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

Contenido

Introducción

Este documento explica cómo configurar IEEE 802.1x en un Catalyst 6500/6000 que se ejecuta en modo nativo (una sola imagen de Cisco IOS® Software para la Supervisor Engine y 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 el Cisco IOS Software Release 12.2(18)SXF en el Supervisor Engine**Nota:** Necesita la versión 12.1(13)E de software del IOS de Cisco o posterior para soportar la autenticación 802.1x a partir de un puerto.
- 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.

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

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 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.

Nota: Si el Switch recibe los paquetes EAPOL del puerto que no se configura para la autenticación del 802.1x o si el Switch no soporta la autenticación del 802.1x, después los paquetes EAPOL se caen y no se remiten a ningunos dispositivos ascendentes.

Configurar

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

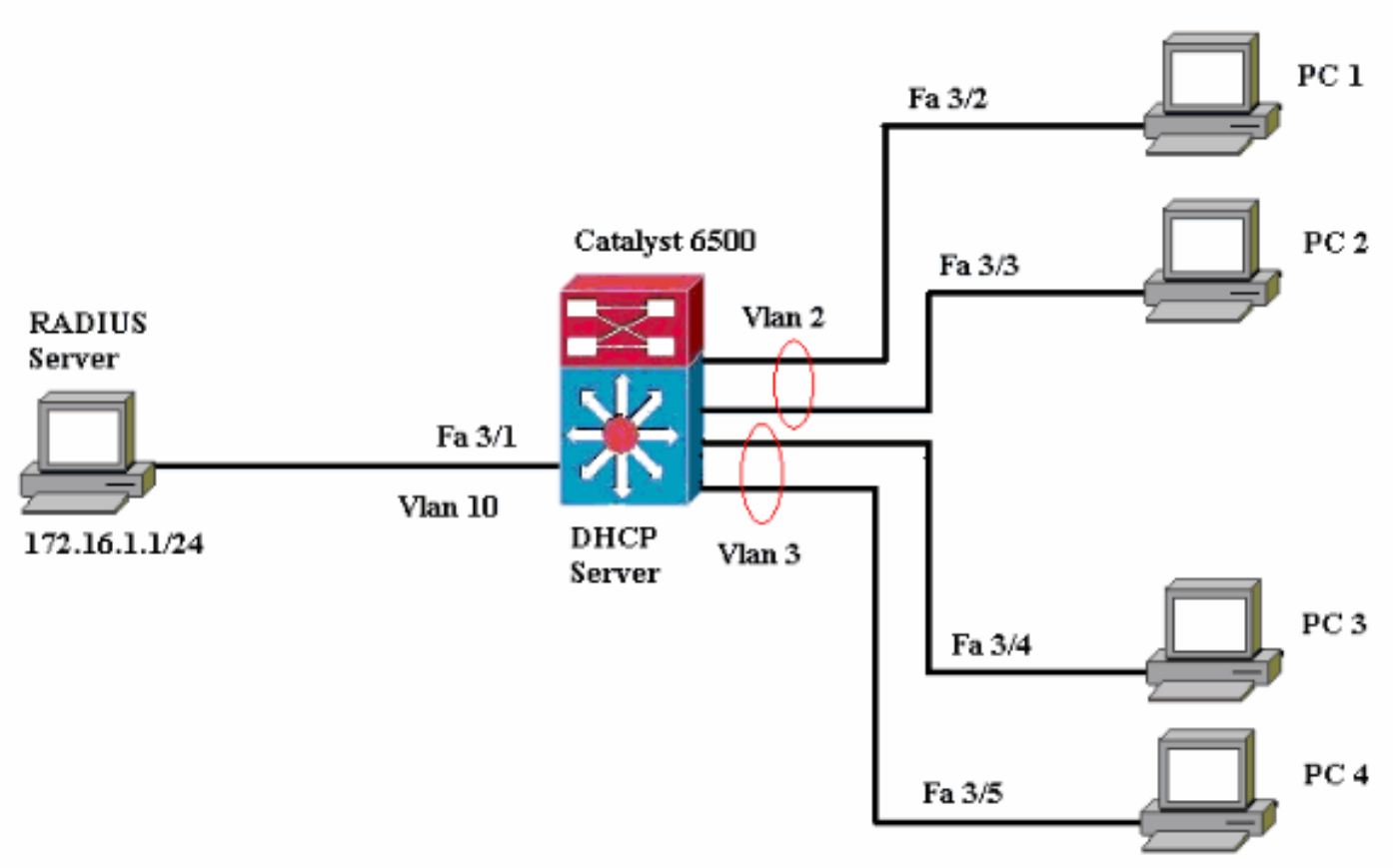
La configuración requiere estos pasos:

- 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. Pide la información de identidad del cliente, verifica esa información con el servidor de RADIUS, y retransmite 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) esos piden el acceso 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 utilizan el mismo credencial de inicio de sesión que está en el VLAN2. Semejantemente, los PC 3 y 4 utilizan 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.

Configure el switch de Catalyst para la autenticación del 802.1x

Esta configuración del switch de la muestra incluye:

