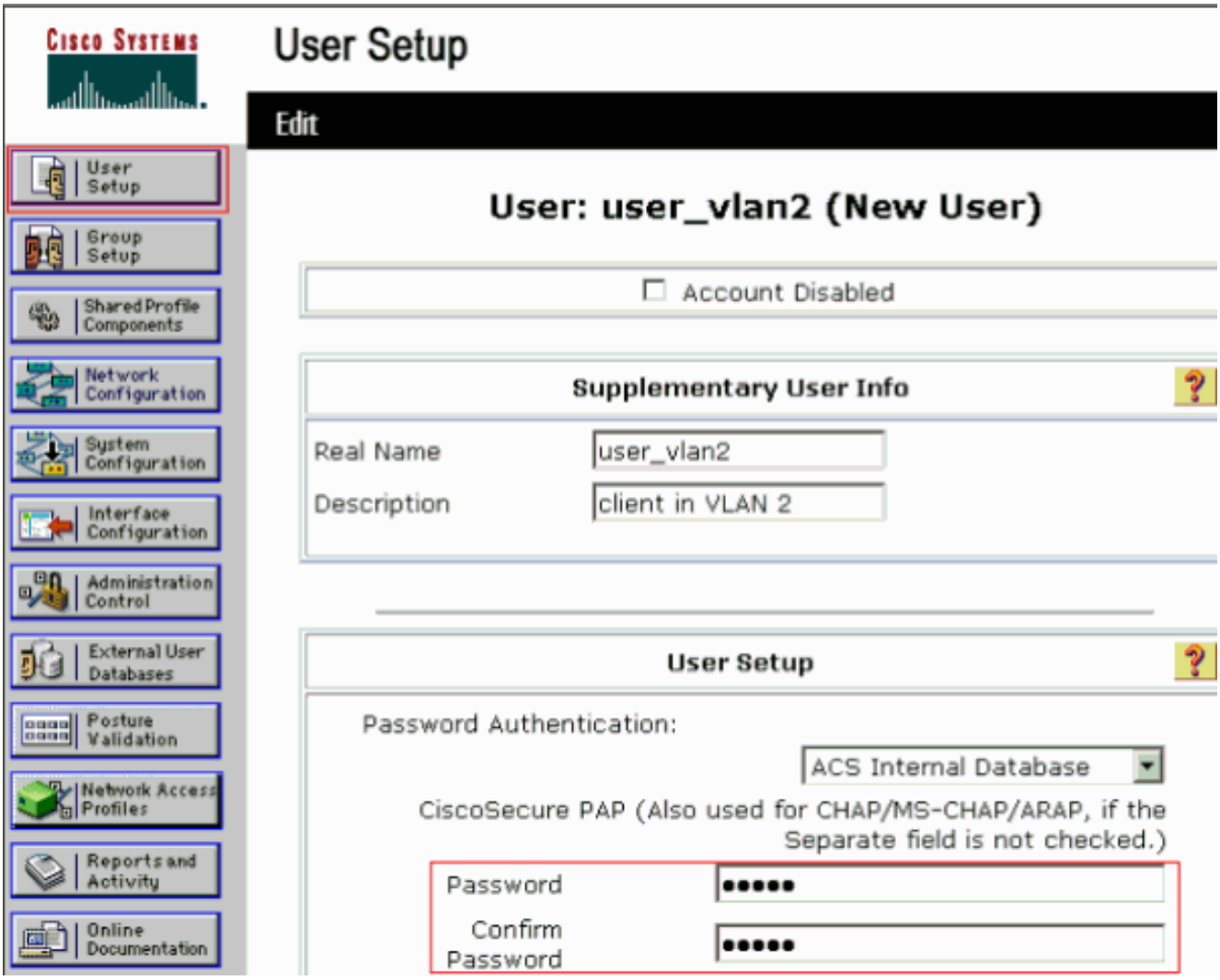
Complete estos pasos para configurar el servidor RADIUS para la autenticación, VLAN y la asignación de dirección IP:

Se deben crear dos nombres de usuario por separado para los clientes que se conectan a VLAN 2 y para VLAN 3. Aquí, se crea un usuario **user_vlan2** para los clientes que se conectan a VLAN 2 y otro usuario **user_vlan3** para los clientes que se conectan a VLAN 3 con este fin.

