Ejemplo de Configuración de Autenticación IEEE 802.1x con Catalyst 6500/6000 que Ejecuta Cisco IOS Software

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Antecedentes
Configurar
Diagrama de la red
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
Verificación
Clientes de PC
Catalyst 6500
Troubleshoot
Información Relacionada

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.

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 Cisco IOS Software Release 12.2(18)SXF en Supervisor Engine**Nota:** Necesita Cisco IOS Software Release 12.1(13)E o posterior para soportar la autenticación basada en puerto 802.1x.
- 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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

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

Nota: Si el switch recibe paquetes EAPOL del puerto que no está configurado para la autenticación 802.1x o si el switch no soporta la autenticación 802.1x, los paquetes EAPOL se descartan y no se reenvían a ningún dispositivo ascendente.

Configurar

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

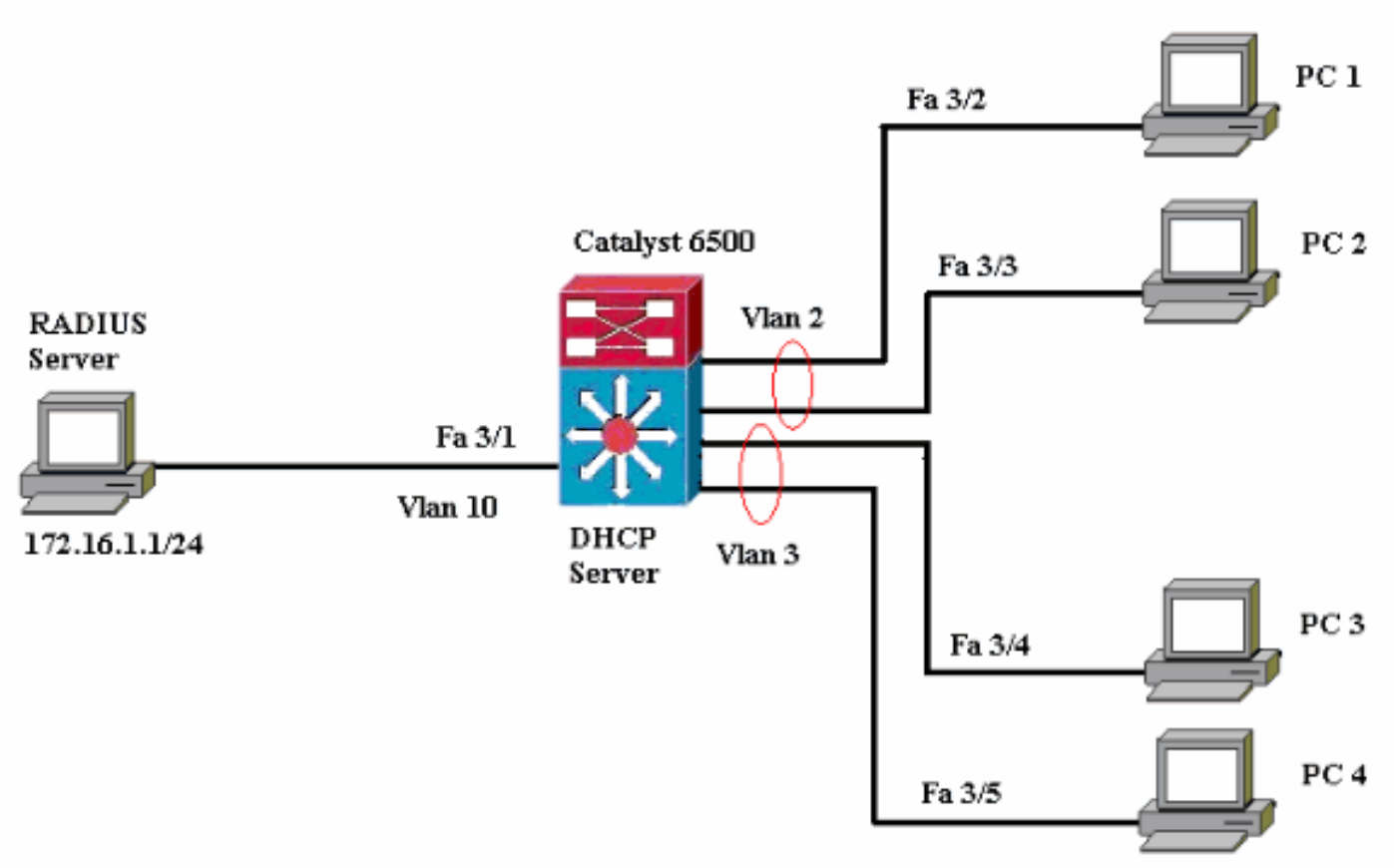
La configuración requiere estos pasos:

- Configure el switch Catalyst para la autenticación 802.1x.
- Configure el servidor RADIUS.

- Configure 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. Solicita información de identidad del cliente, verifica esa información con el servidor RADIUS y retransmite 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 utilizan la misma credencial de inicio de sesión que en VLAN 2. De manera similar, los PC 3 y 4 utilizan una credencial de inicio de sesión para VLAN 3. Los clientes PC se configuran para obtener la dirección IP de un servidor DHCP.

Configuración del switch Catalyst para la autenticación 802.1x

Esta configuración de switch de ejemplo incluye:

- Cómo habilitar la autenticación 802.1x en los puertos FastEthernet.
- Cómo conectar un servidor RADIUS a la VLAN 10 detrás del puerto FastEthernet 3/1.
- Una configuración de servidor DHCP para dos grupos IP, uno para clientes en VLAN 2 y el otro para clientes en VLAN 3.
- Routing entre VLAN para tener conectividad entre clientes después de la autenticación.

Refiérase a Pautas y Restricciones de Autenticación Basada en Puerto 802.1x para 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

```
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
```

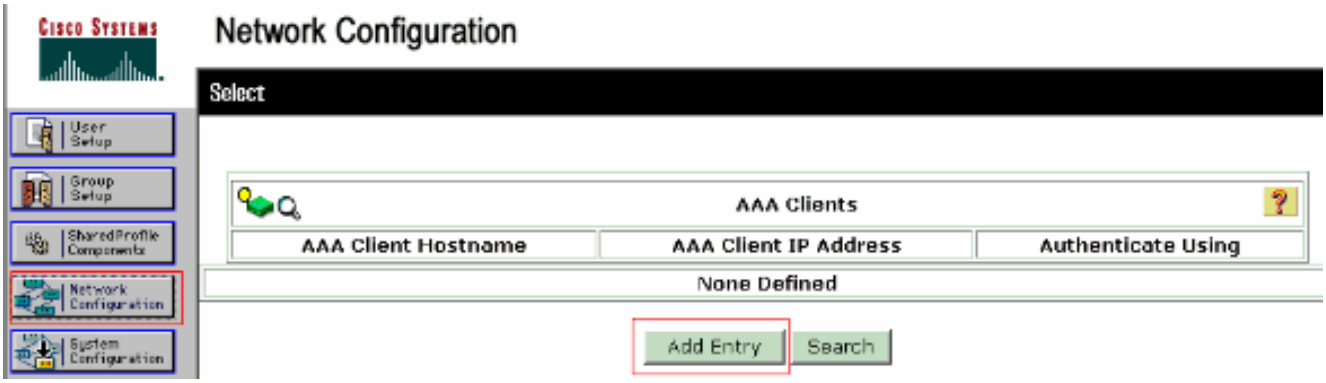
```
server. Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 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 (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

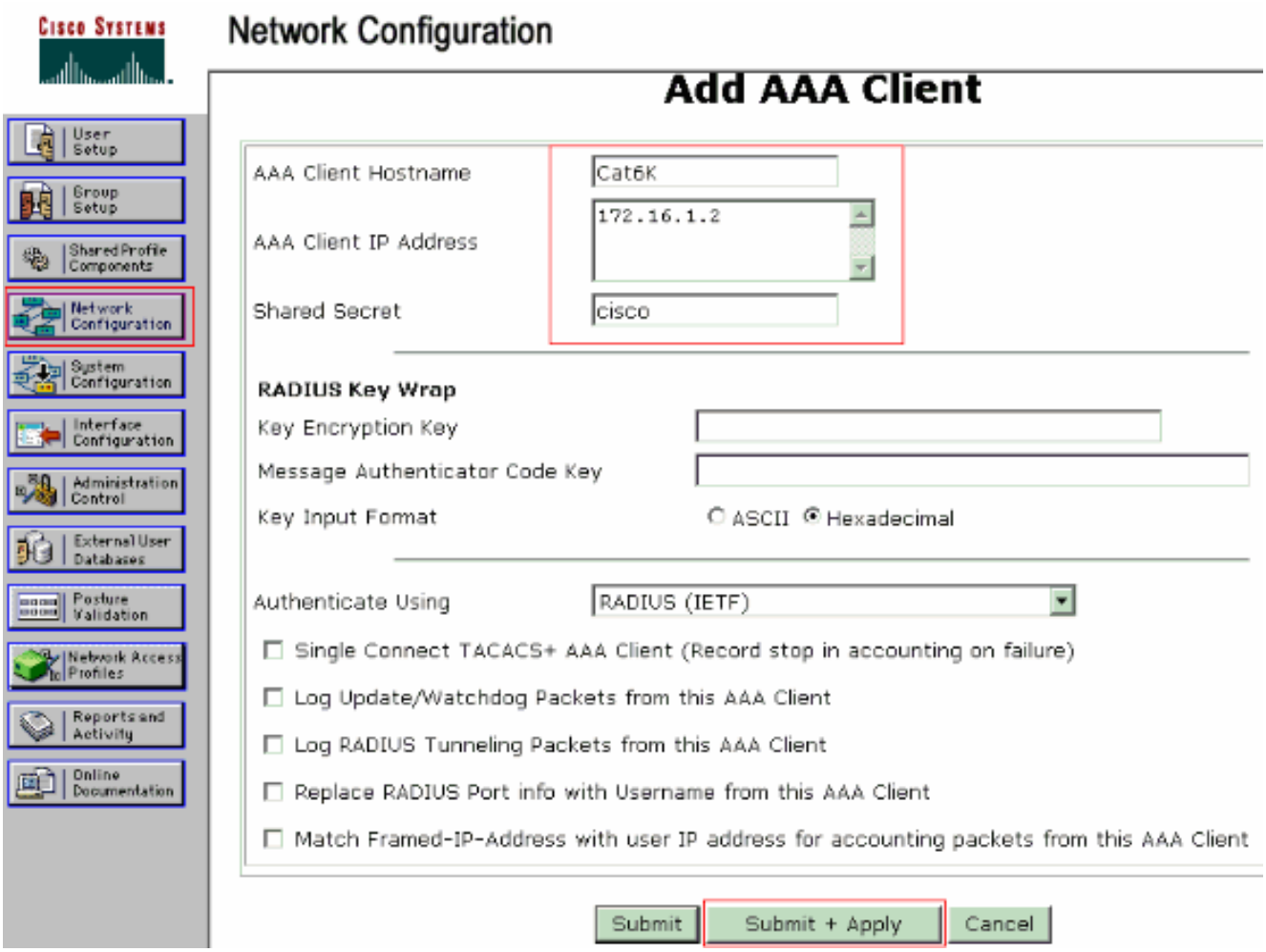
Configuración del servidor RADIUS

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



3. Configure el nombre de host del cliente AAA, la dirección IP, la clave secreta compartida y el tipo de autenticación como:Nombre de host del cliente AAA = Nombre de host del switch (**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 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:

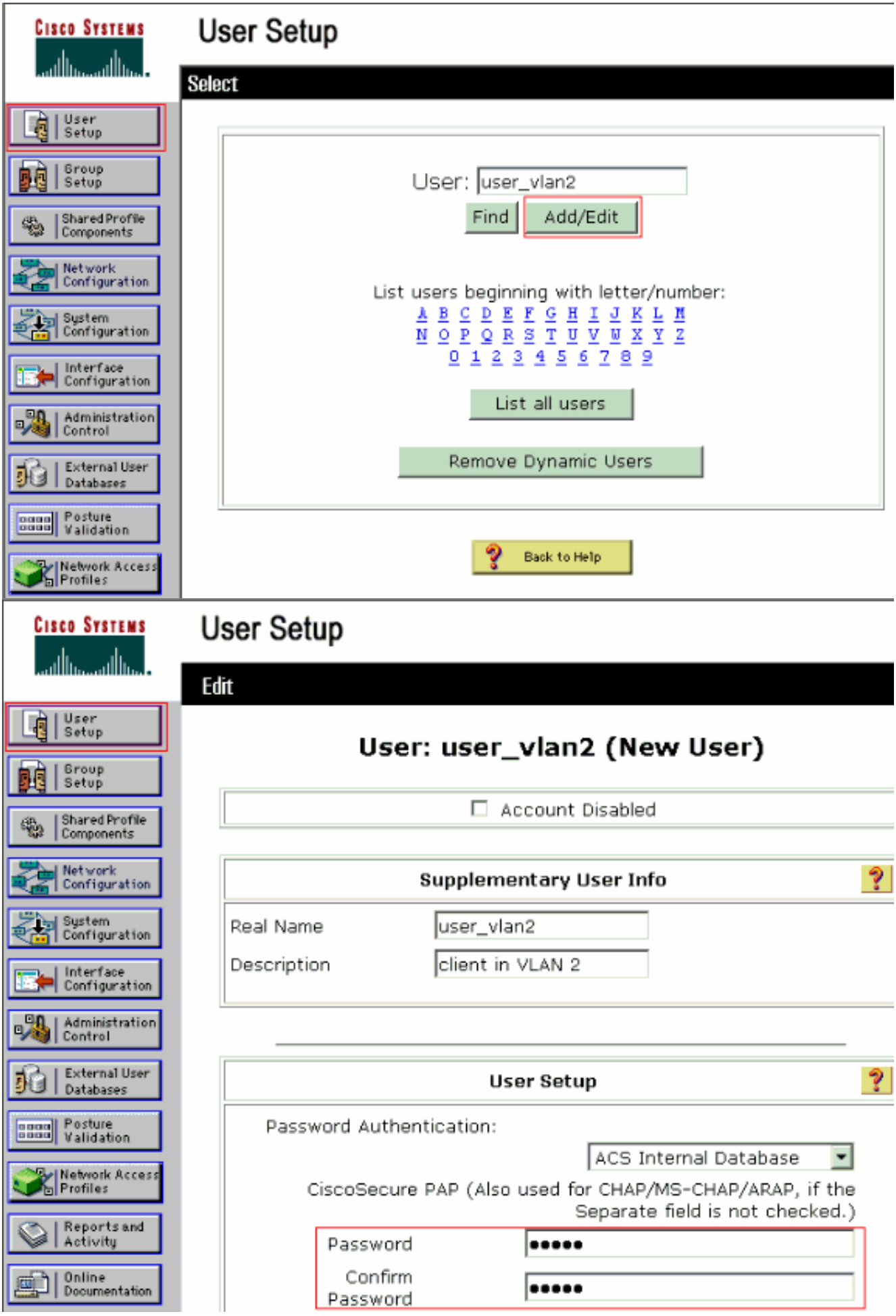


Complete estos pasos para configurar el servidor RADIUS para la autenticación, VLAN y la asignación de dirección IP.

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

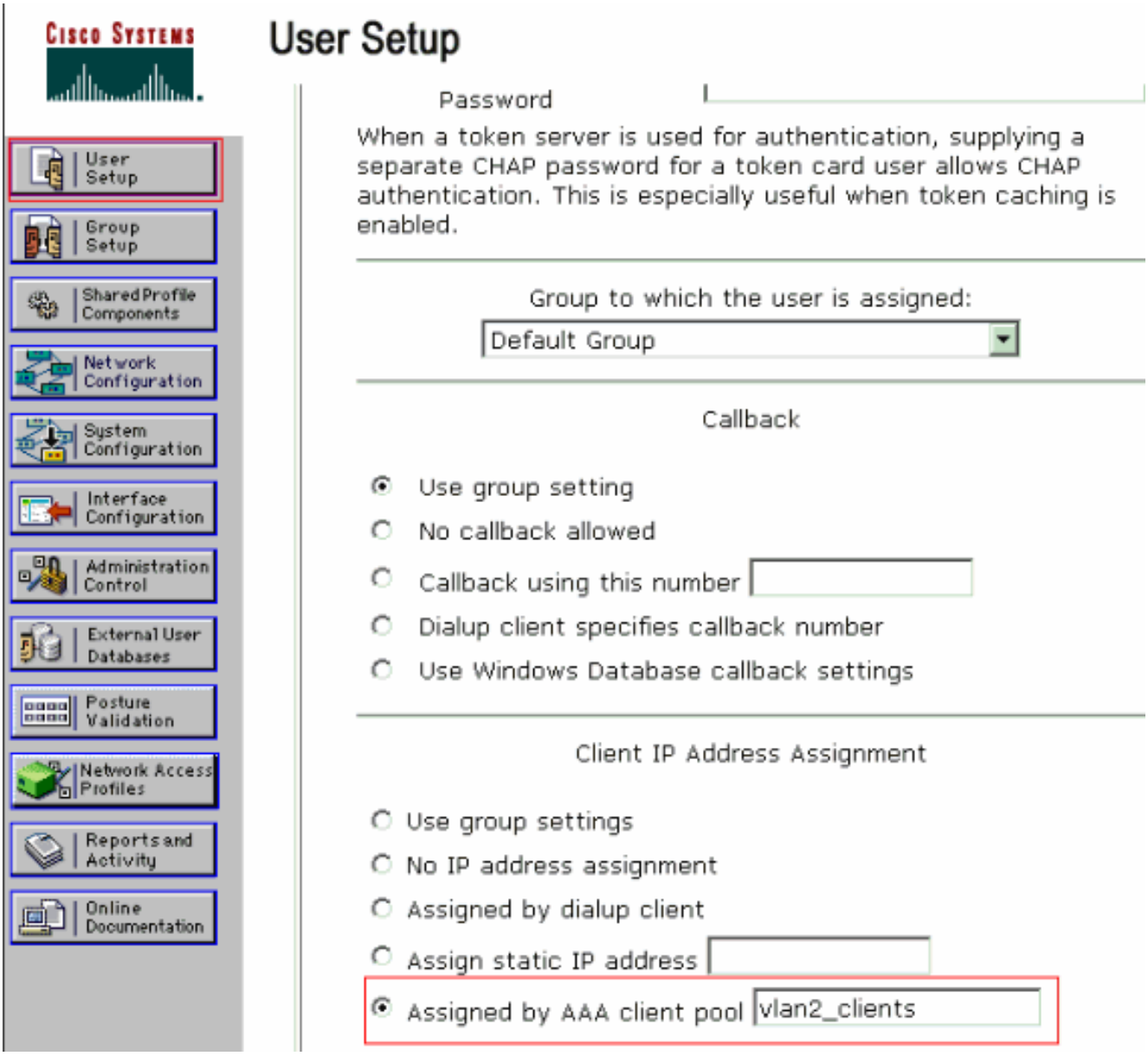
Nota: Aquí, se muestra la configuración del usuario para los clientes que se conectan sólo a VLAN 2. Para los usuarios que se conectan a VLAN 3, siga el mismo procedimiento.

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



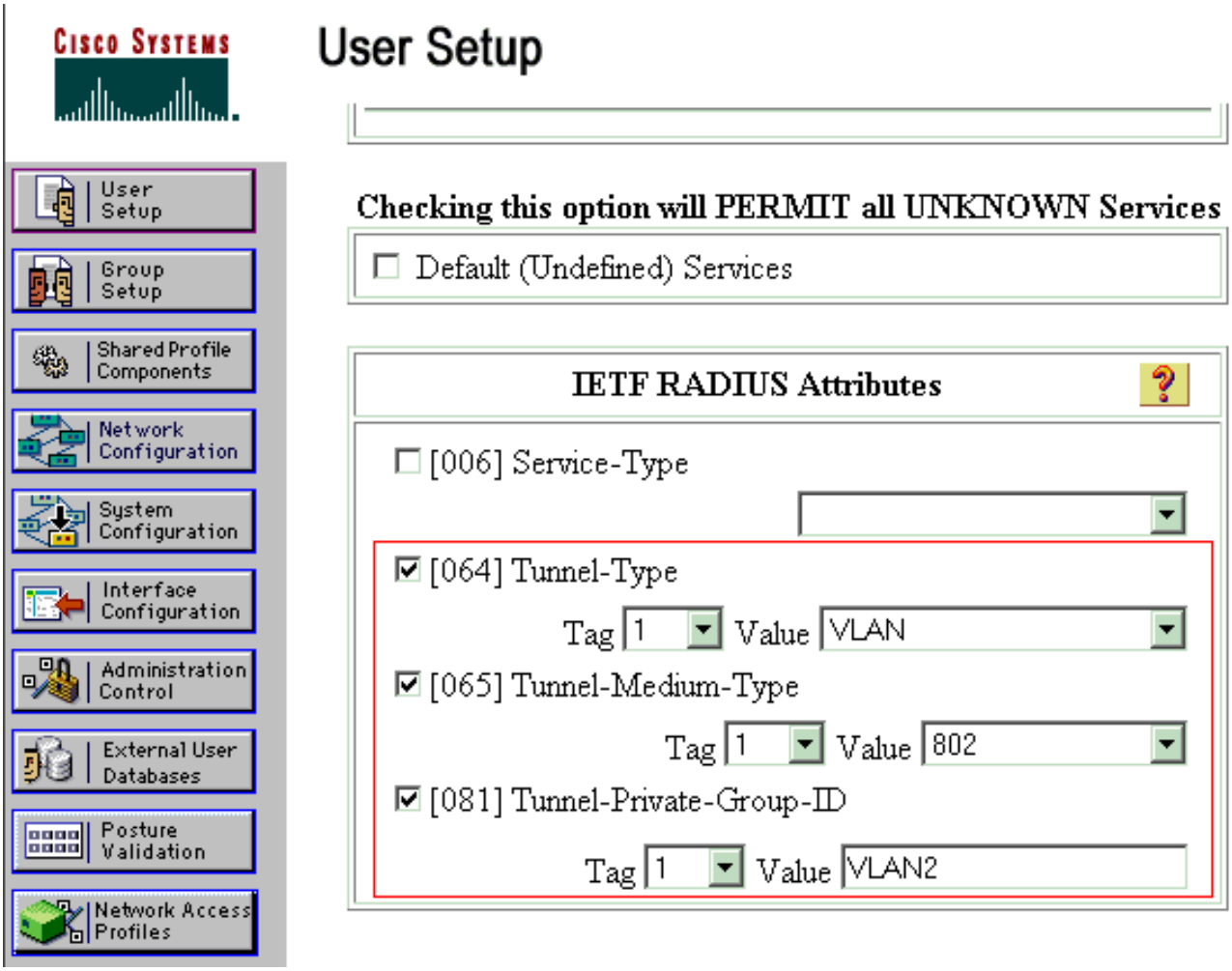
2. Defina la asignación de dirección IP del cliente como **Asignado por el conjunto de clientes AAA**. Introduzca el nombre del conjunto de direcciones IP configurado en el switch para los

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** del Grupo de Trabajo de Ingeniería de Internet (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 o *número* de VLAN que corresponda.**Nota:** Si utiliza el *nombre* de VLAN, debe ser exactamente igual al configurado en el
switch.



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

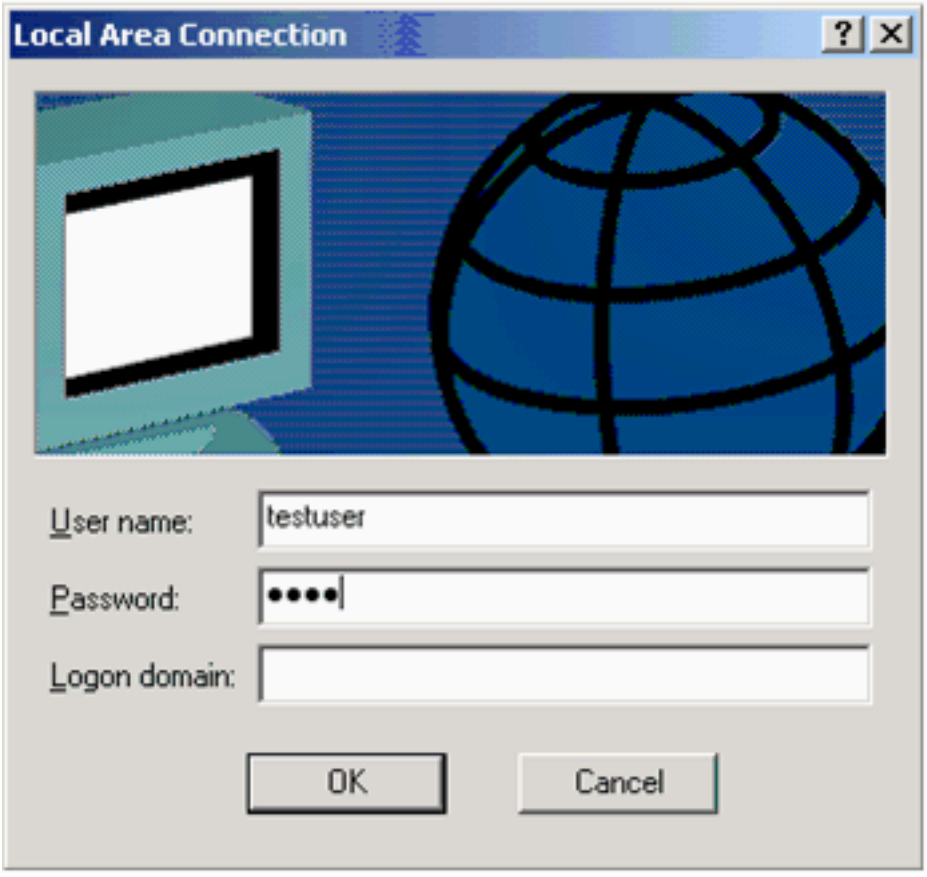
```
%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
VLAN cannot be assigned.
```

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

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

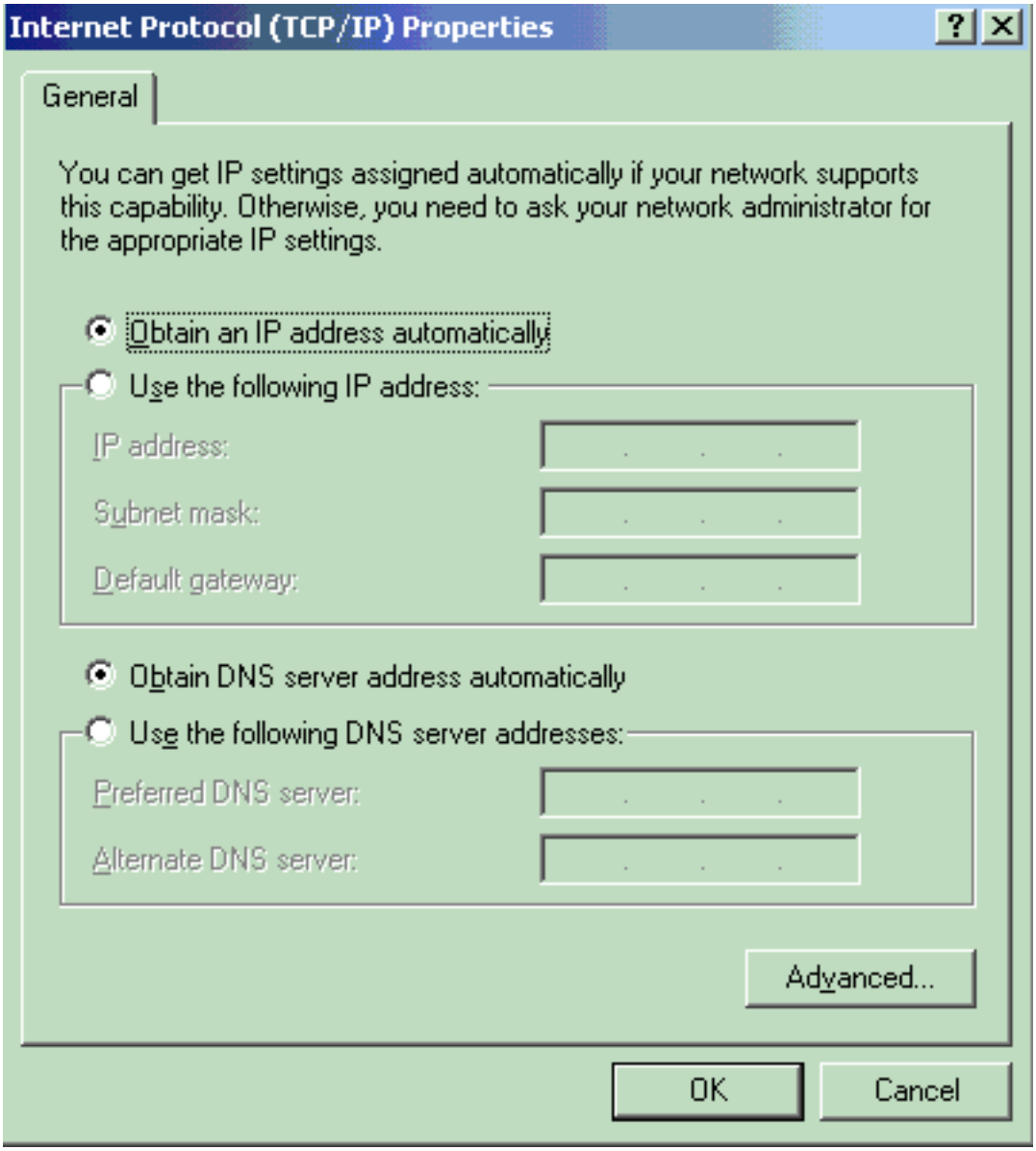
1. Elija **Inicio > Panel de control > Conexiones de red**, luego haga clic con el botón derecho en

su **Conexión de área local** y elija **Propiedades**.
2. Marque **Mostrar icono en el área de notificación cuando esté conectado** en la ficha General.
3. En la ficha Authentication (Autenticación), marque Enable IEEE 802.1x authentication para habilitar la autenticación en esta red.
4. Establezca el tipo EAP en MD5-Challenge tal como se muestra en el ejemplo:



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

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

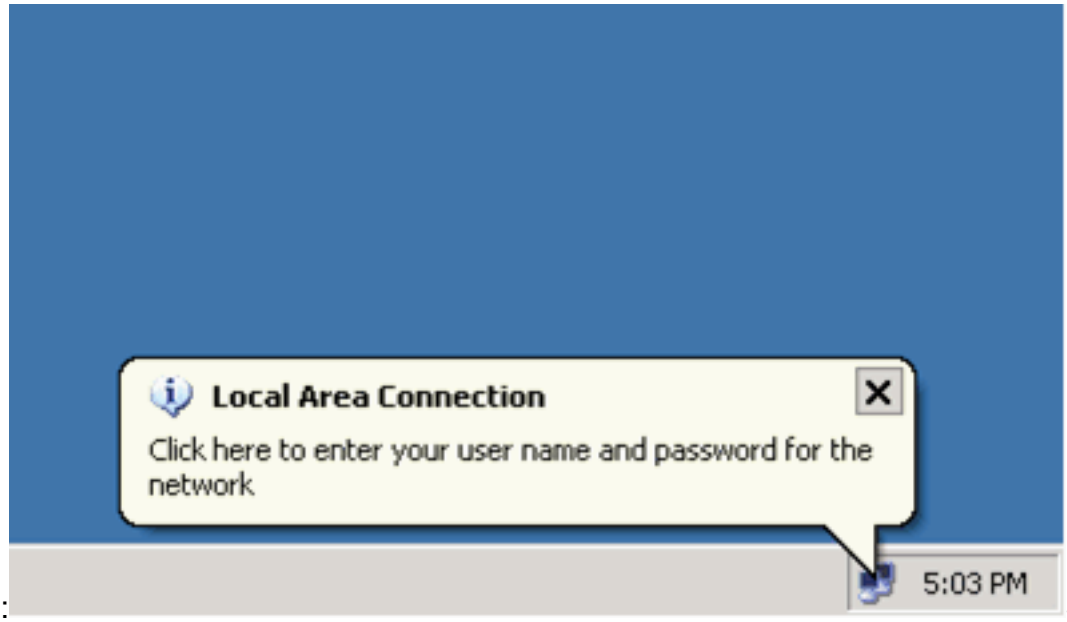


Verificación

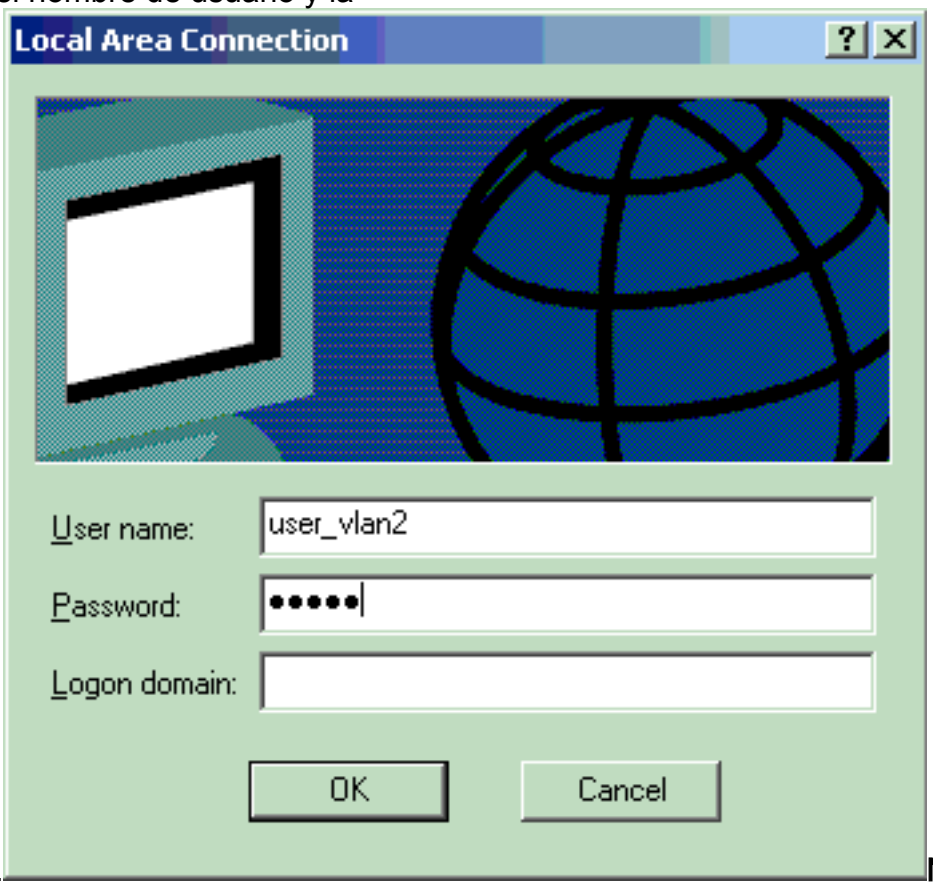
Clientes de PC

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

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

ejemplo: 

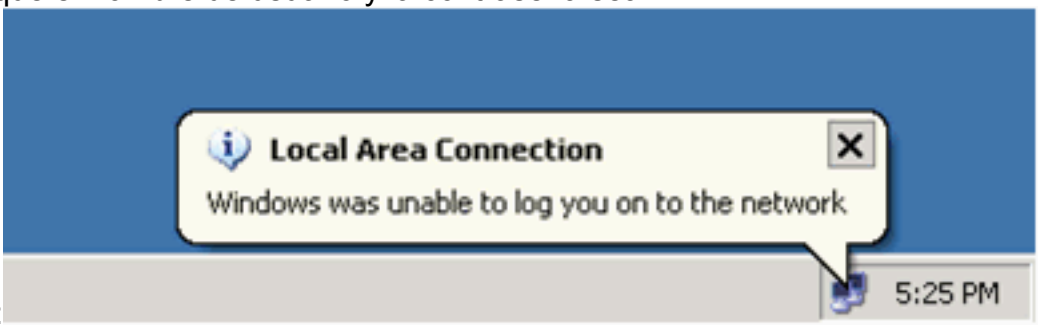
Se muestra una ventana de entrada de nombre de usuario y contraseña.

2. Introduzca el nombre de usuario y la contraseña. 

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

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Wireless Network Connection:

   Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 172.16.2.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.2.1

C:\Documents and Settings\Administrator>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:

Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.3.2

Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

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 AUTHORIZED.

```
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 exitosa.

```
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 estado de enlace DHCP desde el después de la autenticación exitosa.

```
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.

Troubleshoot

Recopile el resultado de estos comandos **debug** para resolver problemas:

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

- **debug dot1x events**: habilita la depuración de sentencias de impresión protegidas por el indicador de eventos 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

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