Autenticación del IEEE 802.1X con el Catalyst 6500/6000 que funciona con el ejemplo de configuración del 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.

prerrequisitos

Requisitos

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

- Guía de instalación para el Cisco Secure ACS for Windows 4.1
- Guía del usuario para el Cisco Secure Access Control Server 4.1
- ¿Cómo el RADIUS trabaja?
- Transferencia del Catalyst y Guía de despliegue ACS

Componentes Utilizados

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

- Catalyst 6500 que funciona con la versión de software CatOS 8.5(6) en el Supervisor Engine y el Cisco IOS Software Release 12.2(18)SXF en el MSFC**Nota:** Usted necesita la versión 6.2 de CatOS o más adelante soportar la autenticación del acceso basado del 802.1x.**Nota:** Antes de que el Software Release 7.2(2), una vez que se autentica el host del 802.1x, él se una a un VLA N Nvram-configurado. Con las versiones del Software Release 7.2(2) y Posterior, después de la autenticación, un host del 802.1x puede recibir su asignación VLAN del servidor de RADIUS.
- 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 habilitar 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.

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.

Convenciones

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

Antecedentes

El estándar del IEEE 802.1X define a un servidor del cliente - el protocolo basado del control de acceso y de autenticación que restringe 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 creando 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 hacer disponible cualesquiera servicios que sean ofrecidos por el Switch o el LAN. Hasta que se autentique el dispositivo, el control de acceso del 802.1x permite solamente el Protocolo de Autenticación Extensible (EAP) 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.

Configurar

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

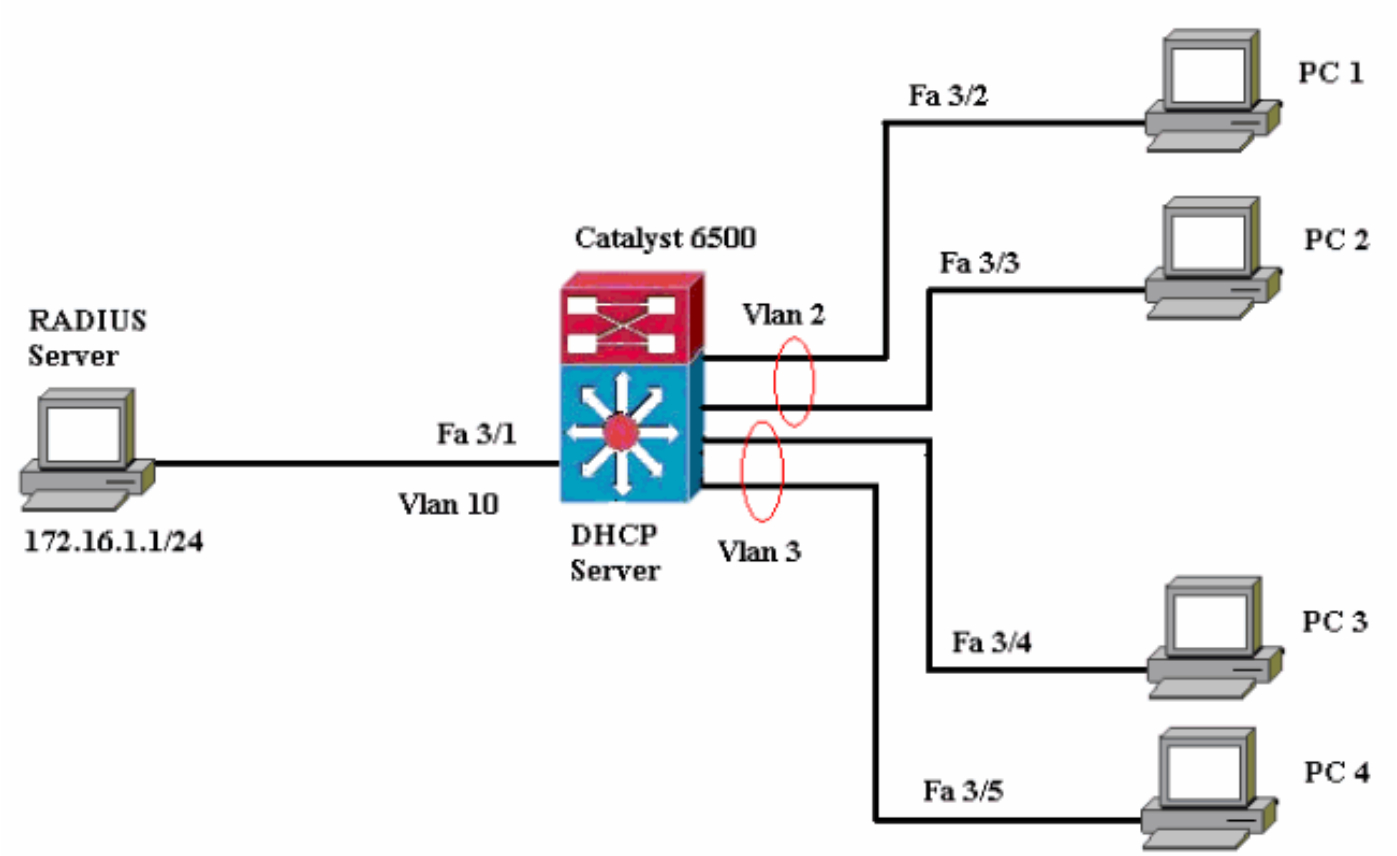
Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