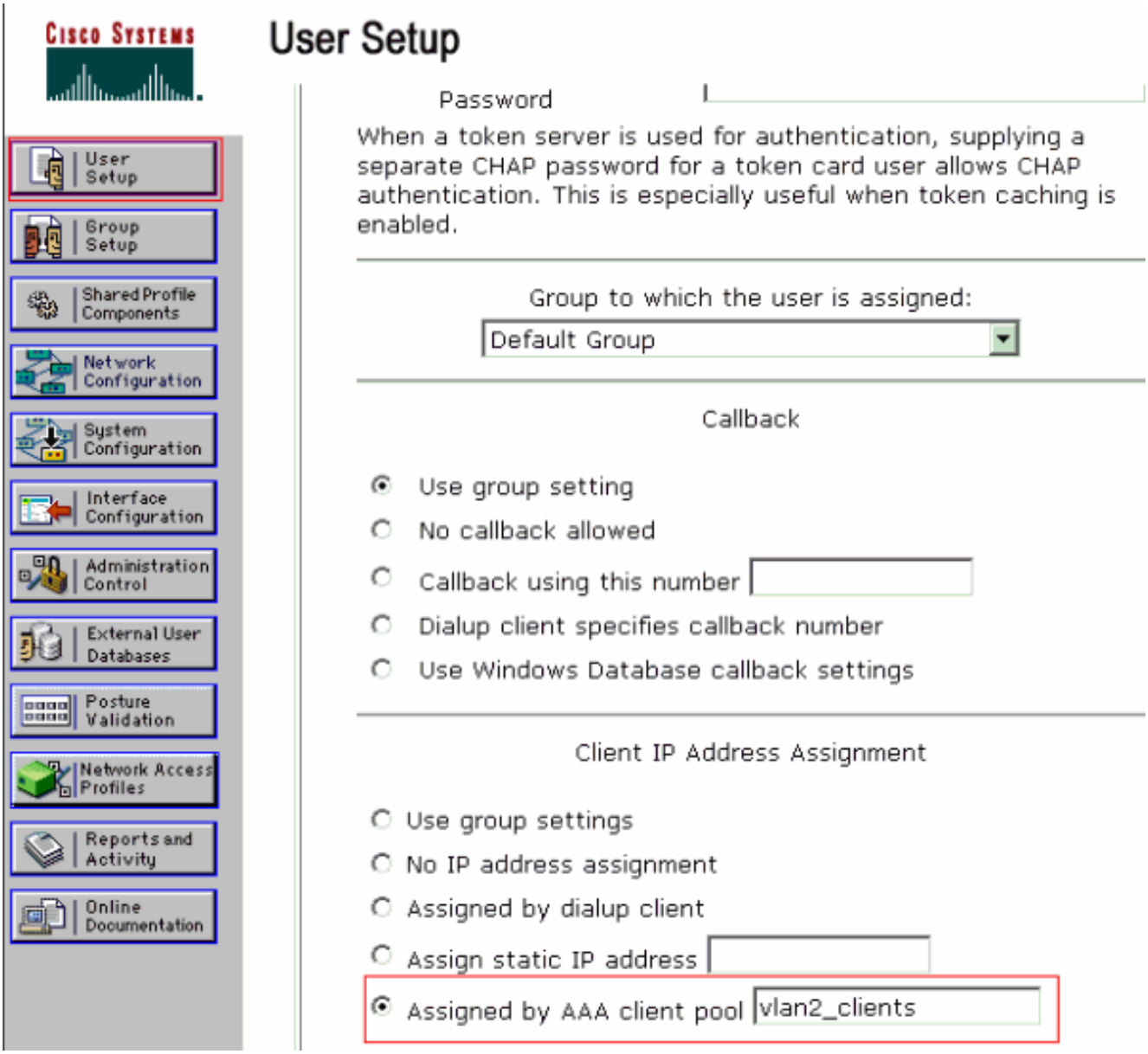
Nota: Aquí, se muestra la configuración del usuario para los clientes que se conectan sólo a VLAN 2. Para los usuarios que se conectan a VLAN 3, complete el mismo procedimiento.

1. Para agregar y configurar usuarios, haga clic en **User Setup** y defina el nombre de usuario y la
contraseña.



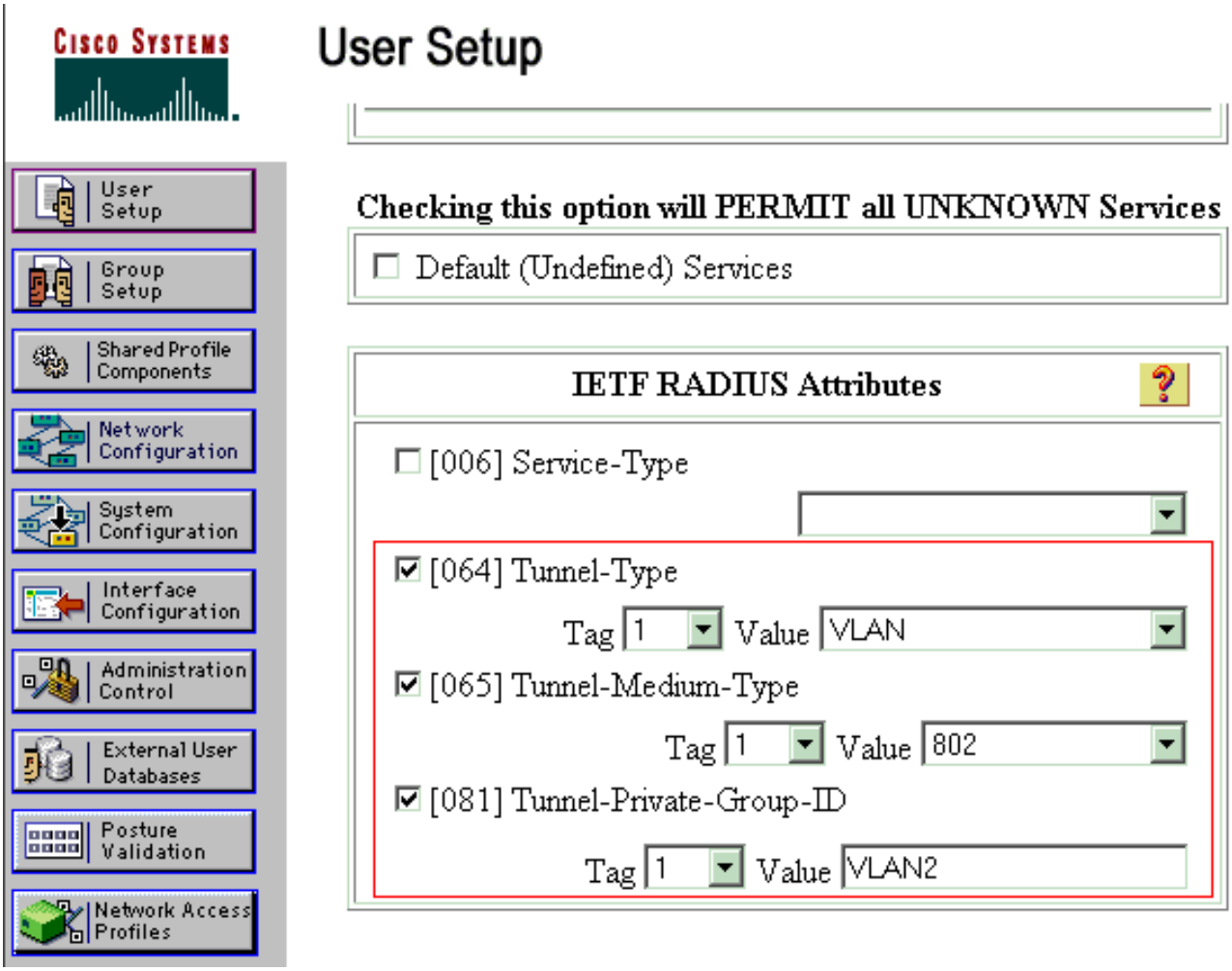


2. Defina la asignación de dirección IP del cliente como **Asignado por el conjunto de clientes AAA**. Introduzca el nombre del conjunto de direcciones IP configurado en el switch para los clientes VLAN
2.



Nota: Seleccione 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.

3. Defina los atributos 64 y 65 de Internet Engineering Task Force (IETF).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 que corresponda.**Nota:** El *nombre* de VLAN debe ser exactamente igual al configurado en el switch.**Nota:** La asignación de VLAN basada en el *número* VLAN no se soporta con CatOS.