- Cómo habilitar la autenticación del 802.1x en los puertos FastEthernets.
- Cómo conectar a un servidor de RADIUS con el VLAN10 detrás del puerto FastEthernet 3/1.
- Una configuración del servidor DHCP para dos agrupaciones IP, una para los clientes en el VLAN2 y la 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 y a las restricciones de la autenticación del acceso basado del 802.1x 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

```
Router#configure terminal Enter configuration commands,
one per line. End with CNTL/Z. Router(config)#hostname
Cat6K !--- Sets the hostname for the switch.
Cat6K(config)#vlan 2 Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3 Cat6K(config-vlan)#name VLAN3
!--- VLAN should be existing in the switch for a
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER !--- This is a
dedicated VLAN for the RADIUS server. Cat6K(config-
vlan)#exit Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport Cat6K(config-if)#switchport
mode access Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut !--- Assigns the port connected
to the RADIUS server to VLAN 10. !--- Note:- All the
active access ports are in VLAN 1 by default.
Cat6K(config-if)#exit Cat6K(config)#dot1x system-auth-
control !--- Globally enables 802.1x.
Cat6K(config)#interface range fastEthernet3/2-48
Cat6K(config-if-range)#switchport Cat6K(config-if-
range)#switchport mode access Cat6K(config-if-
range)#dot1x port-control auto Cat6K(config-if-range)#no
shut !--- Enables 802.1x on all the FastEthernet
interfaces. Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model !--- Enables AAA.
Cat6K(config)#aaa authentication dot1x default group
radius !--- Method list should be default. Otherwise
dot1x does not work. Cat6K(config)#aaa authorization
network default group radius !--- You need authorization
for dynamic VLAN assignment to work with RADIUS.
Cat6K(config)#radius-server host 172.16.1.1 !--- Sets
the IP address of the RADIUS server.
Cat6K(config)#radius-server key cisco !--- The key must
match the key used on the RADIUS server.
Cat6K(config)#interface vlan 10 Cat6K(config-if)#ip
address 172.16.1.2 255.255.255.0 Cat6K(config-if)#no
shut !--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut !--- This is the gateway
address for clients in VLAN 2. Cat6K(config-
if)#interface vlan 3 Cat6K(config-if)#ip address
172.16.3.1 255.255.255.0 Cat6K(config-if)#no shut !---
This is the gateway address for clients in VLAN 3.
```