La configuración requiere estos pasos:

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

Diagrama de la red

En este documento, se utiliza esta configuración de red:



- Servidor de RADIUS — 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, configuran al servidor de RADIUS para la autenticación y la asignación VLAN.
- Switch — 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, pidiendo la información de identidad del cliente, verificando esa información con el servidor de RADIUS, y retransmitiendo una respuesta al cliente. Aquí, el Catalyst 6500 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 agregando la identidad del usuario autenticado en el proceso de detección del DHCP.
- Clientes — Los dispositivos (puestos de trabajo) ese acceso de la petición a los servicios LAN y del Switch y responden a las peticiones del Switch. Aquí, los PC 1 a 4 son los clientes que piden un acceso a la red autenticado. Los PC 1 y 2 utilizarán el mismo credencial de inicio de sesión para estar en el VLAN2. Semejantemente, los PC 3 y 4 utilizarán un credencial de inicio de sesión para el VLA N que configuran a 3. PC cliente para lograr la dirección IP de un

servidor DHCP.**Nota:** En esta configuración, moviéndolos a un VLA N inusitado (VLA N 4 niega cualquier cliente que falle la autenticación o cualquier cliente capaz non-802.1x que conecta con el Switch el acceso a la red o 5) usando las características del VLA N de la falla de autenticación y del invitado.

Configure el switch de Catalyst para la autenticación del 802.1x

Esta configuración del switch de la muestra incluye:

- Habilite la autenticación del 802.1x y las características asociadas en los puertos FastEthernets.
- Conecte al servidor de RADIUS con el VLAN10 detrás del puerto FastEthernet 3/1.
- Configuración del servidor DHCP para dos agrupaciones IP, una para los clientes en el VLAN2 y otra para los clientes en el VLAN3.
- Routing entre VLAN para tener Conectividad entre los clientes después de la autenticación.

Refiera a las guías de consulta de la configuración de autenticación para las guías de consulta en cómo configurar la autenticación del 802.1x.

Nota: Aseegurese que el servidor de RADIUS conecta siempre 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 successsful 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
```

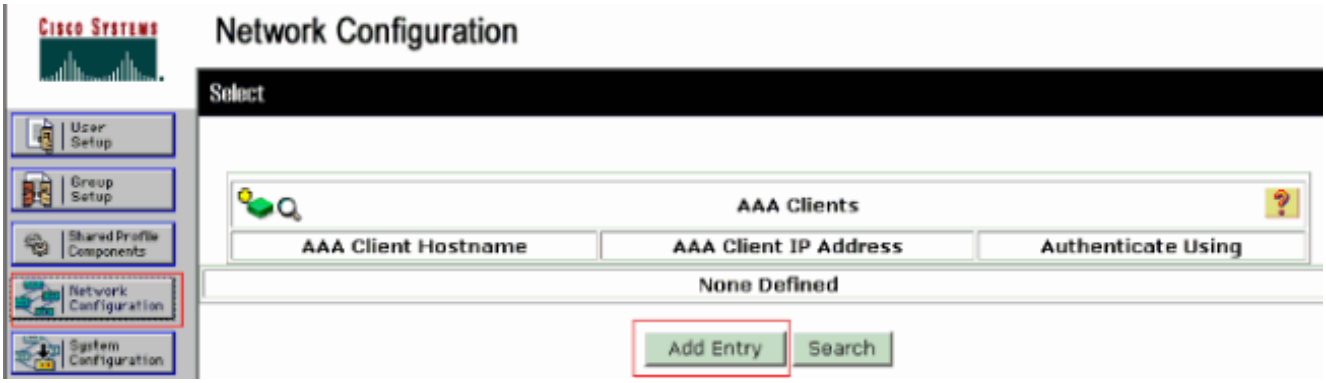
modified. VLAN 1 modified. VLAN Mod/Ports ---- ---------- 10 3/1 *!--- Assigns port connecting to RADIUS server to VLAN 10.* Cat6K> (enable) **set radius server 172.16.1.1 primary** 172.16.1.1 with auth-port 1812 acct-port 1813 added to radius server table as primary server. *!--- Sets the IP address 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)
```

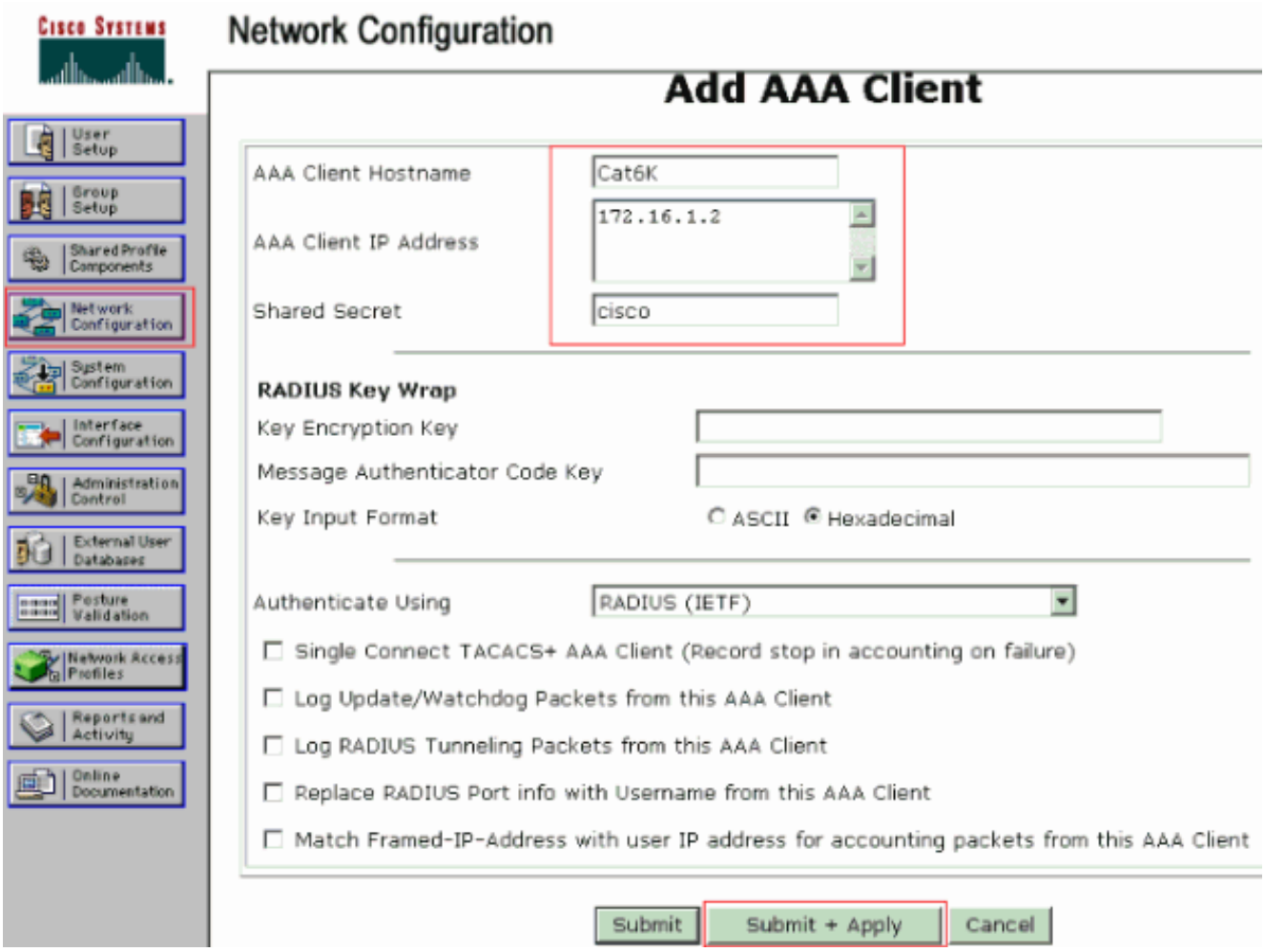
Configure al servidor de RADIUS

Configuran al servidor de RADIUS con un IP Address estático de 172.16.1.1/24. Complete estos pasos para configurar al servidor de RADIUS para un cliente AAA:

1. Para configurar a un cliente AAA, haga clic la **configuración de red** en la ventana de administración ACS.
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 (**Cat6K**).Dirección IP del cliente AAA = interfaz de administración (direccionamiento sc0)IP del Switch (**172.16.1.2**).Secreto compartido = clave del radio configurada en el Switch (**Cisco**).Autentique usando = **RADIUS IETF**.**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.
4. El tecleo **somete + se aplica** para realizar estos cambios eficaces, pues este ejemplo muestra:

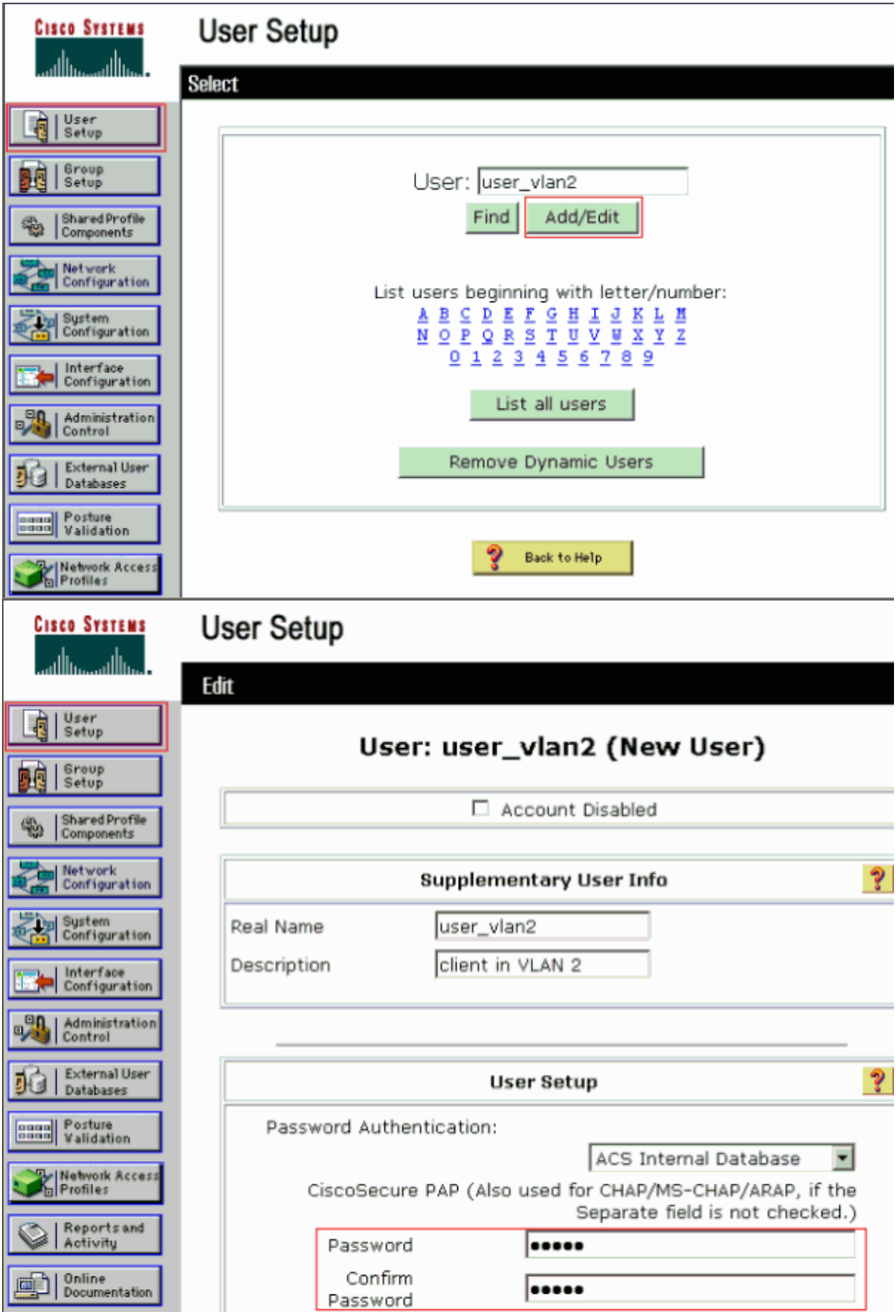


Complete estos pasos para configurar al servidor de RADIUS para la autenticación, la asignación del VLA N y de la dirección IP:

Dos Nombres de usuario tienen que ser creados por separado para los clientes que conectan con el VLAN2 así como para el VLAN3. Aquí, un usuario **user_vlan2** para los clientes que conectan con el VLAN2 y otro usuario **user_vlan3** para los clientes que conectan con el VLAN3 son para este propósito creado.

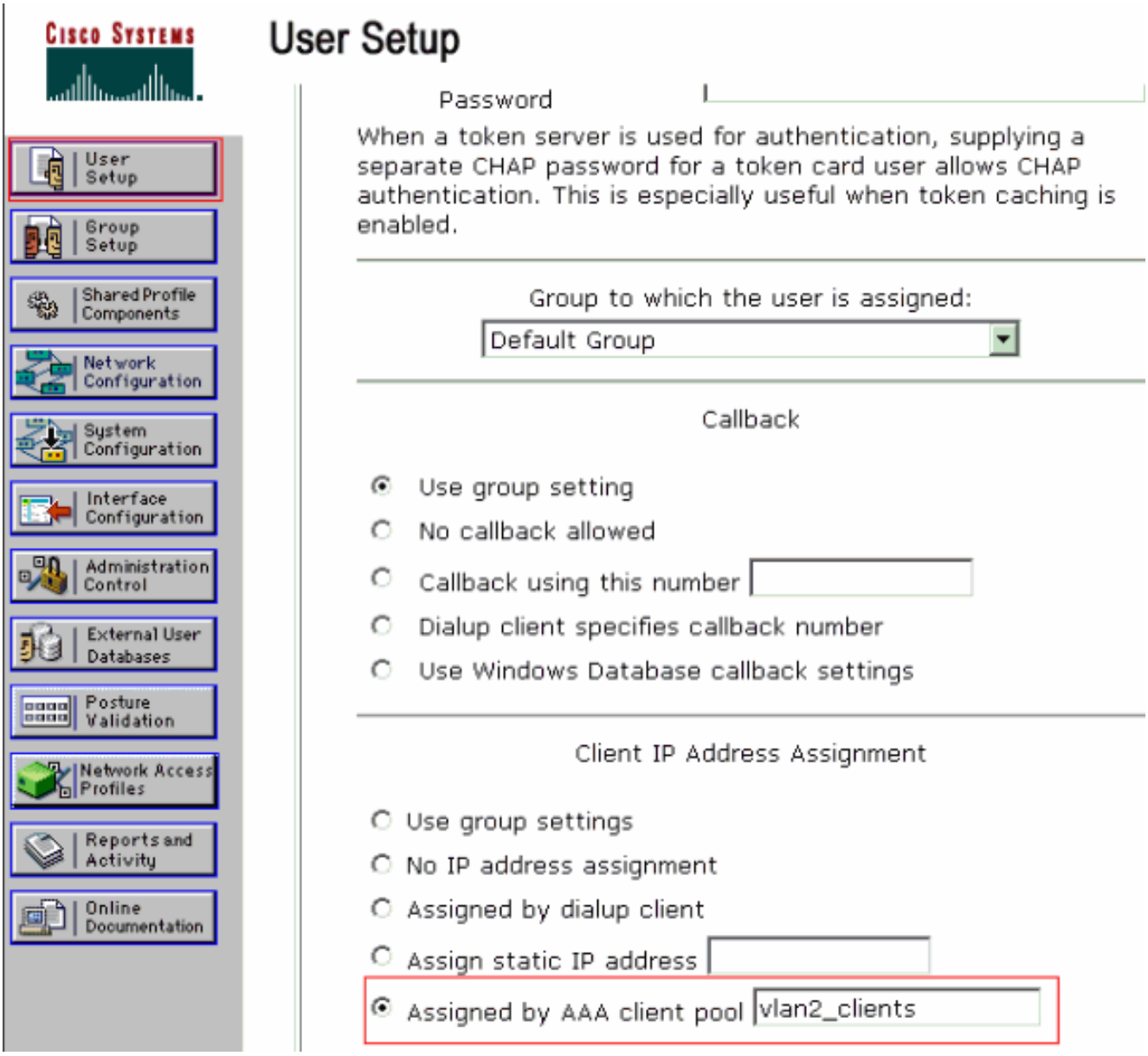
Nota: Aquí, la configuración de usuario se muestra para los clientes que conectan con el VLAN2 solamente. Para los usuarios que conectan con el VLAN3, complete el mismo procedimiento.

1. Para agregar y configurar los usuarios, la **configuración de usuario del** tecleo y definir el nombre de usuario y
   contraseña.



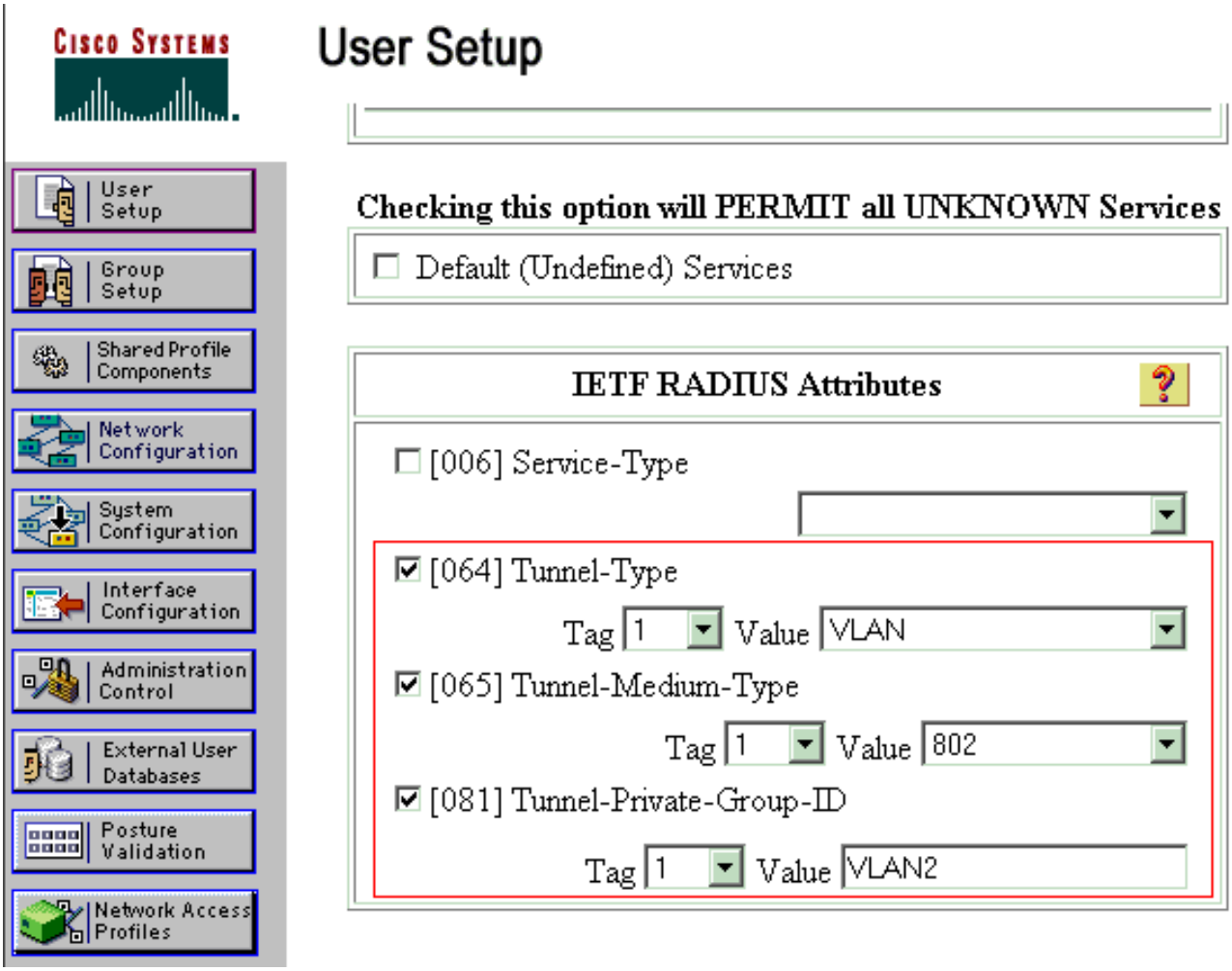
2. Defina la asignación de dirección IP del cliente según lo **asignado por el pool del cliente AAA**. Ingrese el nombre del pool del IP Address configurado en el Switch para los clientes

VLAN2.



Nota: Seleccione 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.

3. Defina los atributos 64 y 65 de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF).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 del* VLA N que corresponda.**Nota:** *El nombre del* VLA N debe ser exactamente lo mismo que el que está configurado en el Switch.**Nota:** La asignación VLAN basada en el número VLAN no se soporta con
CatOS.



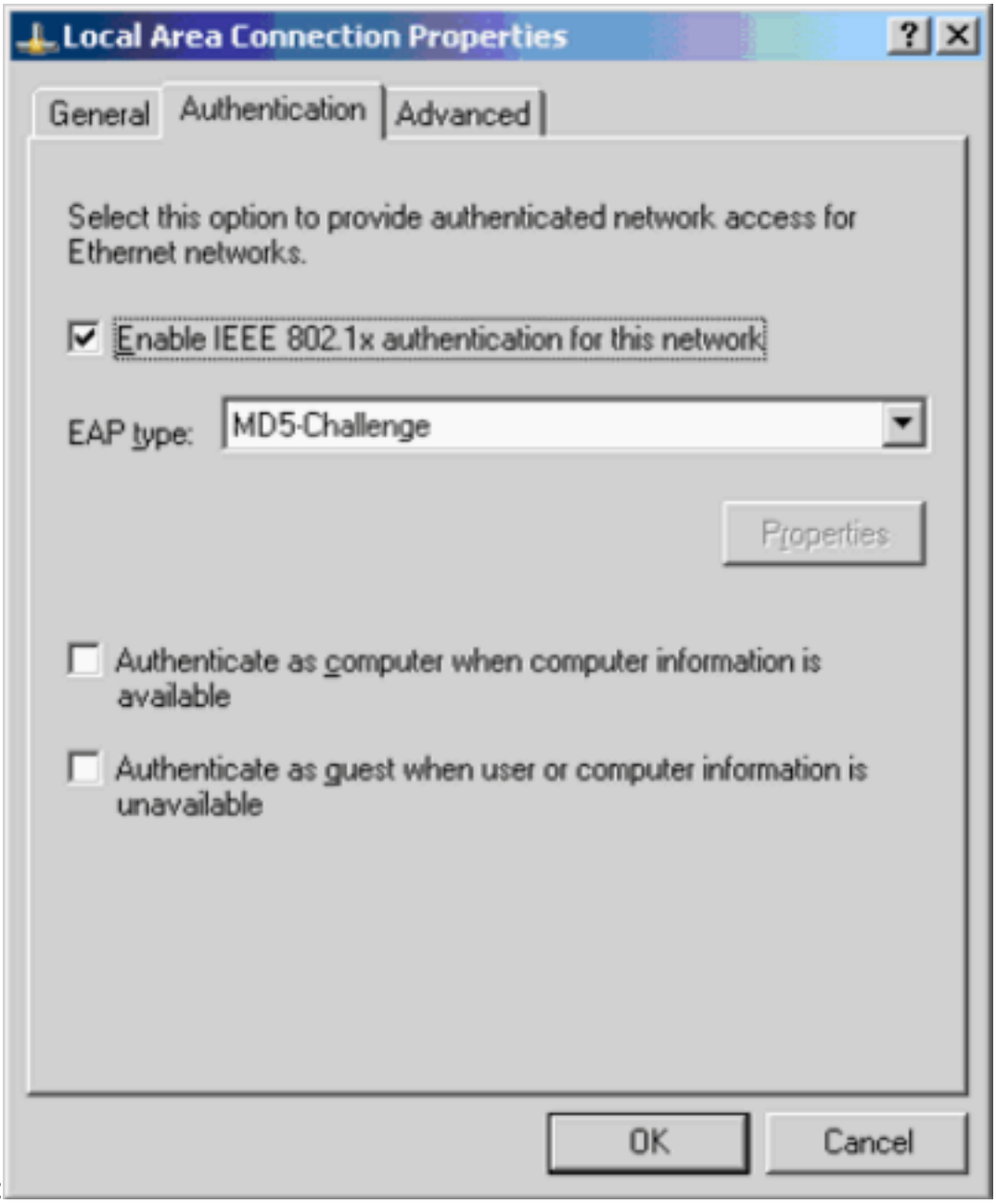
Refiera al RFC 2868: Atributos de RADIUS para el soporte del Tunnel Protocol para más información sobre estos atributos IETF.**Nota:** En la configuración inicial del servidor ACS, los atributos IETF RADIUS pueden no poder visualizar en **configuración de usuario**. Elija la **configuración de la interfaz > RADIUS (IETF)** para habilitar los atributos IETF en la pantalla de la configuración de usuario. Luego, verifique los atributos 64, 65 y 81 en las columnas Usuario y Grupo.

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). Complete estos pasos:

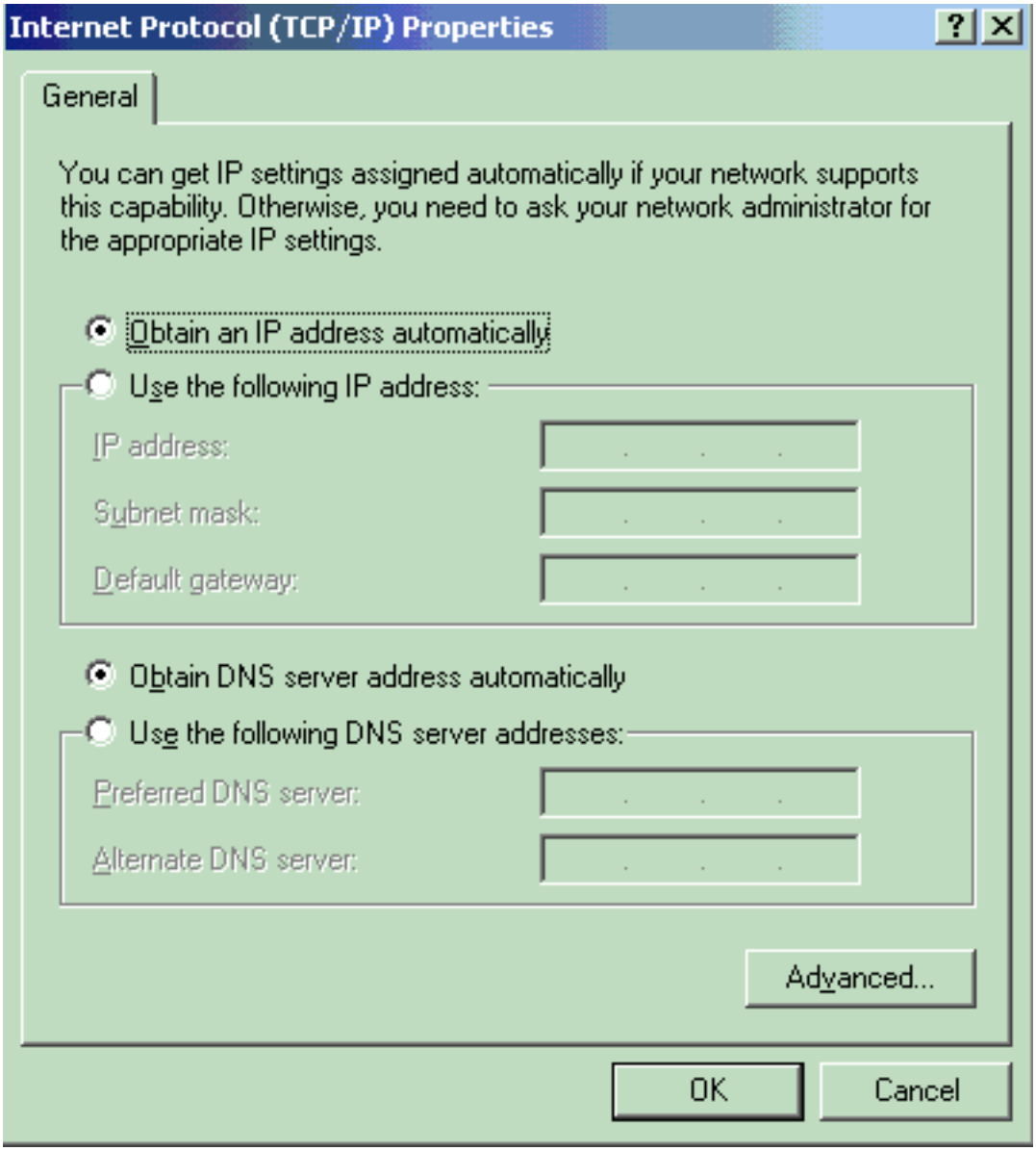
1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**, después haga clic con el botón derecho del ratón en su **conexión de área local** y elija las **propiedades**.
2. Marque el **icono de la demostración en la área de notificación cuando está conectado** 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 una 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**.



Verificación

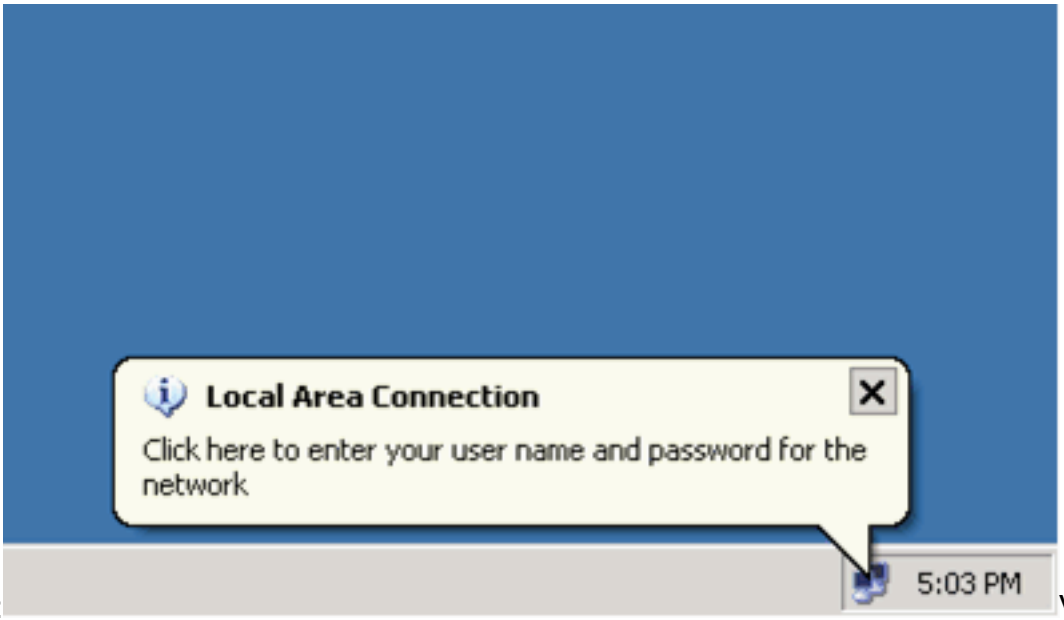
Use esta sección para confirmar que su configuración funciona correctamente.

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.

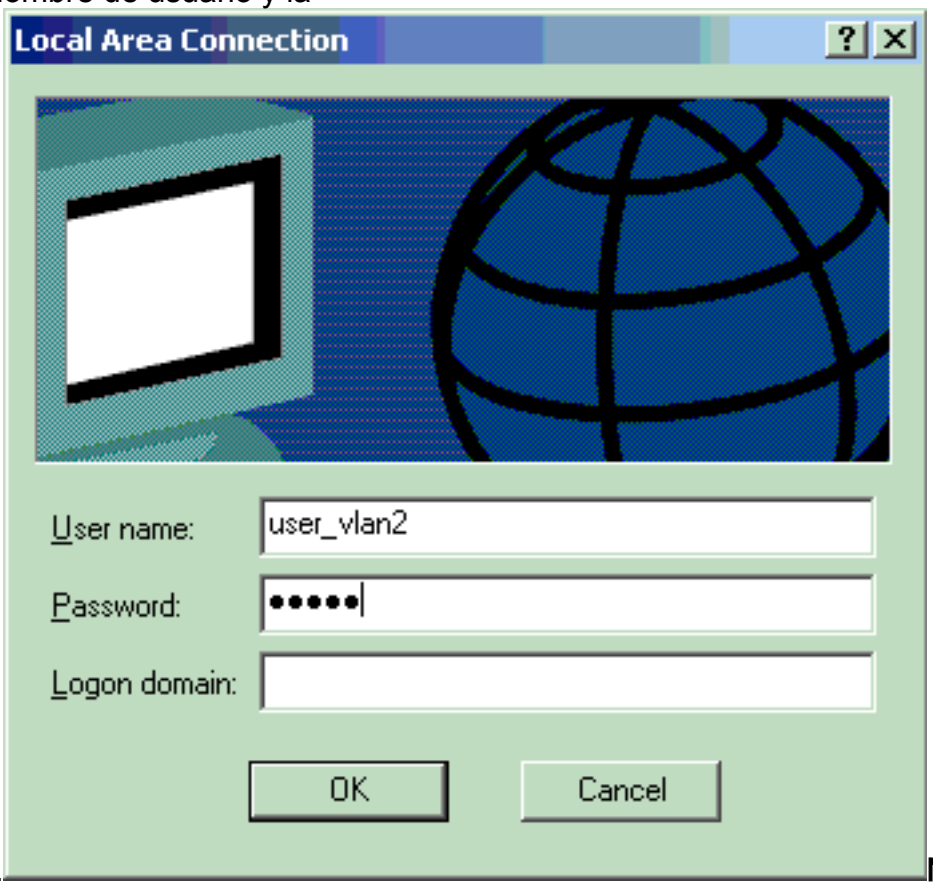
PC cliente

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

1. Haga clic en el prompt, que este ejemplo

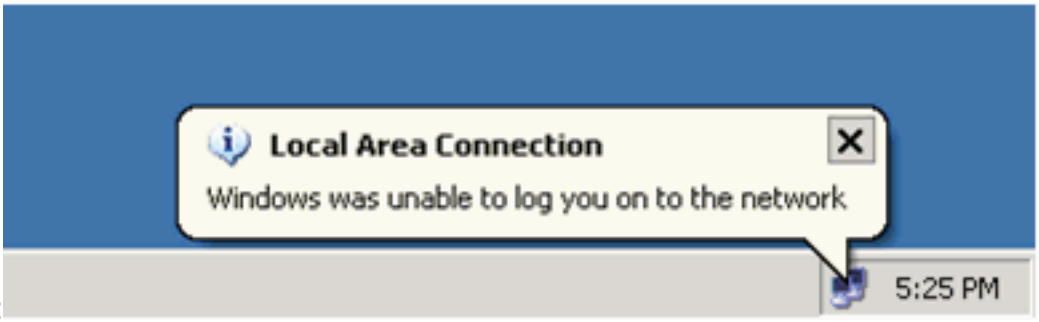
muestra: 

Visualizaciones de una ventana de entrada del nombre de usuario y contraseña.

2. Ingrese el nombre de usuario y la 

contraseña. **Nota:** En el PC1 y 2, ingrese los credenciales de usuario VLAN2. En el PC3 y 4, ingrese los credenciales de usuario VLAN3.
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 **comando ping**. Esto es una salida del PC1, que muestra un ping exitoso a PC

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

correcto: 

Catalyst 6500

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.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 satisfactoria.`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 DHCP que ata el estatus del (MSFC) del módulo de ruteo después de la autenticación satisfactoria.`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`

Troubleshooting

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

Información Relacionada

- Autenticación del IEEE 802.1X con el Catalyst 6500/6000 que funciona con el ejemplo de configuración del Cisco IOS Software
- Transferencia del Catalyst y Guía de despliegue 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