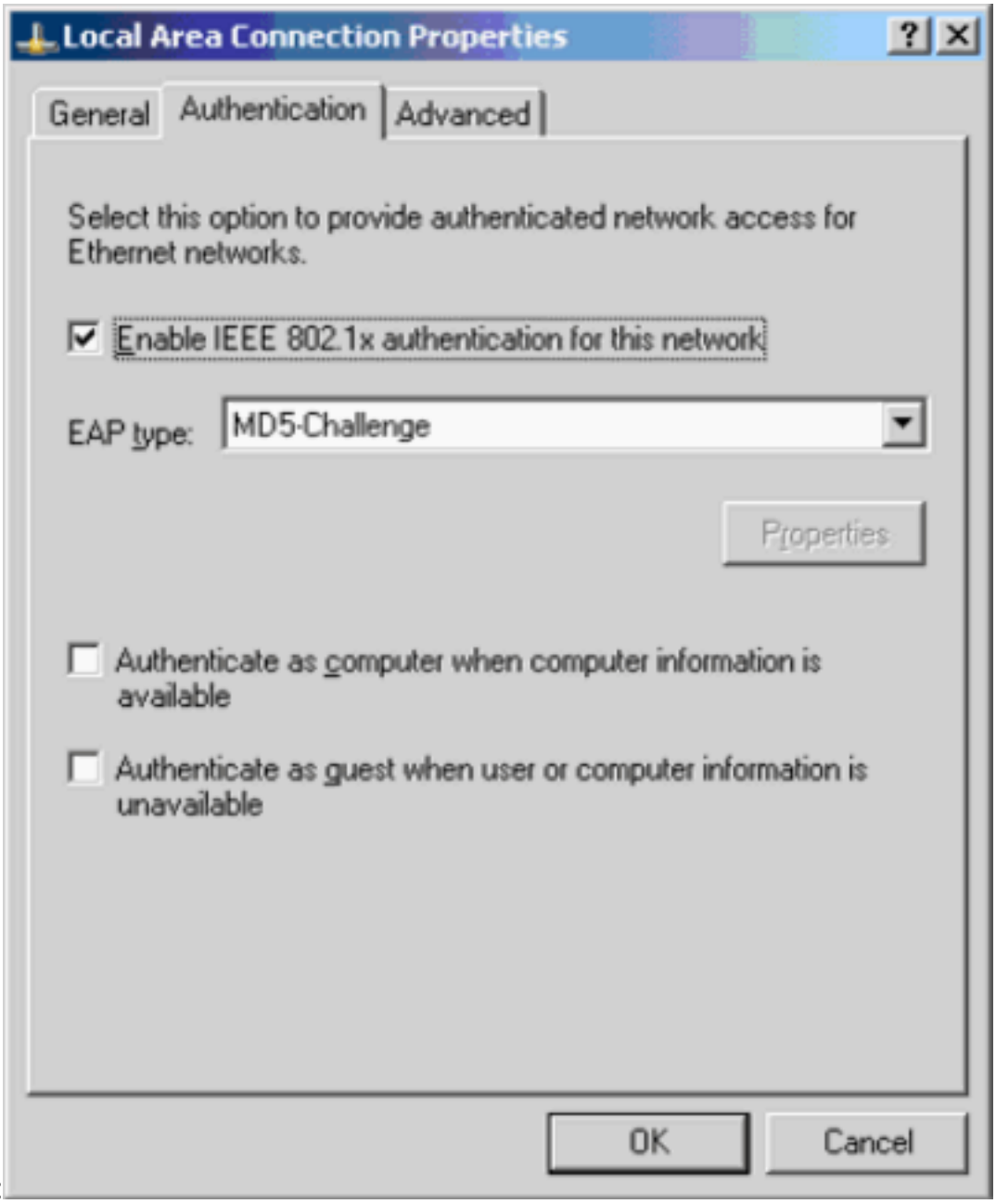
Refiérase a RFC 2868: Atributos RADIUS para el Soporte del Protocolo de Túnel para obtener más información sobre estos atributos IETF.**Nota:** En la configuración inicial del servidor ACS, los atributos RADIUS de IETF pueden no mostrarse en la **Configuración de usuario**. Elija **Interface configuration > RADIUS (IETF)** para habilitar los atributos IETF en la pantalla de configuración del usuario. Luego, verifique los atributos 64, 65 y 81 en las columnas Usuario y Grupo.