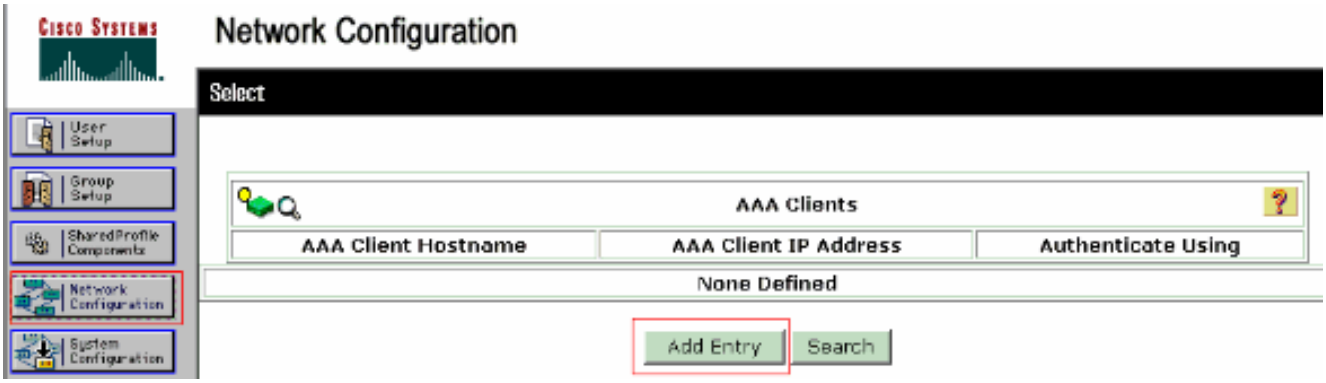
```
Cat6K(config-if)#exit Cat6K(config)#ip dhcp pool
vlan2_clients Cat6K(dhcp-config)#network 172.16.2.0
255.255.255.0 Cat6K(dhcp-config)#default-router
172.16.2.1 !--- This pool assigns ip address for clients
in VLAN 2. Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1 !--- This
pool assigns ip address for clients in VLAN 3.
Cat6K(dhcp-config)#exit Cat6K(config)#ip dhcp excluded-
address 172.16.2.1 Cat6K(config)#ip dhcp excluded-
address 172.16.3.1 Cat6K(config-if)#end Cat6K#show vlan
VLAN Name Status Ports ---- ---------------------------
---- --------- ------------------------------ 1 default
active Fa3/2, Fa3/3, Fa3/4, Fa3/5 Fa3/6, Fa3/7, Fa3/8,
Fa3/9 Fa3/10, Fa3/11, Fa3/12, Fa3/13 Fa3/14, Fa3/15,
Fa3/16, Fa3/17 Fa3/18, Fa3/19, Fa3/20, Fa3/21 Fa3/22,
Fa3/23, Fa3/24, Fa3/25 Fa3/26, Fa3/27, Fa3/28, Fa3/29
Fa3/30, Fa3/31, Fa3/32, Fa3/33 Fa3/34, Fa3/35, Fa3/36,
Fa3/37 Fa3/38, Fa3/39, Fa3/40, Fa3/41 Fa3/42, Fa3/43,
Fa3/44, Fa3/45 Fa3/46, Fa3/47, Fa3/48 2 VLAN2 active 3
VLAN3 active 10 RADIUS_SERVER active Fa3/1 1002 fddi-
default act/unsup 1003 token-ring-default act/unsup 1004
fddinet-default act/unsup 1005 trnet-default act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

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

Configure al servidor de RADIUS

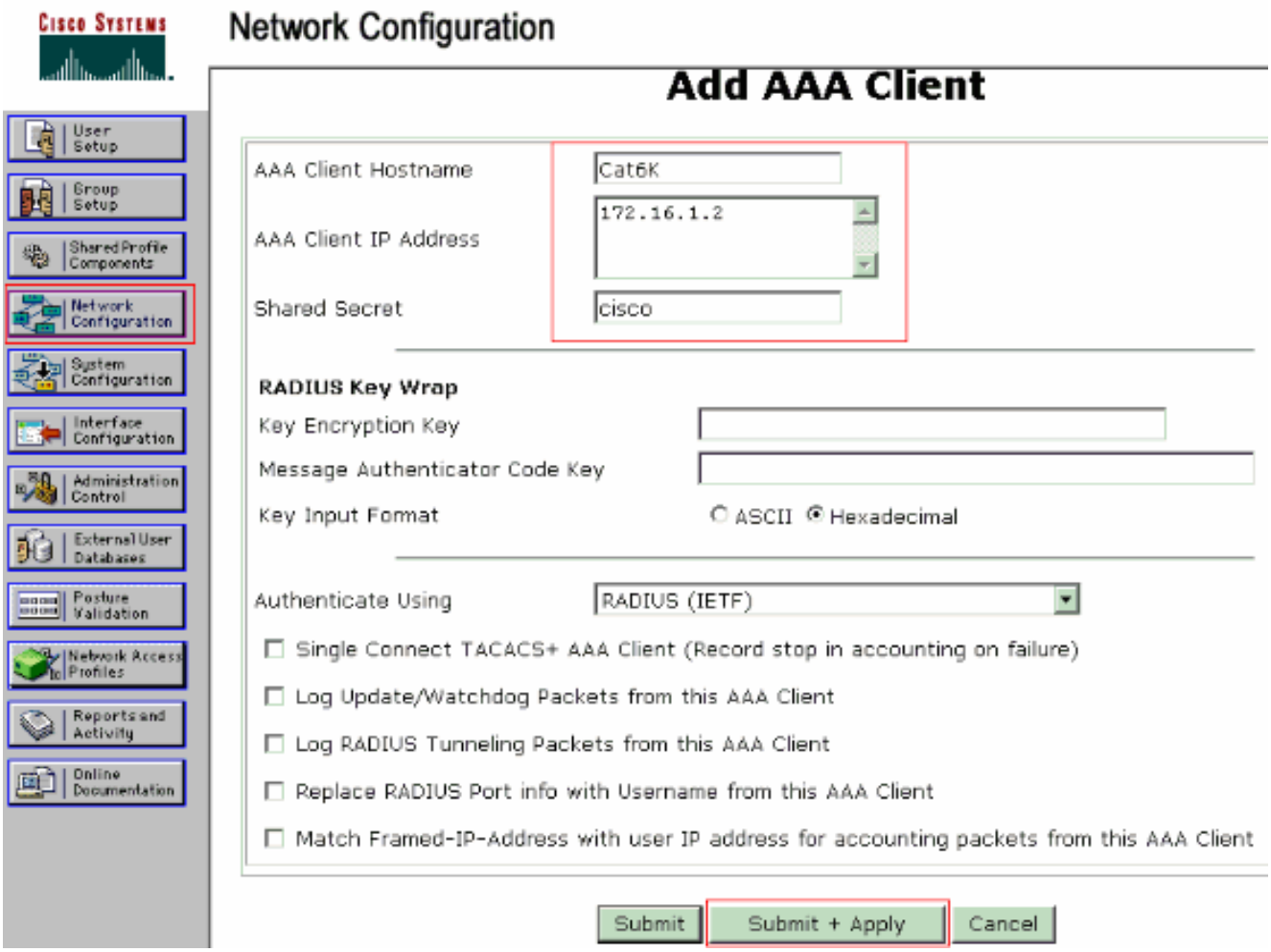
Configuran al servidor de RADIUS con un IP Address estático de 172.16.1.1/24. Complete estos pasos para configurar al servidor de RADIUS para un cliente AAA:

1. 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 (**Cat6K**).Dirección IP del cliente AAA = dirección IP de la interfaz de administración del Switch (**172.16.1.2**).Secreto compartido = clave RADIUS 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:

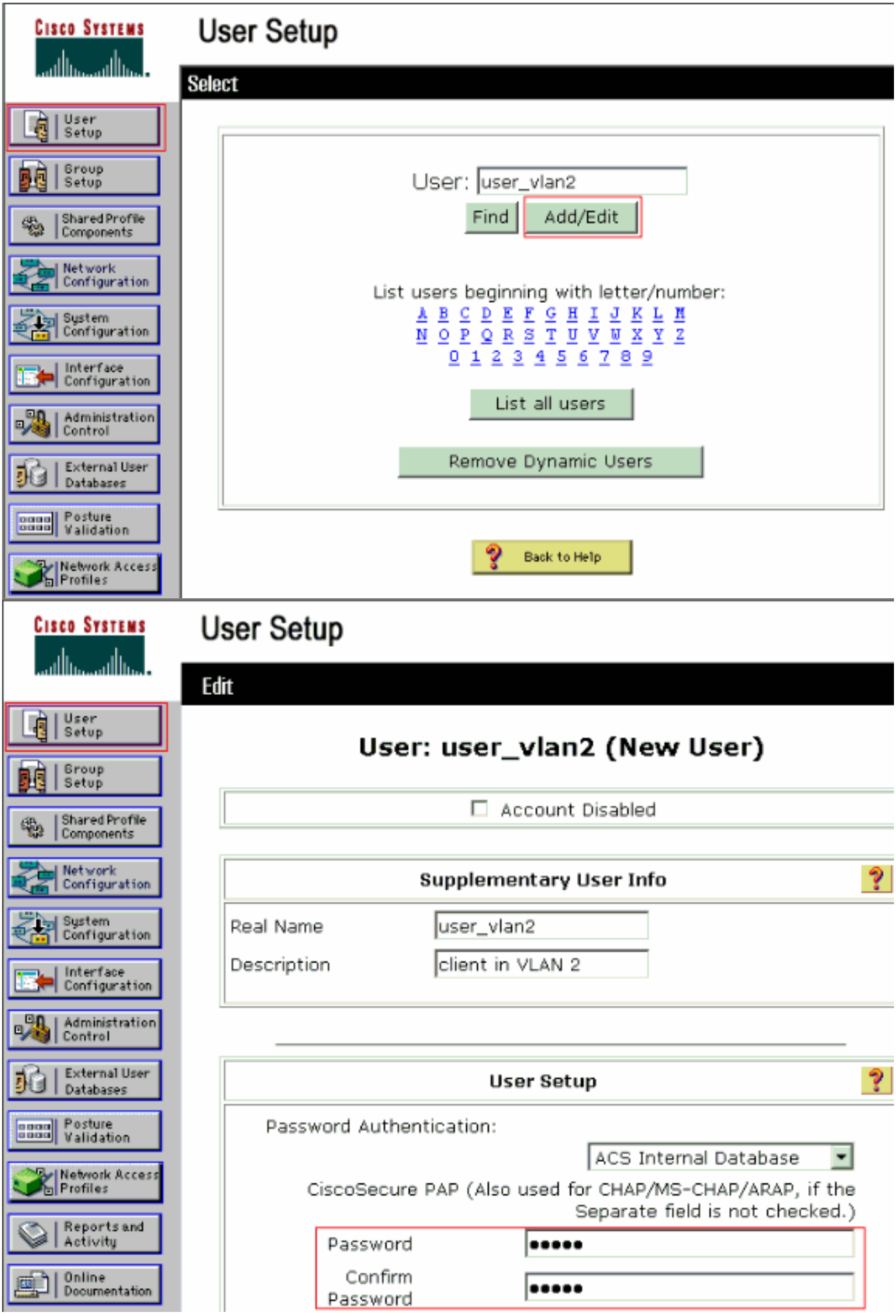


Complete estos pasos para configurar al servidor de RADIUS para la autenticación, la asignación del VLA N y de la dirección IP.

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 VLAN2 y otro usuario **user_vlan3** para los clientes que conectan con el VLAN3 es para este propósito creado.

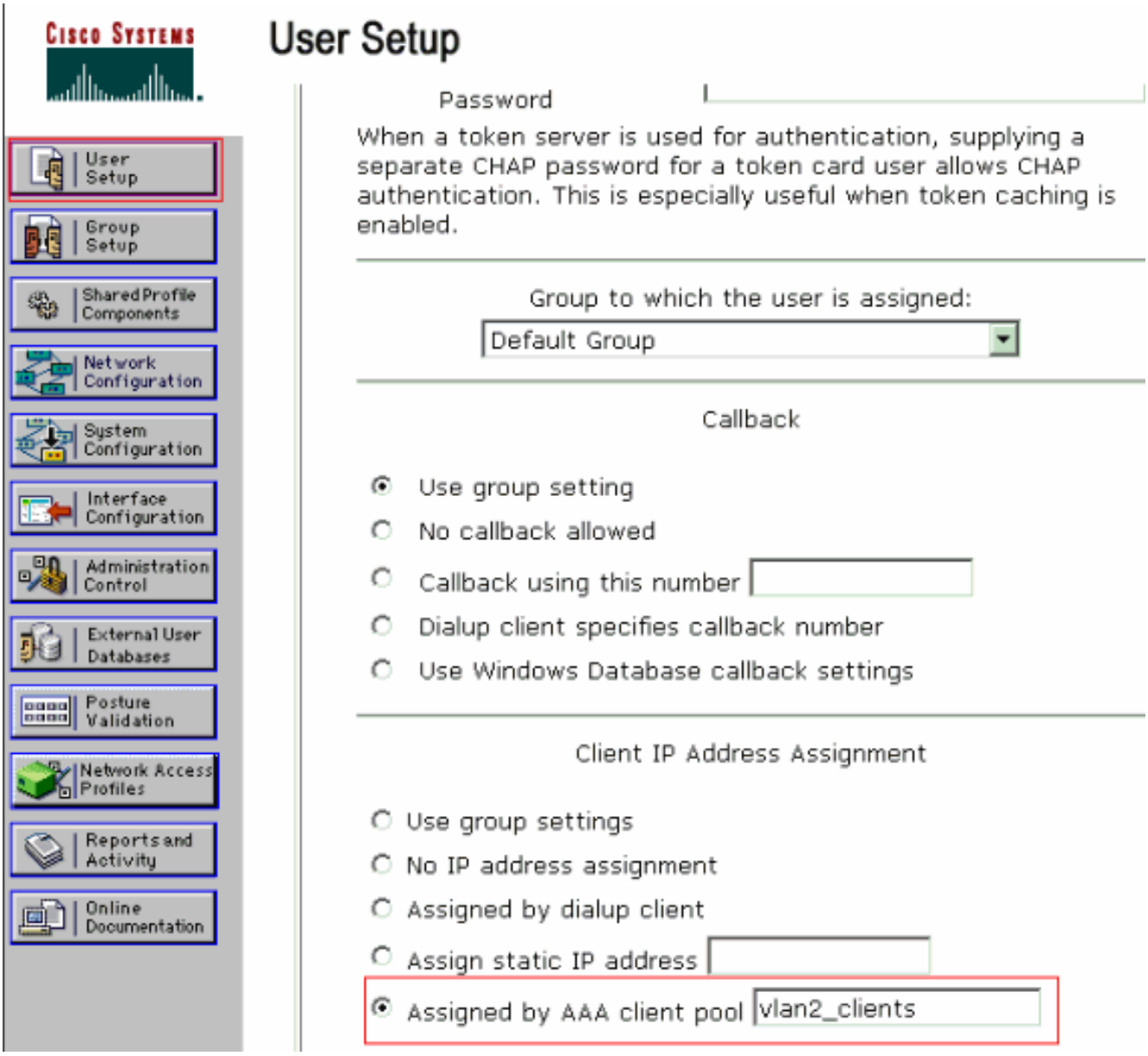
Nota: Aquí, la configuración de usuario se muestra para los clientes que conectan con el VLAN2 solamente. Para los usuarios que conectan con el VLAN3, siga el mismo procedimiento.

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



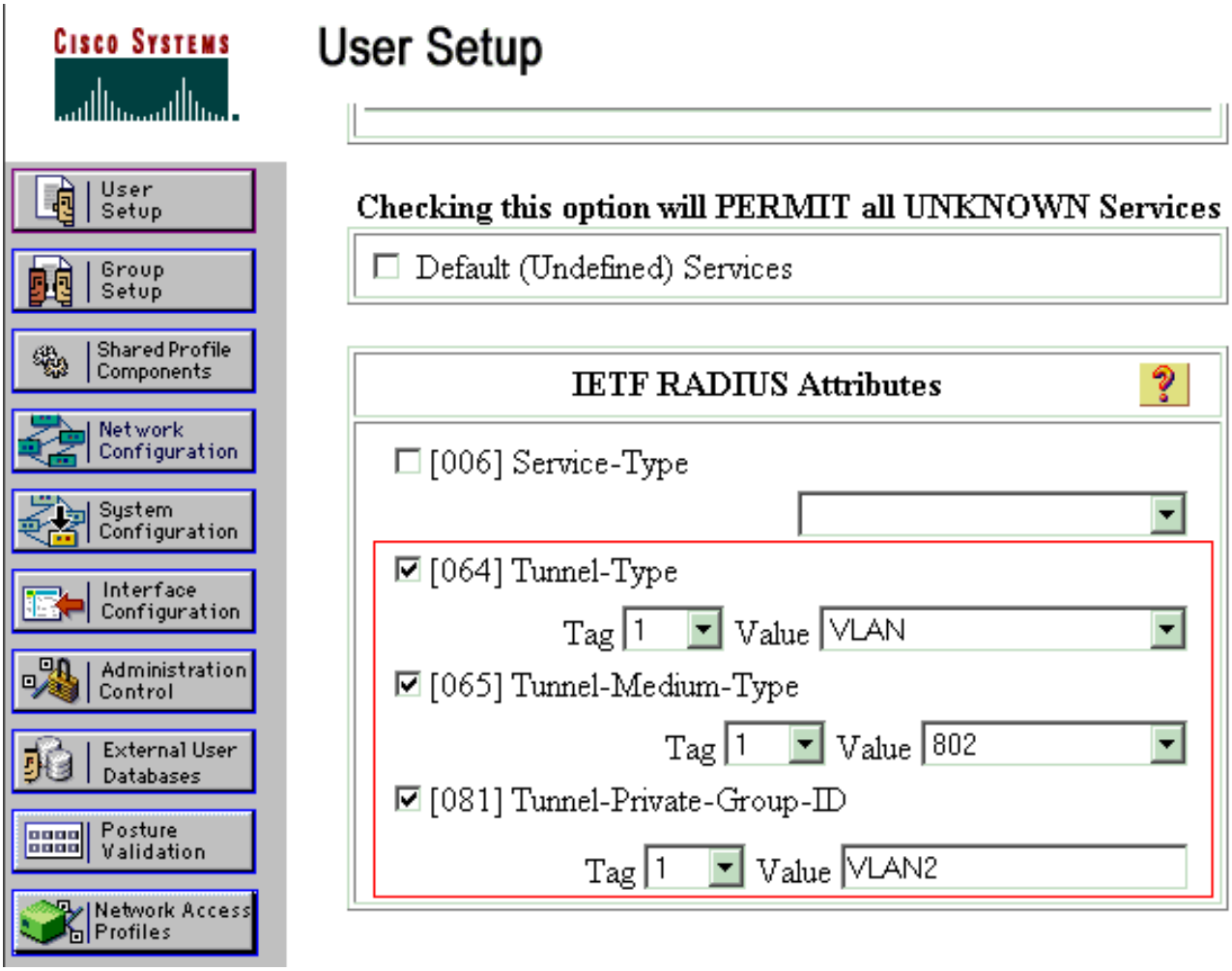
2. Defina la asignación de dirección IP del cliente según lo **asignado por el pool del cliente AAA**. Ingrese el nombre del pool del IP Address configurado en el Switch para los clientes

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* 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: Para más información sobre estos atributos IETF, refiera al [RFC 2868: Atributos RADIUS para el Soporte de protocolos de túnel.](#)**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, el cliente tiene asignación 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 **radio del grupo predeterminado del** comando aaa authorization network 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. Si usted ha definido el atributo **81**, pero usted ha configurado el puerto como puerto ruteado, la negación del acceso ocurre. Aparece este mensaje de error:`%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE: RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose VLAN cannot be assigned.`

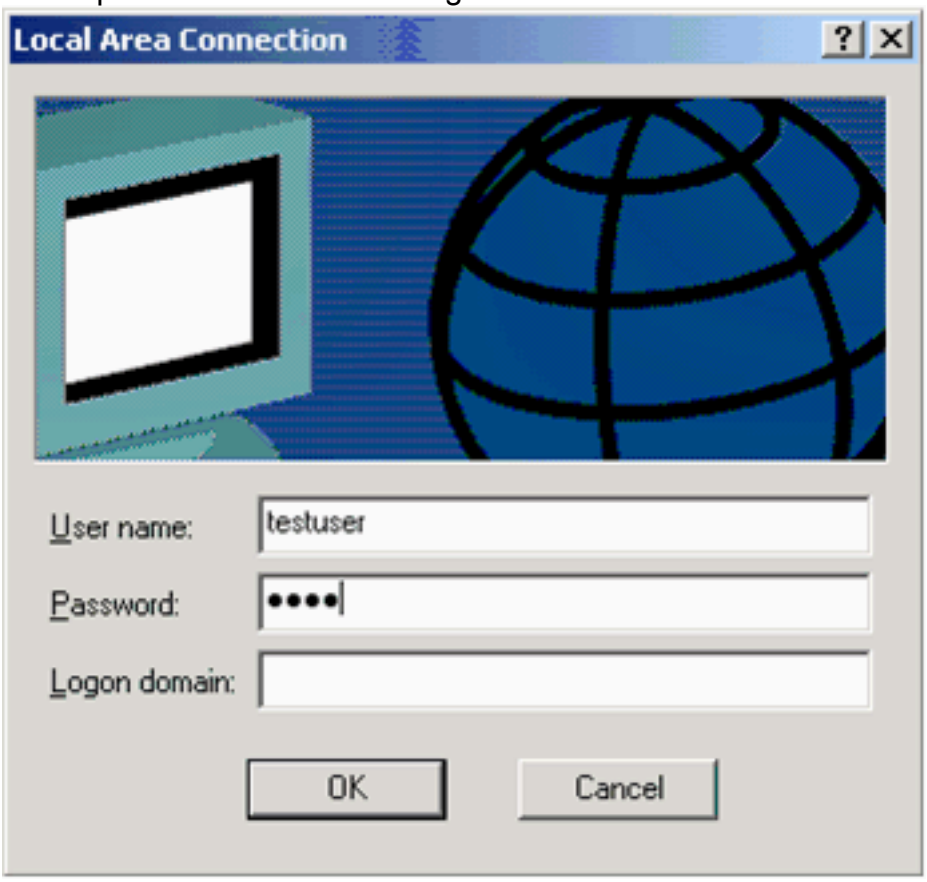
Configure a los PC cliente para utilizar la autenticación del 802.1x

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

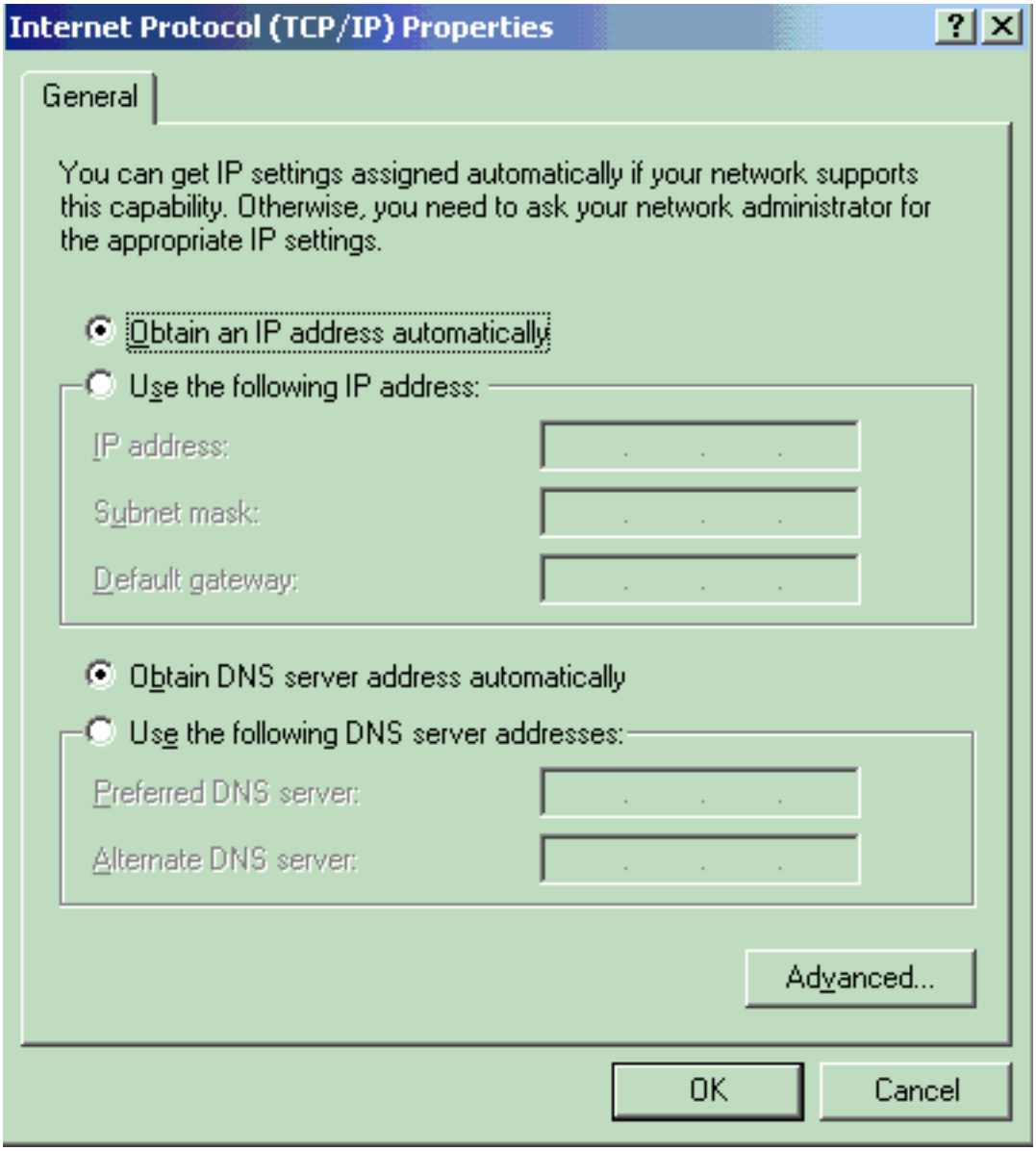
elija las **propiedades**.

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**.



Verificación

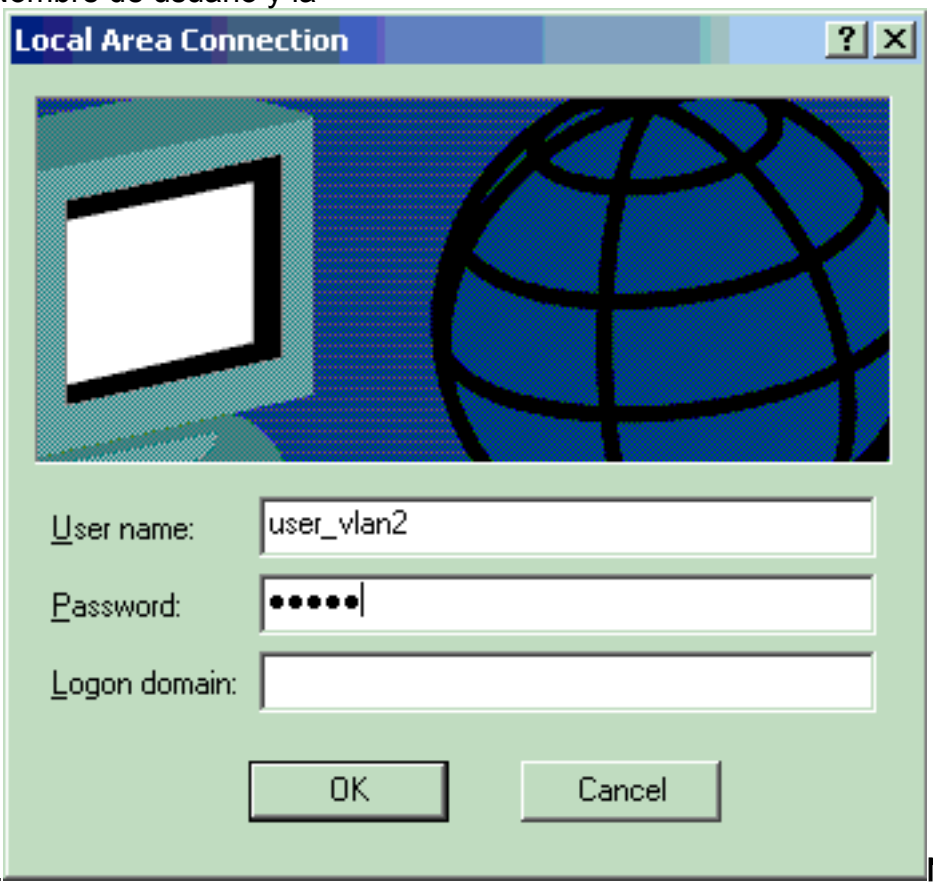
PC cliente

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

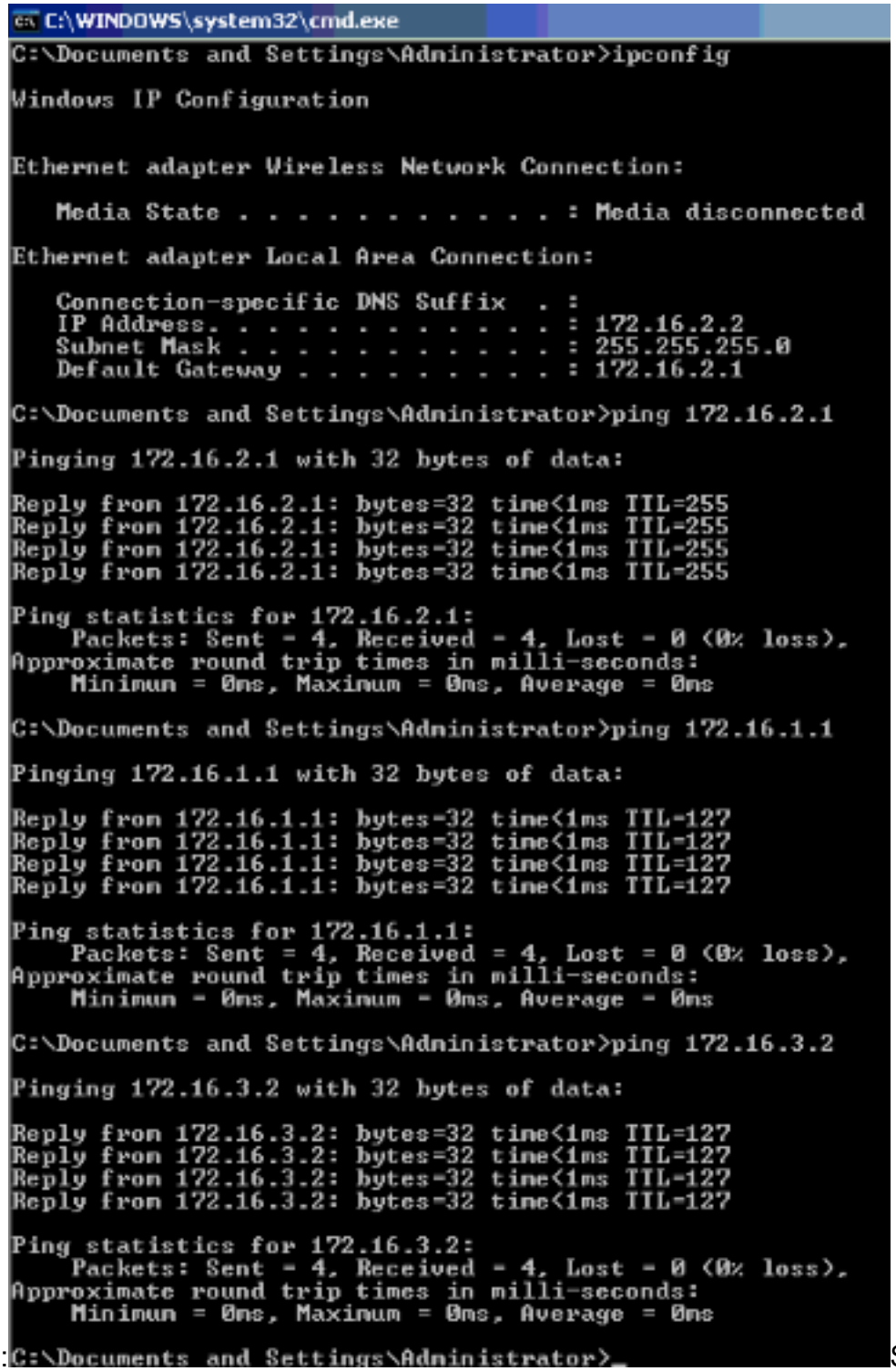
1. Haga clic en el prompt, que este ejemplo

muestra: 

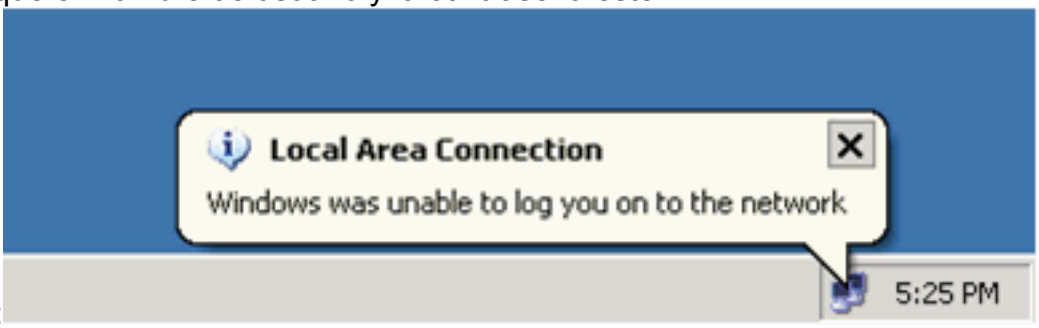
Visualizaciones de la ventana de un Nombre de usuario y de la entrada de contraseña.

2. Ingrese el Nombre de usuario y la contraseña. 

Nota: En el PC1 y 2, ingrese los credenciales de usuario VLAN2 y 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 **ping**. Esta salida es de PC1, y muestra un ping exitoso a PC



4: Si aparece este error, verifique que el Nombre de usuario y la contraseña estén correctos:



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#**show dot1x** Sysauthcontrol = **Enabled** Dot1x Protocol Version = 1 Dot1x Oper Controlled Directions = Both Dot1x Admin Controlled Directions = Both Cat6K#**show dot1x interface fastEthernet 3/2** AuthSM State = AUTHENTICATED BendSM State = IDLE **PortStatus = AUTHORIZED** MaxReq = 2 MultiHosts = Enabled Port Control = Auto QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Cat6K#**show dot1x interface fastEthernet 3/4** AuthSM State = AUTHENTICATED BendSM State = IDLE **PortStatus = AUTHORIZED** MaxReq = 2 MultiHosts = Enabled Port Control = Auto QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds Cat6K#**show dot1x interface fastEthernet 3/1** Default Dot1x Configuration Exists for this interface FastEthernet3/1 AuthSM State = FORCE AUTHORIZED BendSM State = IDLE **PortStatus = AUTHORIZED** MaxReq = 2 MultiHosts = Disabled PortControl = Force Authorized QuietPeriod = 60 Seconds Re-authentication = Disabled ReAuthPeriod = 3600 Seconds ServerTimeout = 30 Seconds SuppTimeout = 30 Seconds TxPeriod = 30 Seconds` Verifique el estado de VLAN después de la autenticación satisfactoria.`Cat6K#**show vlan** VLAN Name Status Ports ---- -------------------- ---------- -------- ------------------------------ 1 default active Fa3/6, Fa3/7, Fa3/8, Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13, Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19, Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25, Fa3/26, Fa3/27, Fa3/28, Fa3/29, Fa3/30, Fa3/31, Fa3/32, Fa3/33, Fa3/34, Fa3/35, Fa3/36, Fa3/37, Fa3/38, Fa3/39, Fa3/40, Fa3/41, Fa3/42, Fa3/43, Fa3/44, Fa3/45, Fa3/46, Fa3/47, Fa3/48 **2 VLAN2 active Fa3/2, Fa3/3 3 VLAN3 active Fa3/4, Fa3/5** 10 RADIUS_SERVER active Fa3/1 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 del 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 Mar 04 2007 06:35 AM Automatic 172.16.2.3 0100.166F.3CA3.42 Mar 04 2007 06:43 AM Automatic 172.16.3.2 0100.145e.945f.99 Mar 04 2007 06:50 AM Automatic 172.16.3.3 0100.1185.8D9A.F9 Mar 04 2007 06:57 AM Automatic` 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.

Troubleshooting

Recoja la salida de estos **comandos debug** para resolver problemas:

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **haga el debug de los eventos del dot1x** — Habilita el debugging de las declaraciones de la impresión guardadas por el indicador de suceso del dot1x.`Cat6K#**debug dot1x events** Dot1x events debugging is on Cat6K# *!--- Debug output for PC 1 connected to Fa3/2.* 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0 00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 **00:13:36: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/2** 00:13:36: dot1x-ev:MAC Address is 0016.3633.339c 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36: dot1x-ev:going to send to backend on SP, length = 6 00:13:36: dot1x-ev:Sent to Bend 00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15 00:13:36: dot1x-ev:Found a process thats already handling therequest for this id 12 00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36: dot1x-ev:going to send to backend on SP, length = 31 00:13:36: dot1x-ev:Sent to Bend 00:13:36: dot1x-ev:Got a Request`

from SP to send it to Radius with id 16 00:13:36: dot1x-ev:Found a process thats already handling therequest for this id 13 **00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32 00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:13:36: dot1x-ev:Vlan name = VLAN2** 00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 16 EAP pkt len = 4 00:13:37: dot1x-ev:The process finished processing the request will pick up any pending requests from the queue Cat6K# Cat6K# *!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0 00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-ev:The Interface on which we got this AAA Request is FastEthernet3/4** 00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:19:58: dot1x-ev:going to send to backend on SP, length = 6 00:19:58: dot1x-ev:Sent to Bend 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9 00:19:58: dot1x-ev:Found a process thats already handling therequest for this id 10 00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:19:58: dot1x-ev:going to send to backend on SP, length = 31 00:19:58: dot1x-ev:Sent to Bend 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10 00:19:58: dot1x-ev:Found a process thats already handling therequest for this id 11 **00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32 00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:19:58: dot1x-ev:Vlan name = 3** 00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4 00:19:58: dot1x-ev:The process finished processing the request will pick up any pending requests from the queue Cat6K#

- debug radius - Muestra información asociada con RADIUS.Cat6K#**debug radius** Radius protocol debugging is on Cat6K# *!--- Debug output for PC 1 connected to Fa3/2.* 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18 CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79 00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18 172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80 18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104 00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80 18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19 172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80 18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124 00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8 01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFE 00:13:36: Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18 11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# *!--- Debug output for PC 3 connected to Fa3/4.* 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11 172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login:

```
length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58:
RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request,
len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS:
Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33
010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58:
RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from
radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in
nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1
00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request,
len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58:
Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343
00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS:
Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6
0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58:
Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004
00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-
login: length of eap packet = 4 Cat6K#
```

Información Relacionada

- Autenticación del IEEE 802.1X con el Catalyst 6500/6000 que funciona con el ejemplo de configuración del software CatOS
- 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
- Configurar la autenticación del acceso basado del IEEE 802.1X
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems