IEEE 802.1x-verificatie met Catalyst 6500/6000-actieve CatOS-softwareconfiguratievoorbeeld

Inhoud

Inleiding

Dit document legt uit hoe u IEEE 802.1x kunt configureren op een Catalyst 6500/6000-server die werkt in een hybride modus (CatOS op de Supervisor Engine en Cisco IOS® Software op de MSFC) en een RADIUS-server (Dial-In User Service) van afstandsverificatie voor verificatie en VLAN-toewijzing.

Voorwaarden

Vereisten

Lezers van dit document zouden kennis moeten hebben van deze onderwerpen:

- Installatiegids voor Cisco Secure ACS voor Windows 4.1
- Gebruikershandleiding voor Cisco Secure Access Control Server 4.1
- Hoe werkt RADIUS?
- Catalyst-switching- en ACS-implementatiegids

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 6500 met CatOS-softwarerelease 8.5(6) op de Supervisor Engine en Cisco IOS-softwarerelease 12.2(18)SXF op de MSFC**Opmerking:** U hebt CatOS release 6.2 of hoger nodig om 802.1x poortgebaseerde verificatie te ondersteunen.**Opmerking:** Voordat de softwarerelease 7.2(2)**,** wanneer de 802.1x-host is geauthentificeerd, wordt er toegevoegd aan een VLAN dat door NVRAM is geconfigureerd. Met softwarerelease 7.2(2) en latere releases, na verificatie, kan een 802.1x-host de VLAN-toewijzing van de RADIUS-server ontvangen.
- Dit voorbeeld gebruikt Cisco Secure Access Control Server (ACS) 4.1 als RADIUS-server.**Opmerking:** Er moet een RADIUS-server worden opgegeven voordat 802.1x in de switch kan worden ingeschakeld.
- PC klanten die 802.1x authenticatie ondersteunen.**Opmerking:** Dit voorbeeld gebruikt Microsoft Windows XP-clients.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

De standaard IEEE 802.1x definieert een op clientserver gebaseerd toegangscontrole- en verificatieprotocol dat onbevoegde apparaten beperkt tot het aansluiten op een netwerk via publiekelijk toegankelijke poorten. 802.1x controleert netwerktoegang door bij elke poort twee verschillende virtuele toegangspunten te creëren. Eén toegangspunt is een ongecontroleerde haven; het andere is een gecontroleerde haven . Al het verkeer door één poort is beschikbaar voor beide toegangspunten. 802.1x verklaart elk gebruikersapparaat dat met een switch poort is verbonden en wijst de poort op een VLAN toe voordat u om het even welke services beschikbaar maakt die door de switch of LAN worden aangeboden. Totdat het apparaat voor authentiek is verklaard, staat 802.1x-toegangscontrole alleen Verkeersverkeer via LAN (EAPOL) via de poort waarop het apparaat is aangesloten toe. Nadat de authenticatie succesvol is, kan het normale verkeer door de poort gaan.

Configureren

In deze sectie wordt u gepresenteerd met de informatie om de 802.1x optie te configureren die in dit document wordt beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

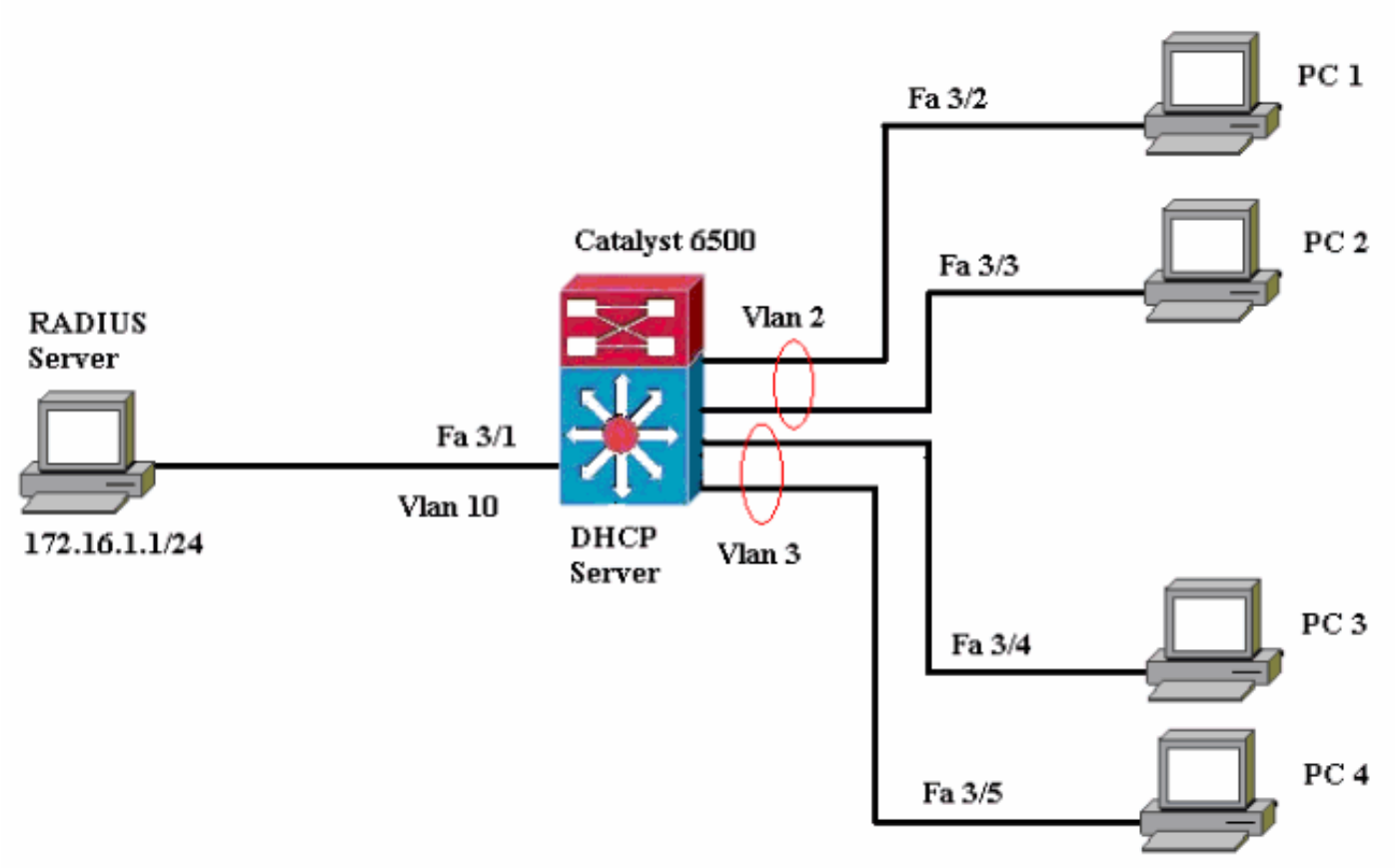
Voor deze configuratie zijn de volgende stappen vereist:

- Configureer de Catalyst Switch voor 802.1x-verificatie

- De RADIUS-server configureren
- Configuratie van de PC Clients om 802.1x verificatie te gebruiken

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



- RADIUS server-voert de eigenlijke authenticatie van de client uit. De RADIUS-server bevestigt de identiteit van de client en deelt de switch mee of de client al dan niet is geautoriseerd om toegang te krijgen tot de LAN- en switch-services. Hier wordt de RADIUS-server ingesteld voor verificatie en VLAN-toewijzing.
- Switch-controleert de fysieke toegang tot het netwerk op basis van de authenticatiestatus van de client. De switch fungeert als een intermediair (proxy) tussen de client en de RADIUS-server, vraagt om identiteitsinformatie van de client, verifieert die informatie met de RADIUS-server en geeft een reactie op de client door. Hier wordt de Catalyst 6500 switch ook geconfigureerd als een DHCP-server. Met de ondersteuning voor 802.1x-verificatie voor het Dynamic Host Configuration Protocol (DHCP) kan de DHCP-server de IP-adressen toewijzen aan de verschillende klassen van eindgebruikers door de geauthenticeerde gebruikersidentiteit in het DHCP-zoekproces toe te voegen.
- Clients-De apparaten (werkstations) die om toegang tot de LAN- en switch-services verzoeken en op verzoeken van de switch reageren. Hier zijn PC's 1 tot 4 de klanten die een geauthentiseerde netwerktoegang vragen. PCs 1 en 2 zullen de zelfde openings van een opening van een netwerkverbinding gebruiken om in VLAN 2 te zijn. Op dezelfde manier zullen PCs 3 en 4 een openings van een verbinding voor VLAN 3 gebruiken. PC cliënten worden gevormd om het IP adres van een server van DHCP te bereiken.**Opmerking:** In deze configuratie wordt elke client die de verificatie niet heeft voltooid of elke niet-802.1x geschikte client die verbinding maakt met de switch, netwerktoegang ontzegd door ze naar een

ongebruikt VLAN (VLAN 4 of 5) te verplaatsen met behulp van de verificatie-mislukking en de functies van gastVLAN.

Configureer de Catalyst Switch voor 802.1x-verificatie

Deze configuratie van de switch omvat:

- 802.1x-verificatie en bijbehorende functies op FastEthernet-poorten inschakelen.
- Sluit RADIUS-server aan op VLAN 10 achter Fast Ethernet-poort 3/1.
- DHCP-serverconfiguratie voor twee IP-pools, één voor klanten in VLAN 2 en andere voor klanten in VLAN 3.
- Routing tussen VLAN's om connectiviteit tussen klanten na verificatie te hebben.

Raadpleeg de Verificatierichtlijnen voor de richtlijnen over het configureren van 802.1x verificatie.

Opmerking: Zorg ervoor dat de RADIUS-server altijd achter een geautoriseerde poort verbonden is.

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
```

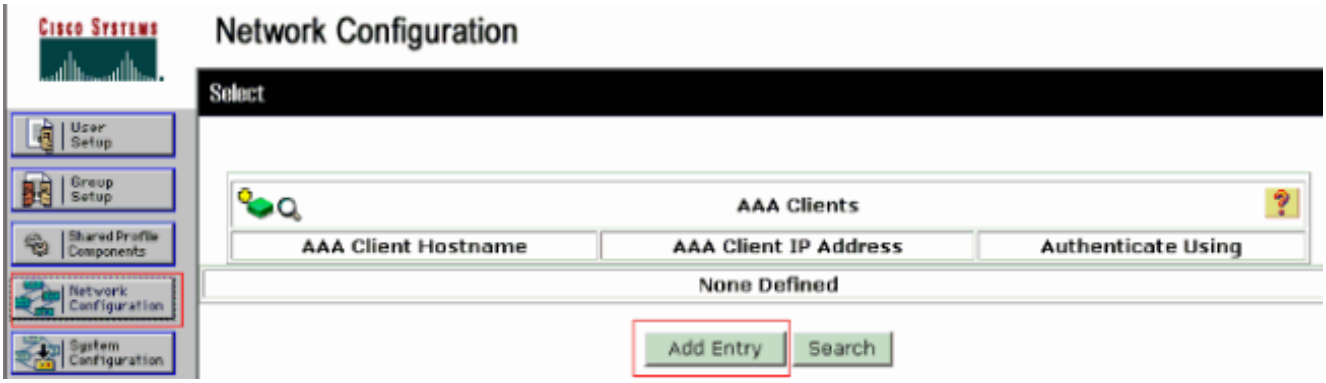
```
!--- This is used as the gateway address in RADIUS
server. Router(config-if)#no shut
Router(config-if)#interface vlan 2
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#no shut
!--- This is the gateway address for clients in VLAN 2.
Router(config-if)#interface vlan 3
Router(config-if)#ip 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)
```

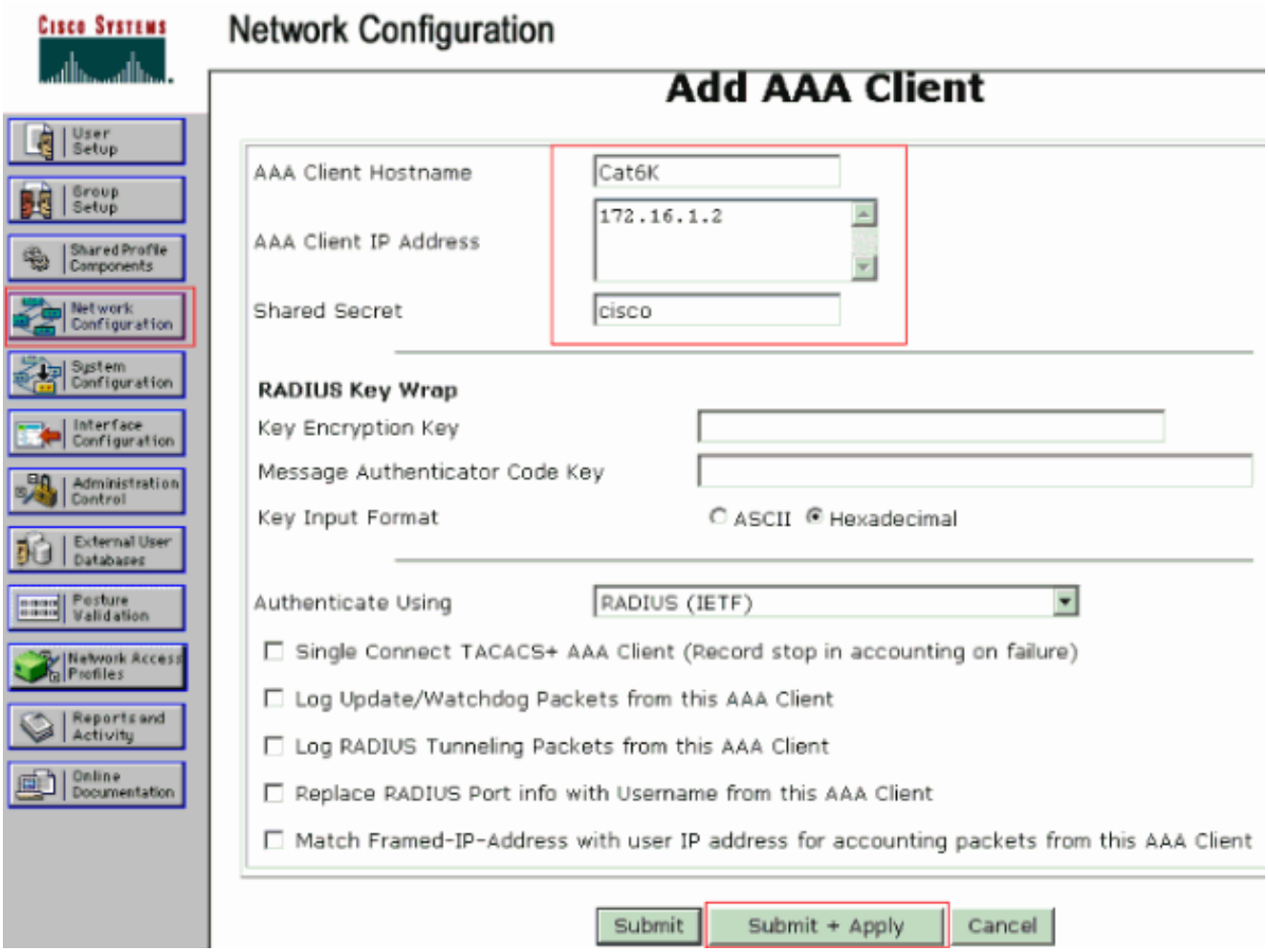
De RADIUS-server configureren

De RADIUS-server is geconfigureerd met een statisch IP-adres van 172.16.1.1/24. Voltooi deze stappen om de RADIUS-server voor een AAA-client te configureren:

1. Klik om een AAA-client te configureren op **Network Configuration** in het ACS-beheervenster.
2. Klik op **Ingang toevoegen** onder het kopje AAA-clients.



3. Configureer de AAA client-hostname, IP-adres, gedeelde geheime sleutel en type verificatie als volgt:AAA client hostname = Switch Hostname (**Cat6K**).AAA client-IP-adres = Management interface (SC0) IP-adres van de switch (**172.16.1.2**).Gedeeld geheim = Radius Key ingesteld op de switch (**cisco**).Verifieer het gebruik met = **RADIUS IETF**.**Opmerking:** Voor een correct gebruik moet de gedeelde geheime sleutel identiek zijn op de AAA-client en ACS. Toetsen zijn hoofdlettergevoelig.
4. Klik op **Inzenden + Toepassen** om deze veranderingen effectief te maken, zoals dit voorbeeld toont:



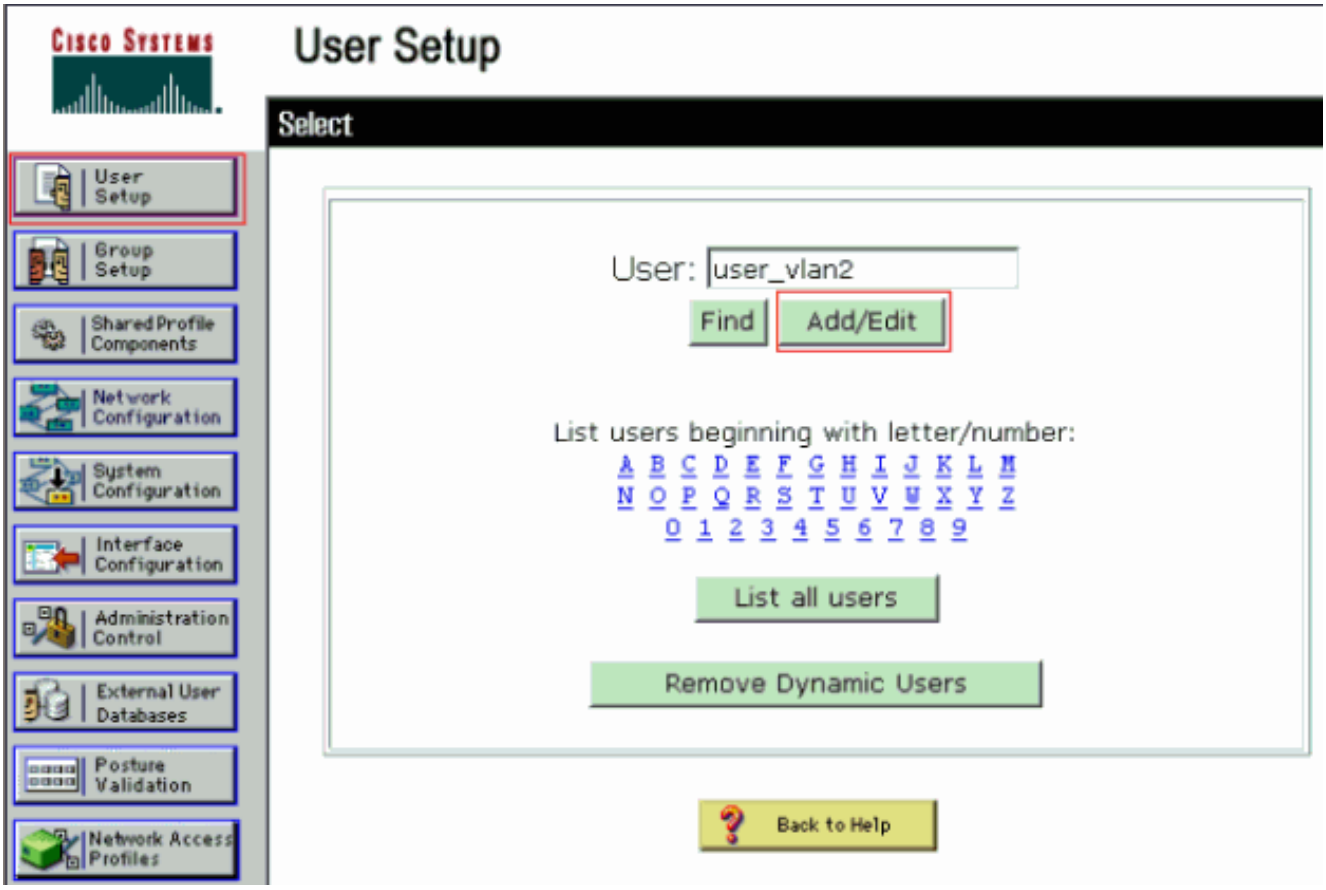
Voltooi deze stappen om de RADIUS-server voor verificatie, VLAN en IP-adrestoewijzing te configureren:

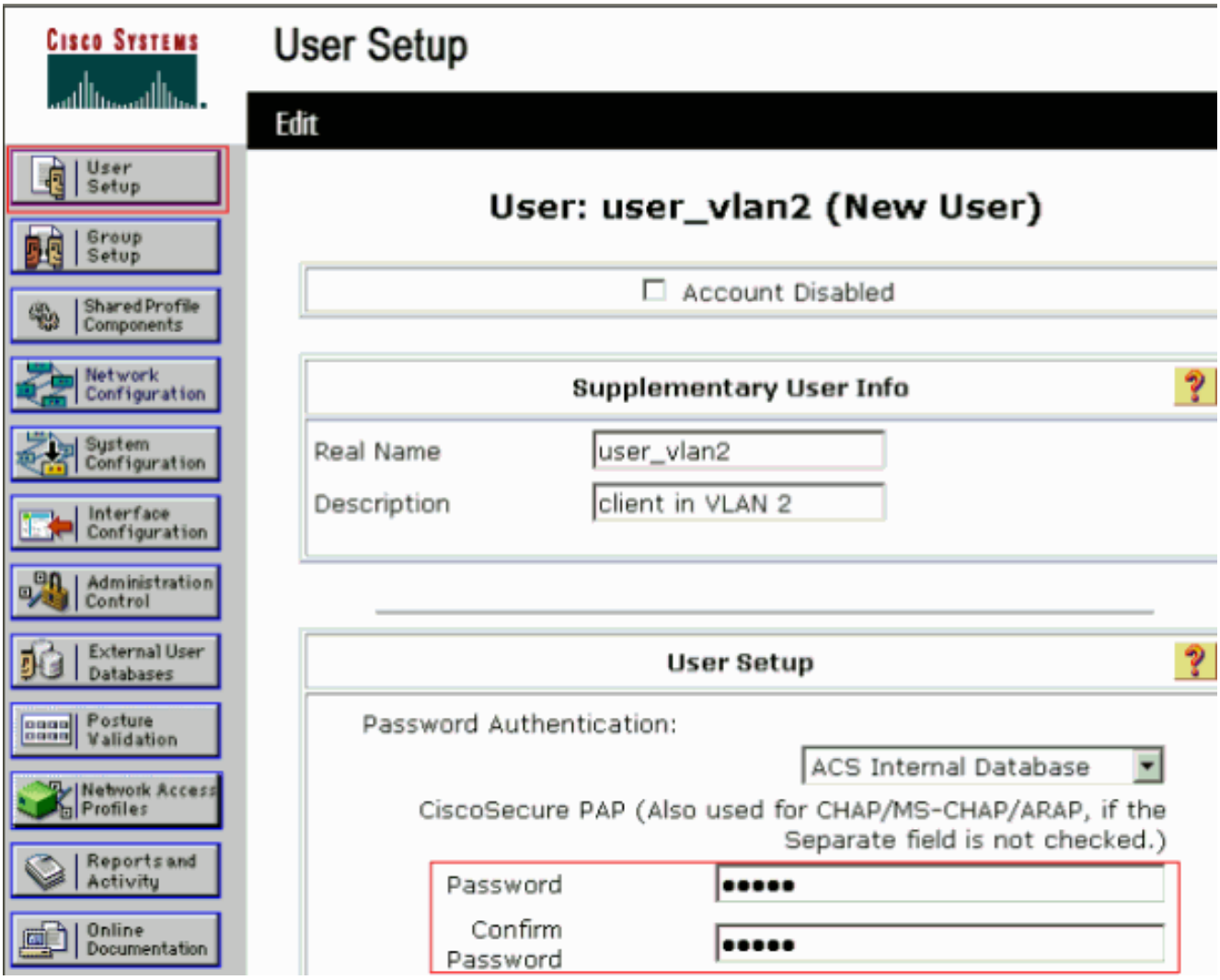
Twee gebruikersnamen moeten afzonderlijk worden gemaakt voor klanten die zich verbinden met

VLAN 2 zowel als voor VLAN 3. Hier wordt een gebruiker **user_VLAN2** voor klanten die met VLAN 2 verbinden en een andere gebruiker **user_VLAN3** voor klanten die met VLAN 3 verbinden gecreëerd voor dit doel.

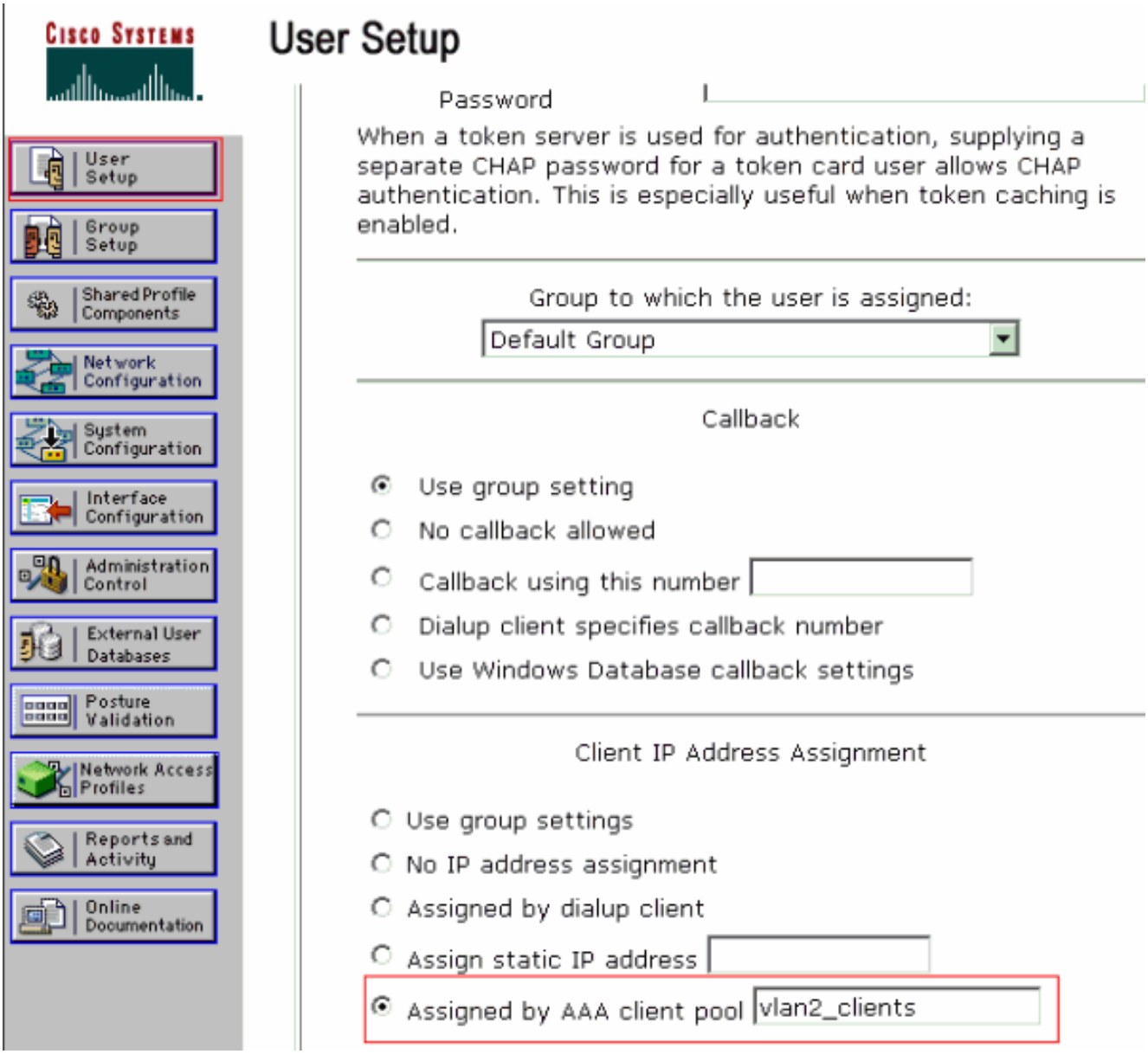
Opmerking: Hier wordt de gebruikersconfiguratie weergegeven voor klanten die alleen VLAN 2 aansluiten. Voor gebruikers die verbinding maken met VLAN 3, voltooien de zelfde procedure.

1. Om gebruikers toe te voegen en te configureren klikt u op **Gebruikersinstelling** en bepaalt u de gebruikersnaam en het wachtwoord.



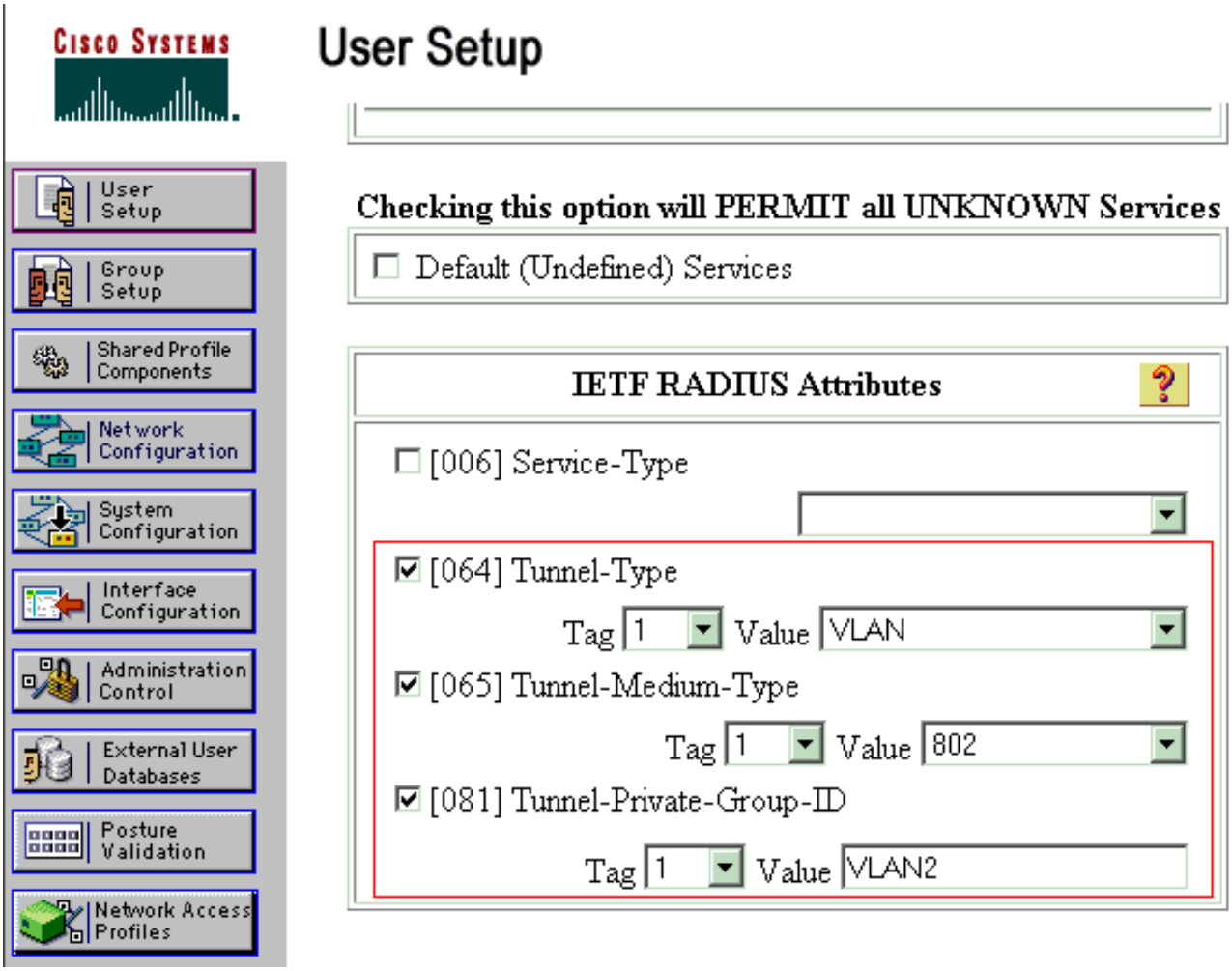


2. Defineert de client-IP-adrestoewijzing zoals **toegewezen door AAA-clientpool**. Voer de naam in van de IP-adrespool die op de switch voor VLAN 2-clients is ingesteld.



Opmerking: Selecteer deze optie en typ de naam van de AAA-client-IP-pool in het vak. Alleen als deze gebruiker het IP-adres wil toewijzen door een IP-adresgroep op de AAA-client te configureren.

3. Defineert de eigenschappen van de Internet Engineering Task Force (IETF) 64 en 65.Zorg ervoor dat de tags van de waarden op 1 zijn ingesteld, zoals in dit voorbeeld wordt weergegeven. Catalyst negeert een andere tag dan 1. Om een gebruiker aan een specifiek VLAN toe te wijzen, moet u eigenschap 81 ook definiëren met een VLAN-*naam* die correspondeert.**Opmerking:** de *naam* van VLAN zou precies hetzelfde moeten zijn als de naam die in de switch is ingesteld.**Opmerking:** VLAN-toewijzing op basis van VLAN-*nummer* wordt niet ondersteund met
CatOS.



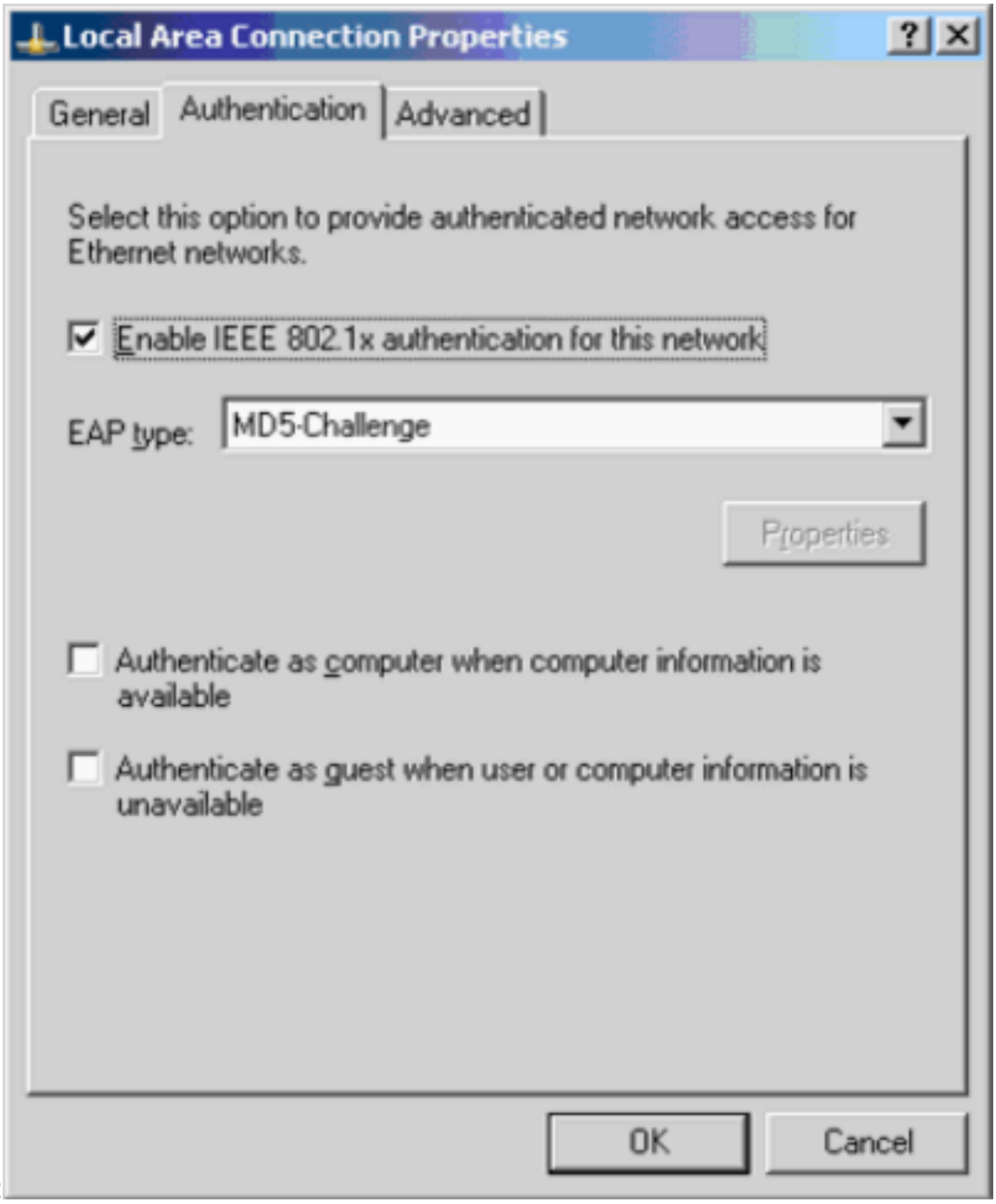
Raadpleeg RFC 2868: RADIUS-kenmerken voor tunnelprotocolondersteuning voor meer informatie over deze IETF-kenmerken.**Opmerking:** In de eerste configuratie van de ACS-server kunnen de RADIUS-kenmerken van IETF niet worden weergegeven in de **gebruikersinstelling**. Kies **interfaceconfiguratie > RADIUS (IETF)** om IETF-eigenschappen in het configuratiescherm van de gebruiker in te schakelen. Controleer vervolgens de eigenschappen **64**, **65** en **81** in de User and Group kolommen.

Configuratie van de PC Clients om 802.1x verificatie te gebruiken

Dit voorbeeld is specifiek voor de Microsoft Windows XP Extensible Authentication Protocol (EAP) over LAN (EAPOL) client. Voer de volgende stappen uit:

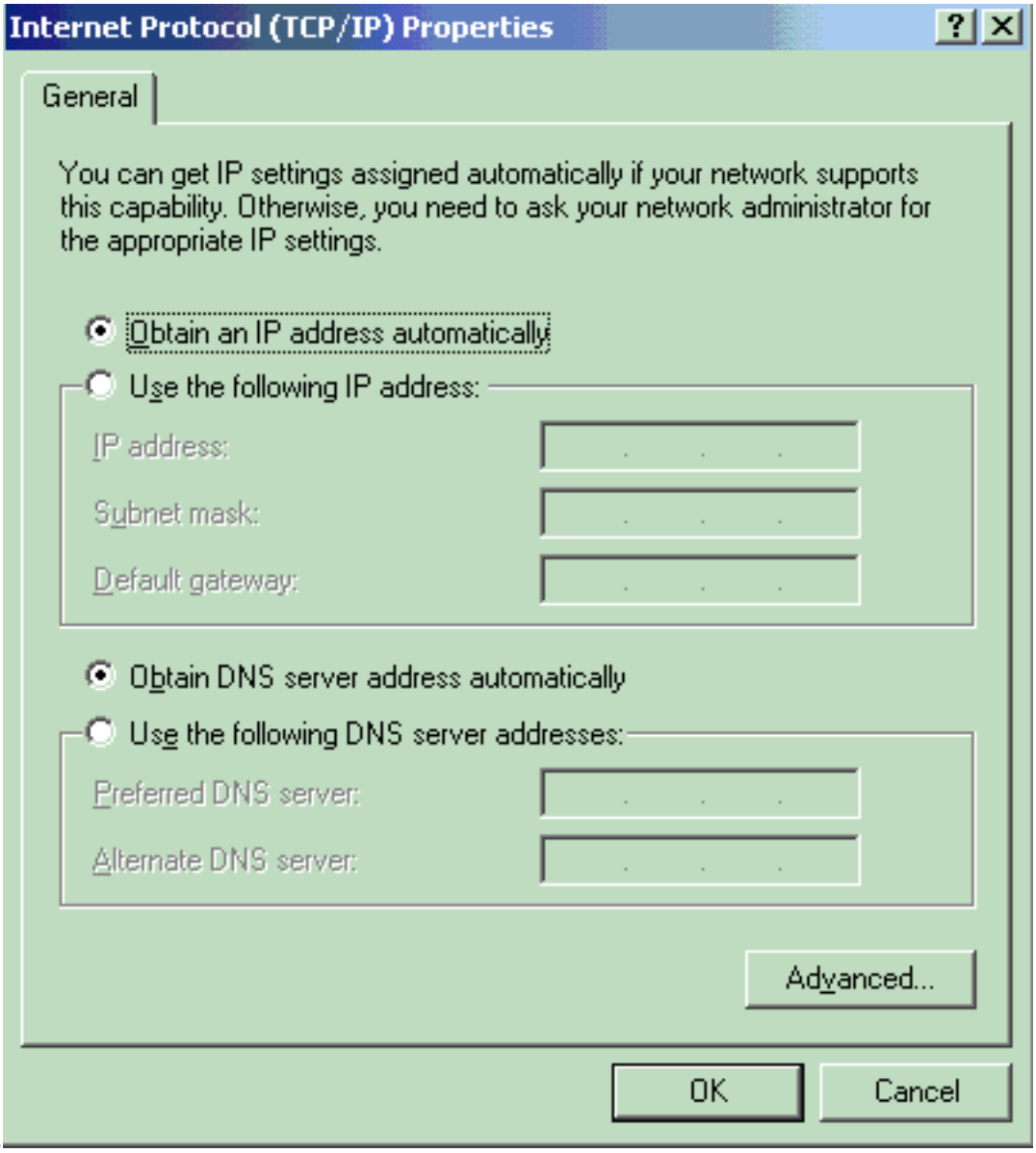
1. Kies **Start > Control Panel > Network Connections**, klik met de rechtermuisknop op uw **Local Area Connection** en kies **Properties**.
2. Controleer **pictogram in waarschuwing** op **het** tabblad Algemeen.
3. Controleer onder het tabblad Verificatie de **verificatie van IEEE 802.1x voor dit netwerk in**.
4. Stel het EAP-type in op **MD5-Challenge**, zoals dit voorbeeld laat

zien:



Voltooi deze stappen om de clients te configureren om een IP-adres te verkrijgen van een DHCP-server:

1. Kies **Start > Control Panel > Network Connections**, klik met de rechtermuisknop op uw **Local Area Connection** en kies **Properties**.
2. Klik onder het tabblad General op **Internet Protocol (TCP/IP)** en vervolgens op **Properties**.
3. Kies **automatisch een IP-adres**



verkrijgen.

Verifiëren

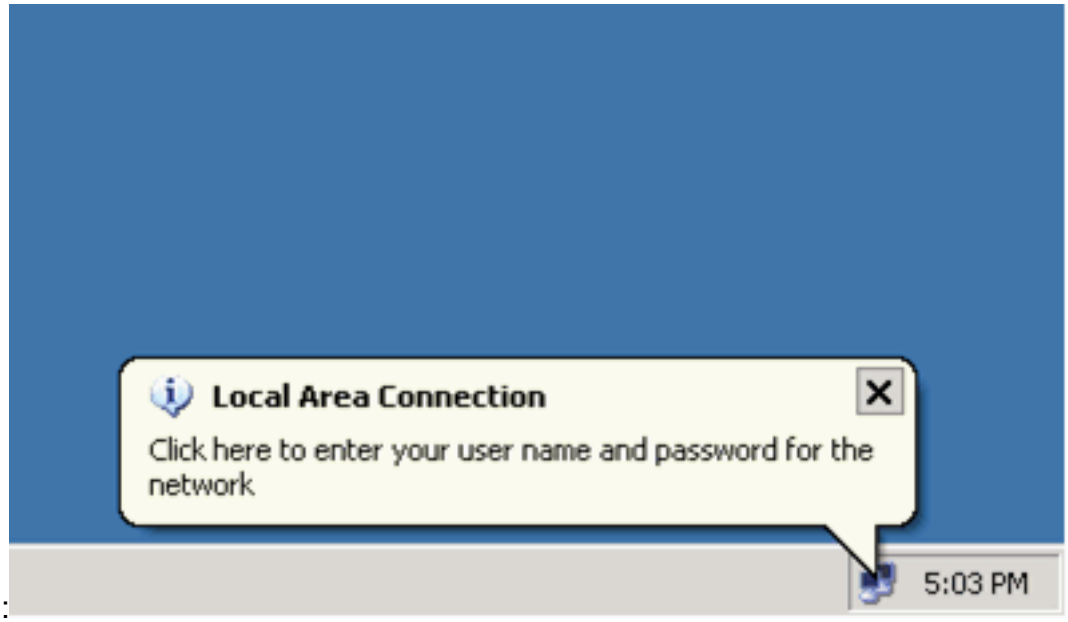
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

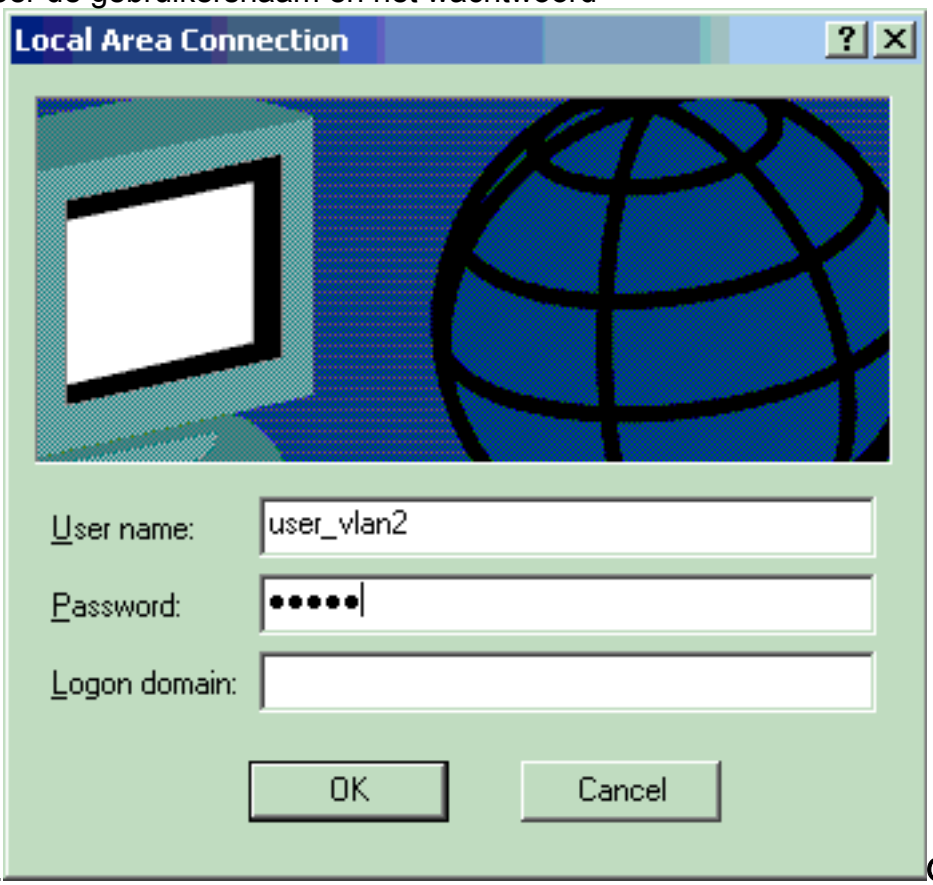
PC-clients

Als u de configuratie juist hebt voltooid, geven de PC clients een pop-upmelding weer om een gebruikersnaam en wachtwoord in te voeren.

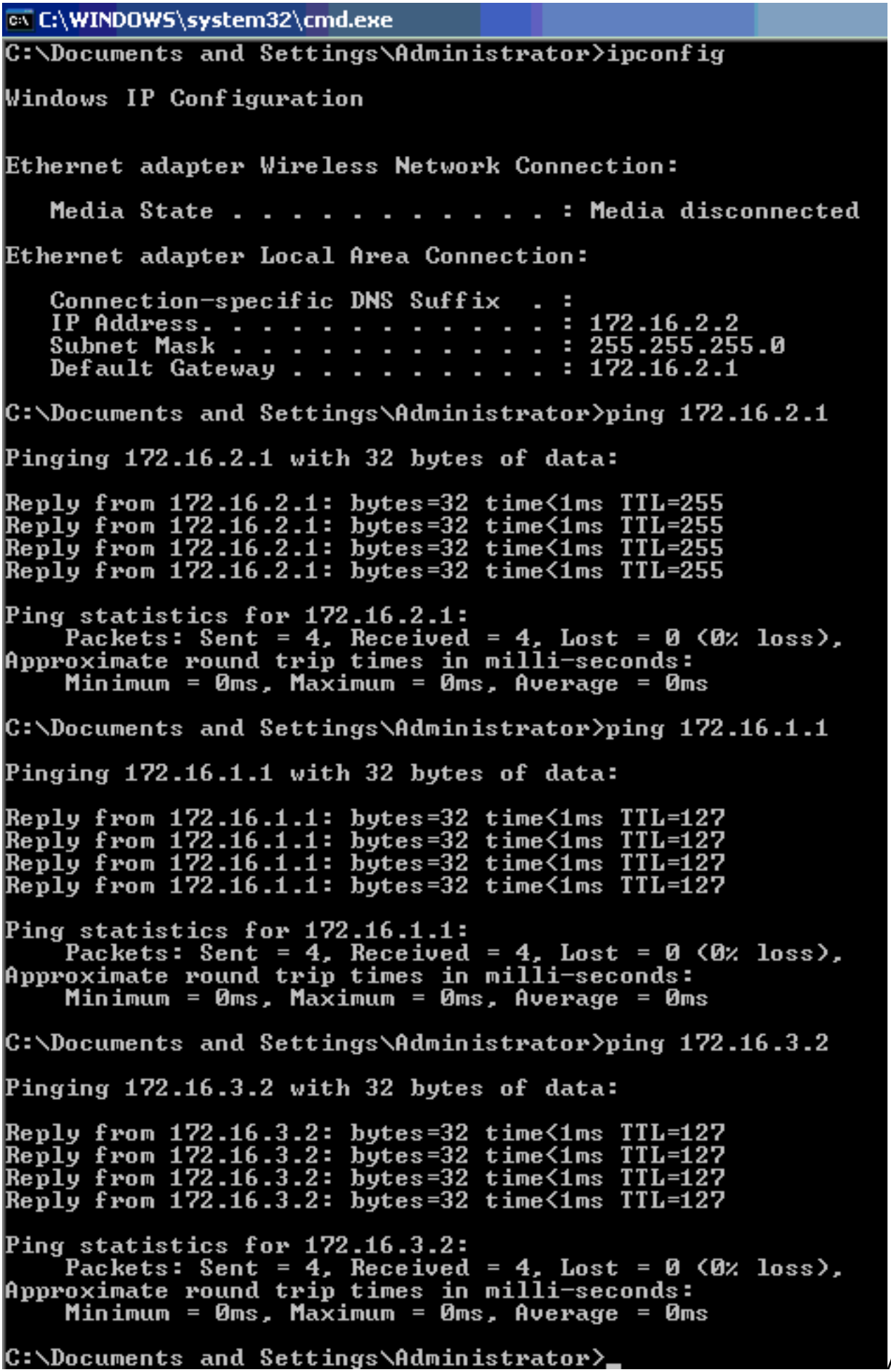
1. Klik op de prompt, die wordt weergegeven in dit

voorbeeld: 

Het venster voor gebruikersnaam en wachtwoord wordt weergegeven.

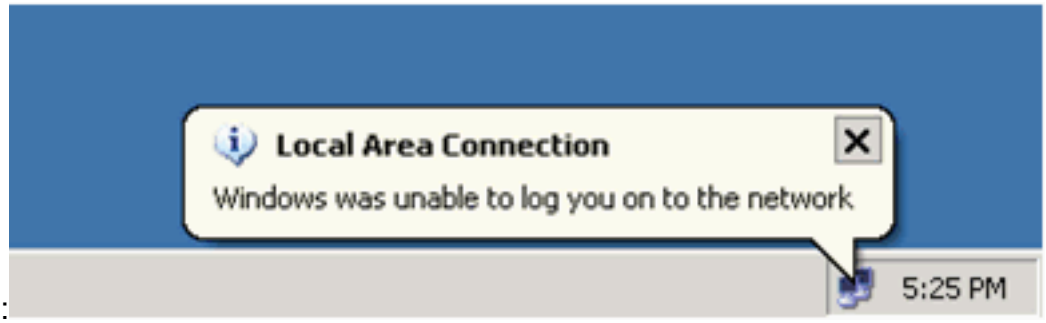
2. Voer de gebruikersnaam en het wachtwoord in. 

Opmerking: Voer in PC 1 en 2 VLAN 2 gebruikersreferenties in. In PC 3 en 4, ga VLAN 3 gebruikersgeloofsbrieven in.
3. Als er geen foutmeldingen verschijnen, controleer dan de connectiviteit met de gebruikelijke methoden, zoals door toegang tot de netwerkbronnen en met de **ping**-opdracht. Dit is een uitvoer van PC 1, die een succesvol **pingelen** aan PC 4 toont:



Als deze fout verschijnt, controleer of de gebruikersnaam en het wachtwoord juist

zijn:



Catalyst 6500

Als het wachtwoord en de gebruikersnaam correct lijken te zijn, verifieert u de 802.1x poortstaat op de switch.

1. Zoek naar een havenstatus die `geautoriseerd` aangeeft.

```
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
```

   Controleer de VLAN-status na succesvolle verificatie.

```
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. Controleer de DHCP-bindende status van de routingmodule (MSFC) na succesvolle verificatie.

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- IEEE 802.1x-verificatie met Catalyst 6500/6000 actieve Cisco IOS-softwareconfiguratie - voorbeeld
- Catalyst-switching- en ACS-implementatiegids
- RFC 2868: RADIUS-kenmerken voor tunnelprotocolondersteuning
- 802.1x-verificatie configureren
- Productondersteuningspagina's voor LAN
- Ondersteuningspagina voor LAN-switching
- Technische ondersteuning en documentatie – Cisco Systems