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

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

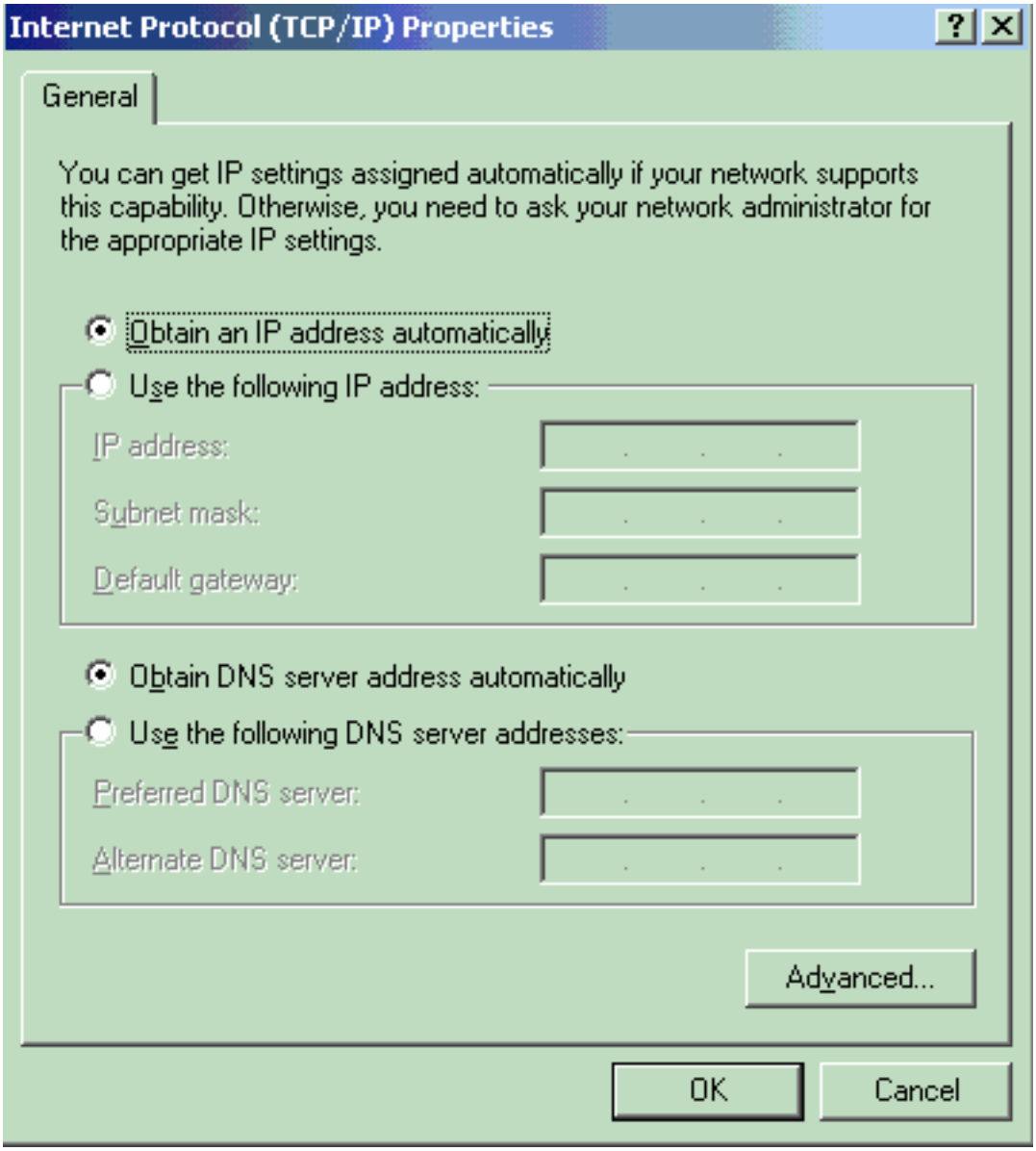
1. Elija **Inicio > Panel de control > Conexiones de red**, luego haga clic con el botón derecho en su **Conexión de área local** y elija **Propiedades**.
2. Marque **Mostrar icono en el área de notificación cuando esté conectado** en la ficha General.
3. En la ficha Authentication (Autenticación), marque 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 una 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**.



Verificación

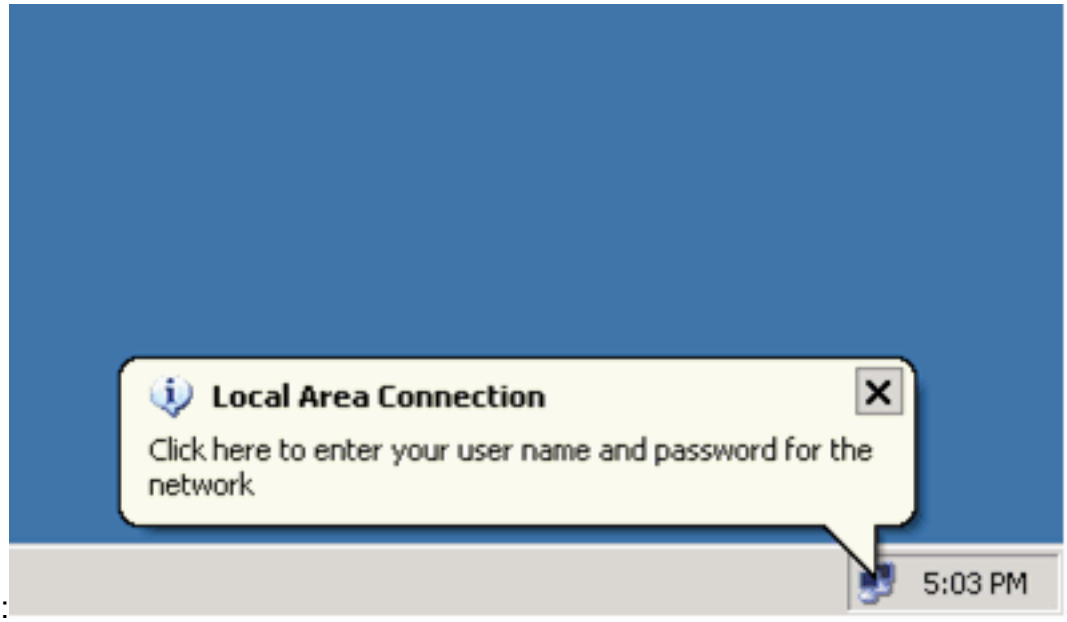
Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

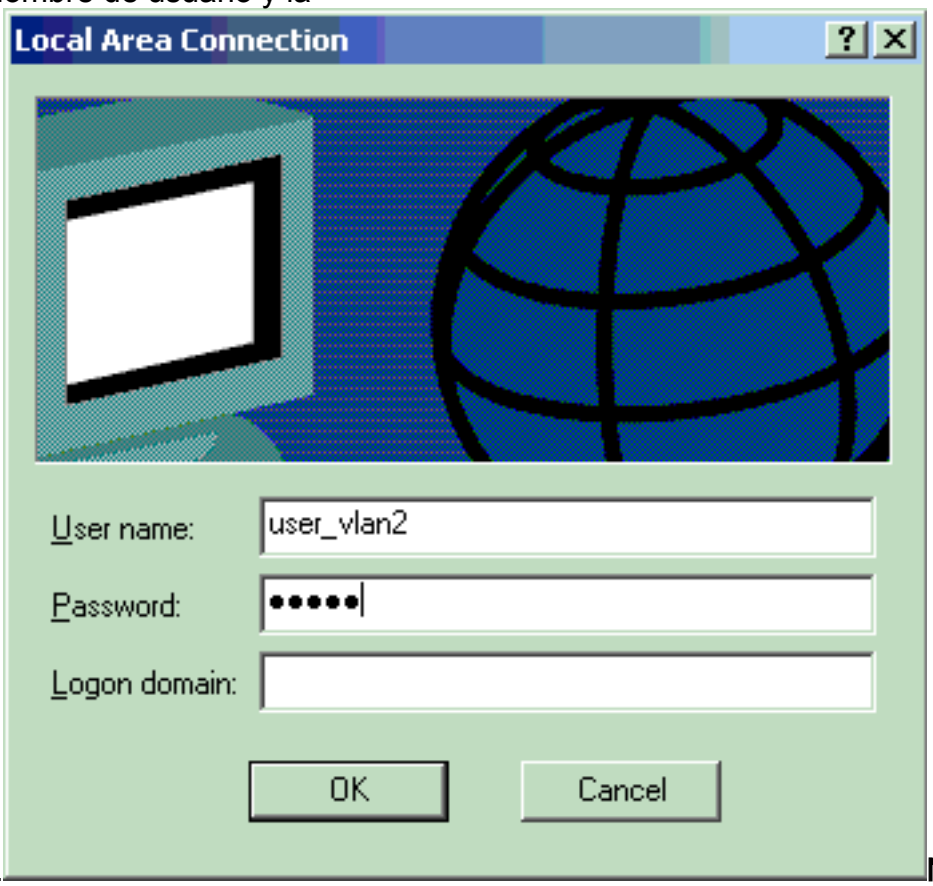
Clientes de PC

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

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

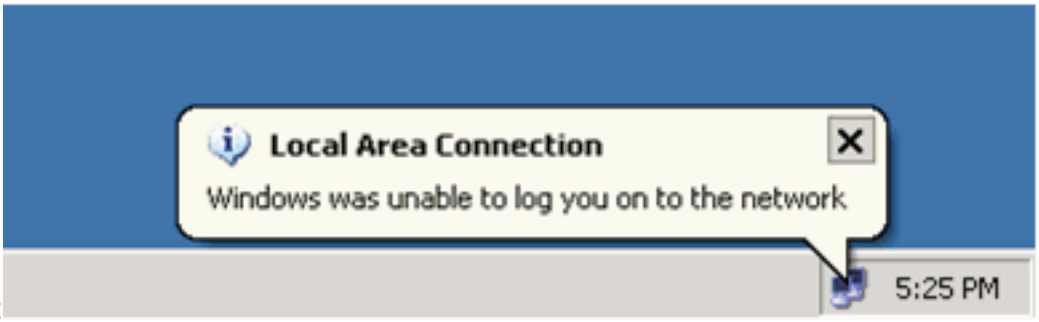
ejemplo: 

Se muestra una ventana de entrada de nombre de usuario y contraseña.

2. Ingrese el nombre de usuario y la contraseña. 

Nota: En PC 1 y 2, introduzca las credenciales de usuario de VLAN 2. En PC 3 y 4, introduzca las credenciales de usuario de VLAN 3.
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 el comando **ping**. Esta es una salida de PC 1, que muestra un **ping** exitoso a PC

4: Si aparece este error, verifique que el nombre de usuario y la contraseña sean

correctos: 

Catalyst 6500

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 `autorizado`.

```
Cat6K> (enable) show port dot1x 3/1-5

Port  Auth-State          BEnd-State Port-Control        Port-Status
----- ------------------- ---------- ------------------- -------------
 3/1  force-authorized    idle       force-authorized    authorized
 !--- This is the port to which RADIUS server is connected. 3/2 authenticated       idle
auto                 authorized
 3/3  authenticated       idle       auto                authorized
 3/4  authenticated       idle       auto                authorized
 3/5  authenticated       idle       auto                authorized

Port  Port-Mode     Re-authentication    Shutdown-timeout
----- ------------- -----------------    ----------------
 3/1  SingleAuth    disabled             disabled
 3/2  SingleAuth    disabled             disabled
 3/3  SingleAuth    disabled             disabled
 3/4  SingleAuth    disabled             disabled
 3/5  SingleAuth    disabled             disabled
```

   Verifique el estado de VLAN después de la autenticación exitosa.

```
Cat6K> (enable) show vlan
VLAN Name                             Status    IfIndex Mod/Ports, Vlans
---- -------------------------------- --------- ------- -------------------------

1    default                          active    6       2/1-2
                                                        3/6-48
2    VLAN2                            active    83      3/2-3
3    VLAN3                            active    84      3/4-5
4    AUTHFAIL_VLAN                    active    85
5    GUEST_VLAN                       active    86
10   RADIUS_SERVER                    active    87      3/1
1002 fddi-default                     active    78
1003 token-ring-default               active    81
1004 fddinet-default                  active    79
1005 trnet-default                    active    80
!--- Output suppressed.
```

2. Verifique el estado de enlace DHCP del módulo de routing (MSFC) después de la autenticación correcta.

```
Router#show ip dhcp binding
IP address       Hardware address        Lease expiration        Type
172.16.2.2       0100.1636.3333.9c       Feb 14 2007 03:00 AM    Automatic
172.16.2.3       0100.166F.3CA3.42       Feb 14 2007 03:03 AM    Automatic
172.16.3.2       0100.145e.945f.99       Feb 14 2007 03:05 AM    Automatic
172.16.3.3       0100.1185.8D9A.F9       Feb 14 2007 03:07 AM    Automatic
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Ejemplo de Configuración de Autenticación IEEE 802.1x con Catalyst 6500/6000 que Ejecuta Cisco IOS Software
- Guía de implementación de Catalyst Switching y ACS
- RFC 2868: Atributos de RADIUS para soporte a protocolo de túnel
- Configuración de la Autenticación 802.1x
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems