IEEE 802.1x-verificatie met Catalyst 6500/6000 actieve Cisco IOS-softwareconfiguratie - voorbeeld

Inhoud

Inleiding

Dit document legt uit hoe u IEEE 802.1x kunt configureren op een Catalyst 6500/6000-server die in de native modus loopt (één Cisco IOS® Software-afbeelding voor de Supervisor Engine en MSFC) en een RADIUS-server (Remote Authentication Dial-User Service) 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 Cisco IOS-softwarerelease 12.2(18)SXF op Supervisor Engine**Opmerking:** U hebt Cisco IOS-softwarerelease 12.1(13)E of later nodig om 802.1x poortgebaseerde verificatie te ondersteunen.
- Dit voorbeeld gebruikt Cisco Secure Access Control Server (ACS) 4.1 als RADIUS-server.**Opmerking:** U dient een RADIUS-server op te geven voordat u 802.1x in de switch activeert.
- PC-klanten die 802.1x-verificatie 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 de Cisco Technical Tips Convention 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 echt maakt elk gebruikersapparaat dat met een switch poort is verbonden en wijst de poort op een VLAN toe voordat er services beschikbaar zijn die door de switch of het 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.

Opmerking: Als de switch EAPOL-pakketten van de haven ontvangt die niet zijn ingesteld voor 802.1x-verificatie of als de switch geen 802.1x-verificatie ondersteunt, worden de EAPOL-pakketten verwijderd en niet naar een upstream-voorziening doorgestuurd.

Configureren

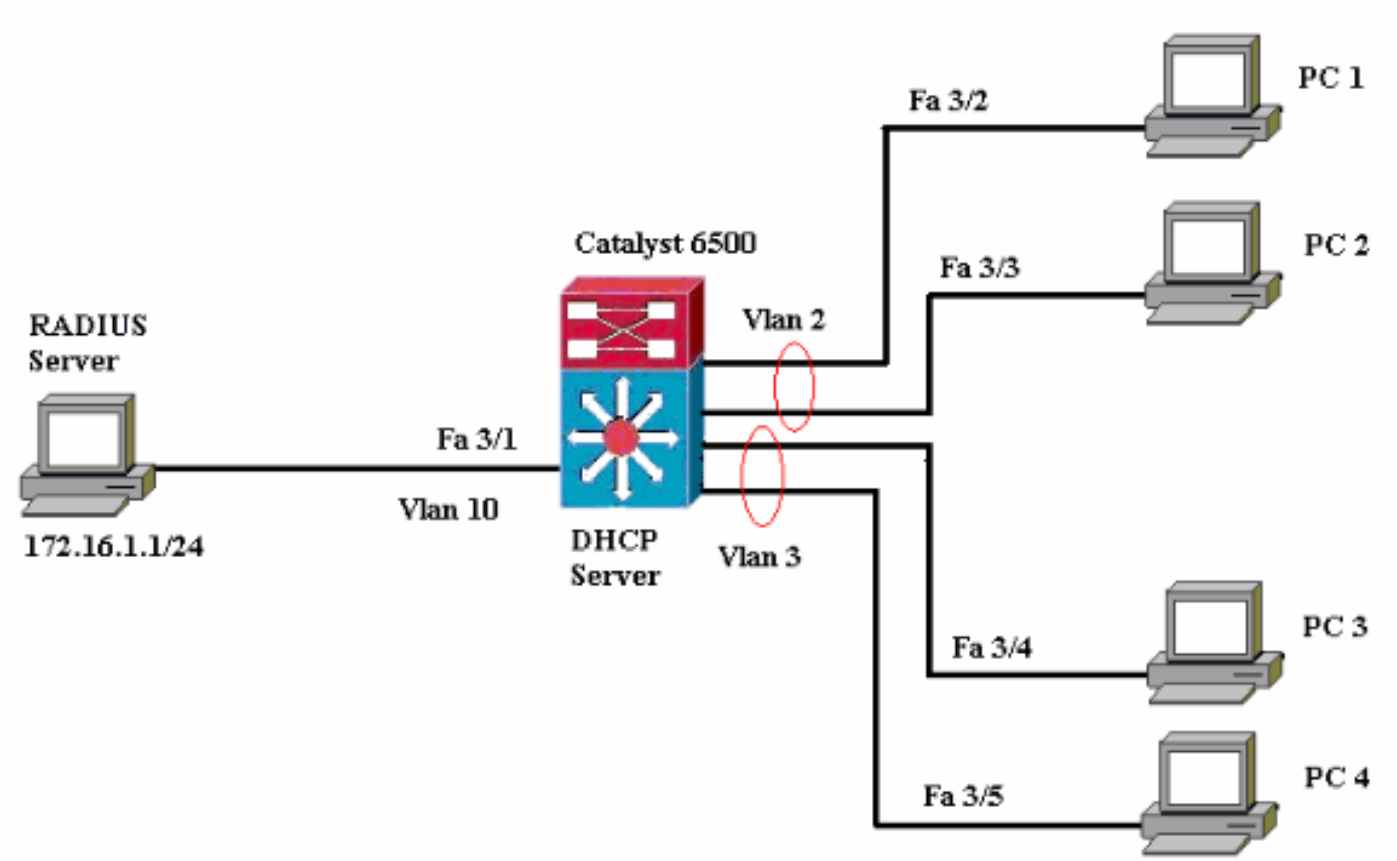
In deze sectie wordt u gepresenteerd met de informatie om de 802.1x optie te configureren die in dit document wordt beschreven.

Voor deze configuratie zijn de volgende stappen vereist:

- Configureer de Catalyst switch voor 802.1x-verificatie.
- Configureer de RADIUS-server.
- Configureer de PC-clients met de 802.1x-verificatie.

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. Het vraagt om identiteitsinformatie van de cliënt, verifieert die informatie met de server van de RADIUS, en geeft een antwoord op de cliënt terug. 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 toegang tot de LAN- en switch-services vragen 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 gebruiken de zelfde openings van een opening van een verbinding die in VLAN 2 is. Op dezelfde manier gebruiken PCs 3 en 4 een openings van een verbinding voor VLAN 3. PC cliënten worden gevormd om het IP adres van een server van DHCP te bereiken.

Configureer de Catalyst Switch voor 802.1x-verificatie

Deze configuratie van de switch omvat:

- Hoe u 802.1x-verificatie kunt inschakelen voor Fast Ethernet-poorten.
- Hoe een RADIUS-server op VLAN 10 aan te sluiten achter Fast Ethernet-poort 3/1.
- Een DHCP-serverconfiguratie voor twee IP-pools, één voor klanten in VLAN 2 en één voor klanten in VLAN 3.
- Routing tussen VLAN's om connectiviteit tussen klanten na verificatie te hebben.

Raadpleeg 802.1x Port-gebaseerde verificatierichtlijnen en -beperkingen voor de richtlijnen voor de configuratie van 802.1x-verificatie.

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

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
```

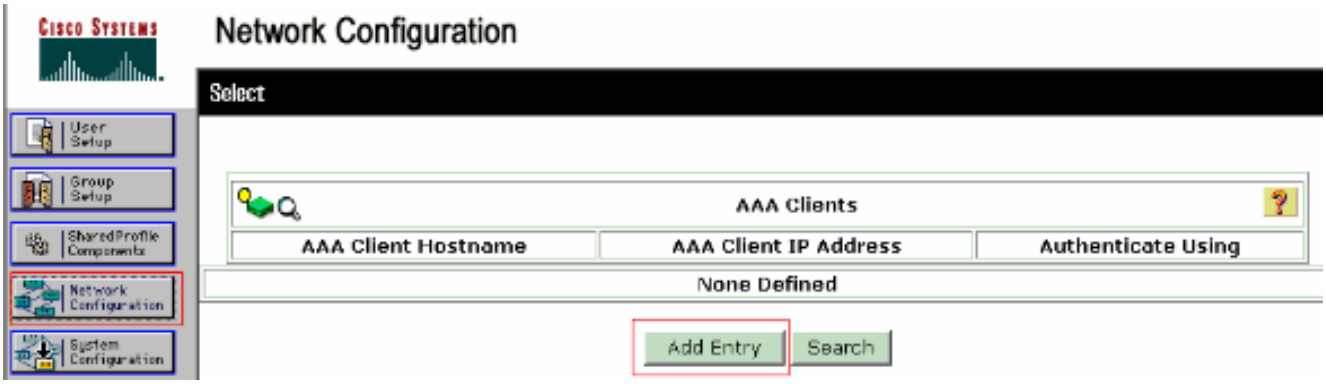
```
Cat6K(config-if)#no shut
!--- This is used as the gateway address in RADIUS
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
!--- This is the gateway address for clients 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.
```

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

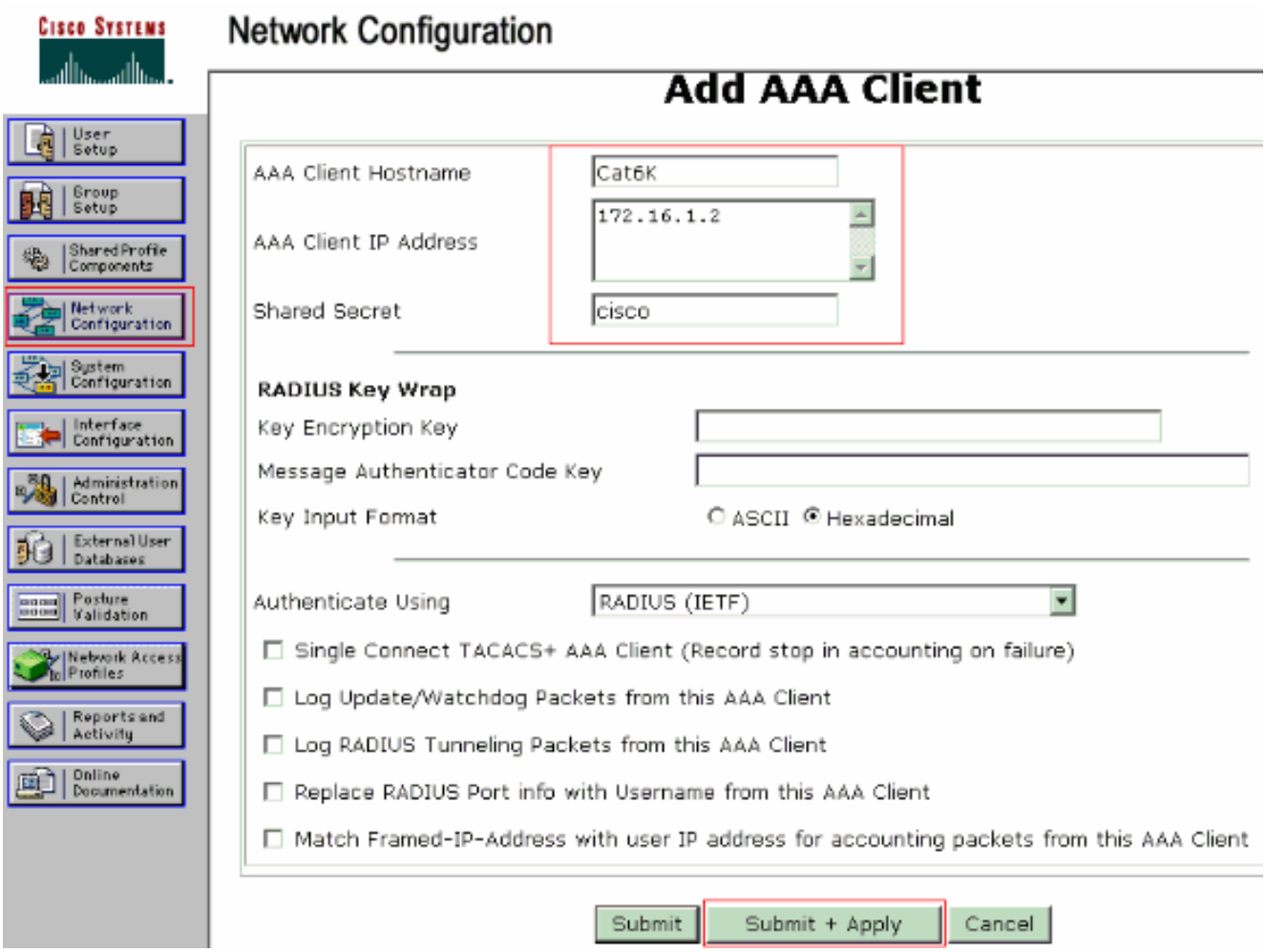
De RADIUS-server configureren

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 op **Network Configuration** in het ACS-beheervenster om een AAA-client te configureren.
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-adres van de switch (**172.16.1.2**).Gedeeld geheim = RADIUS-toets 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:

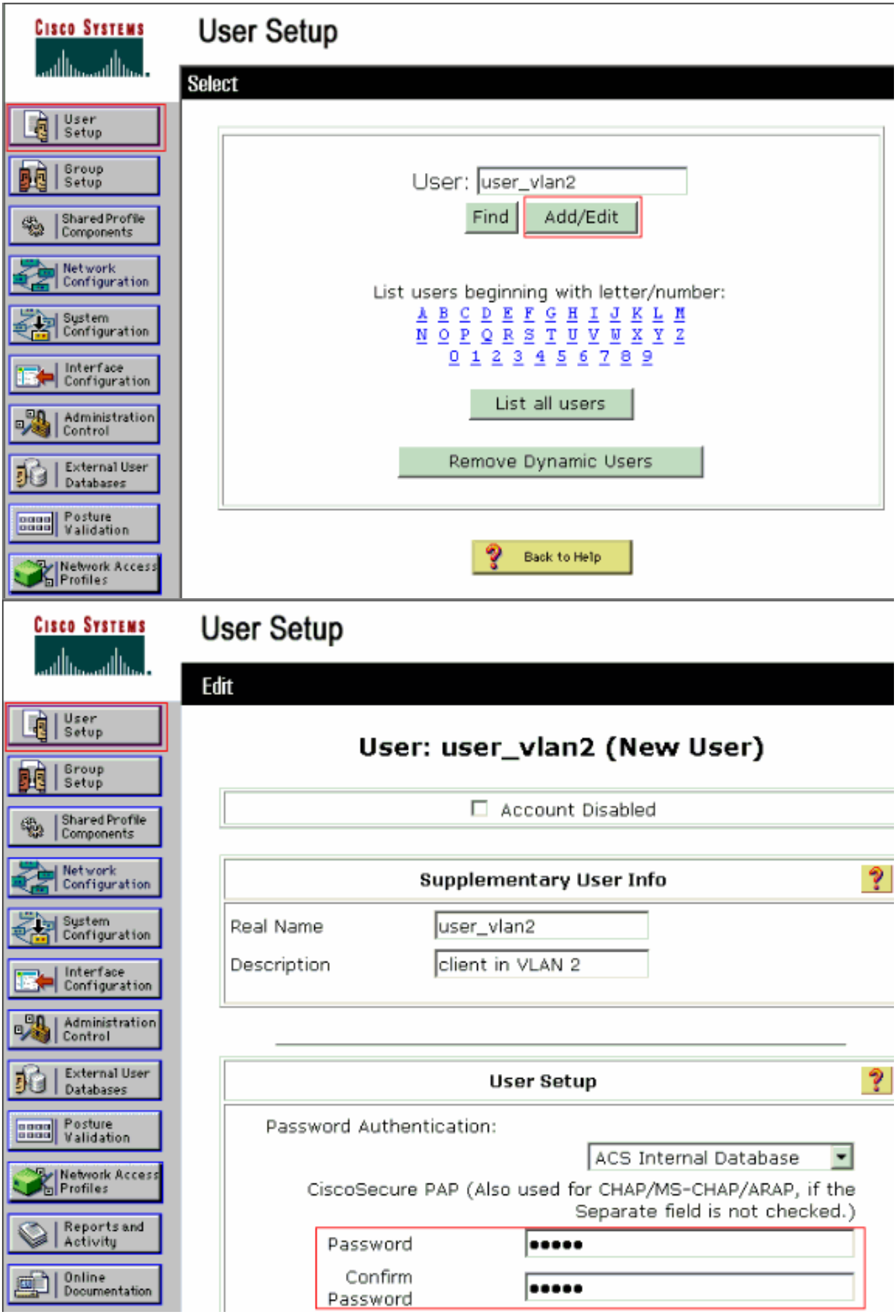


Voltooi deze stappen om de RADIUS-server voor verificatie, VLAN en IP-adrestoewijzing te configureren.

Twee gebruikersnamen moeten afzonderlijk worden gemaakt voor klanten die aan VLAN 2 verbinden zowel als voor VLAN 3. Hier wordt een gebruiker **user_VLAN2** voor klanten die aan VLAN 2 verbinden en een andere gebruiker **user_VLAN3** voor klanten die aan VLAN 3 verbinden gecreëerd voor dit doel.

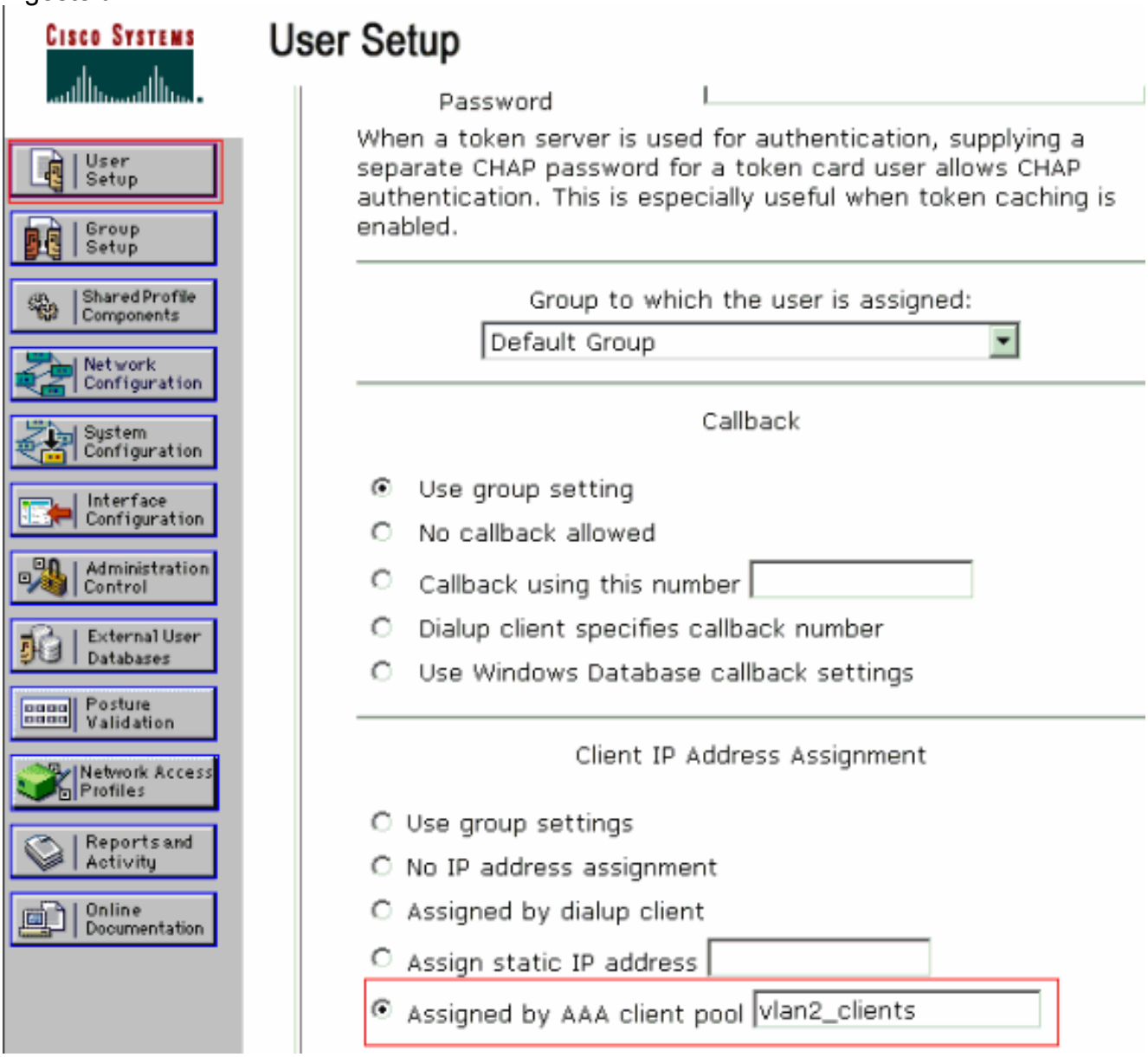
Opmerking: Hier wordt de gebruikersconfiguratie weergegeven voor klanten die alleen VLAN 2 aansluiten. Voor gebruikers die aan VLAN 3 verbinden, volg de zelfde procedure.

1. Om gebruikers toe te voegen en te configureren klikt u op **Instellingen gebruiker** en bepaalt u de naam en het
   wachtwoord.



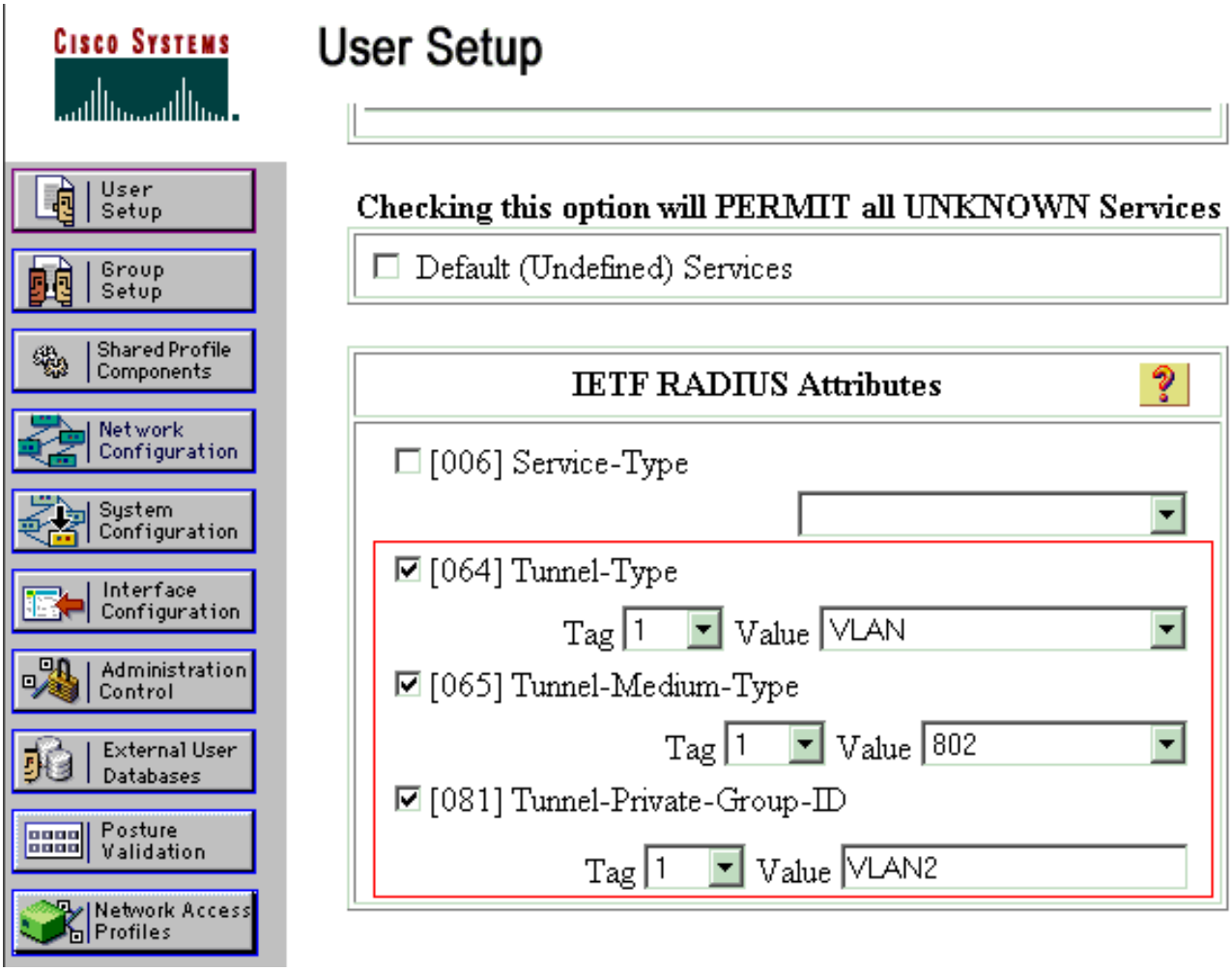
2. Defineert de client-IP-adrestoewijzing zoals **toegewezen door AAA-clientpool**. Voer de naam in van de IP-adrespool die op de switch voor VLAN 2-clients is

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 ook eigenschap **81** definiëren met een VLAN-*naam* of VLAN-*nummer* dat correspondeert.**Opmerking:** Als u de *naam* van VLAN gebruikt, moet deze precies hetzelfde zijn als de naam die in de switch is ingesteld.



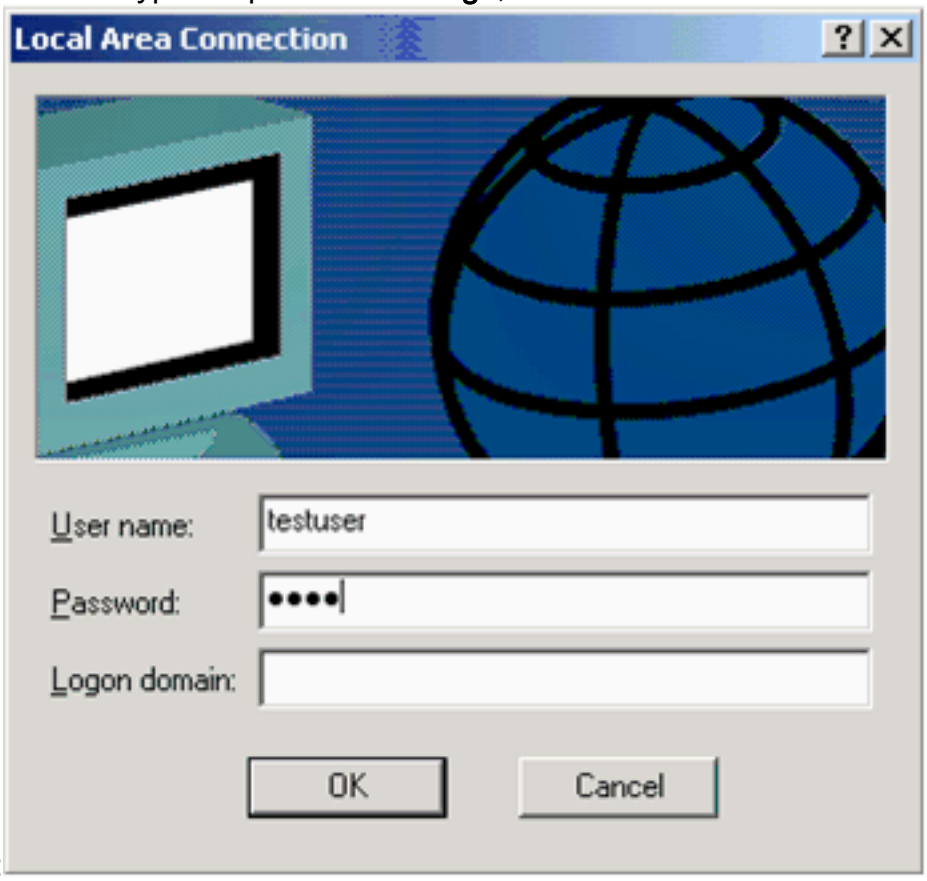
OPMERKING: Voor meer informatie over deze eigenschappen van IETF, zie RFC 2868: RADIUS-kenmerken voor ondersteuning van tunnelprotocollen .**Opmerking:** In de eerste configuratie van de ACS-server kunnen de RADIUS-kenmerken van IETF niet worden weergegeven in de **gebruikersinstelling**. Selecteer de optie **Interfaceconfiguratie > RADIUS (IETF)** om de IETF-eigenschappen in gebruikersconfiguratiescherm in te schakelen. Controleer vervolgens de eigenschappen **64**, **65** en **81** in de User and Group kolommen.**Opmerking:** Als u de eigenschap IETF **81** niet definieert en de poort een poort op de toegangsmodus is, heeft de client een toewijzing aan het toegangsVLAN van de poort. Als u de eigenschap **81** voor dynamische VLAN toewijzing hebt gedefinieerd en de poort een switch poort in toegangsmodus is, moet u de opdracht **een autorisatie netwerk standaardgroepsstraal** op de switch uitgeven. Deze opdracht wijst de poort aan het VLAN toe dat de RADIUS-server biedt. Anders verplaatst 802.1x de haven naar de `toegelaten` staat na verificatie van de gebruiker; maar de poort is nog in het standaard VLAN van de poort en connectiviteit kan falen. Als u de eigenschap **81** hebt gedefinieerd, maar u hebt de poort als een routepoort ingesteld, komt de toegangsontkenning voor. Deze foutmelding wordt weergegeven:

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

Configuratie van de PC Clients om 802.1x verificatie te gebruiken

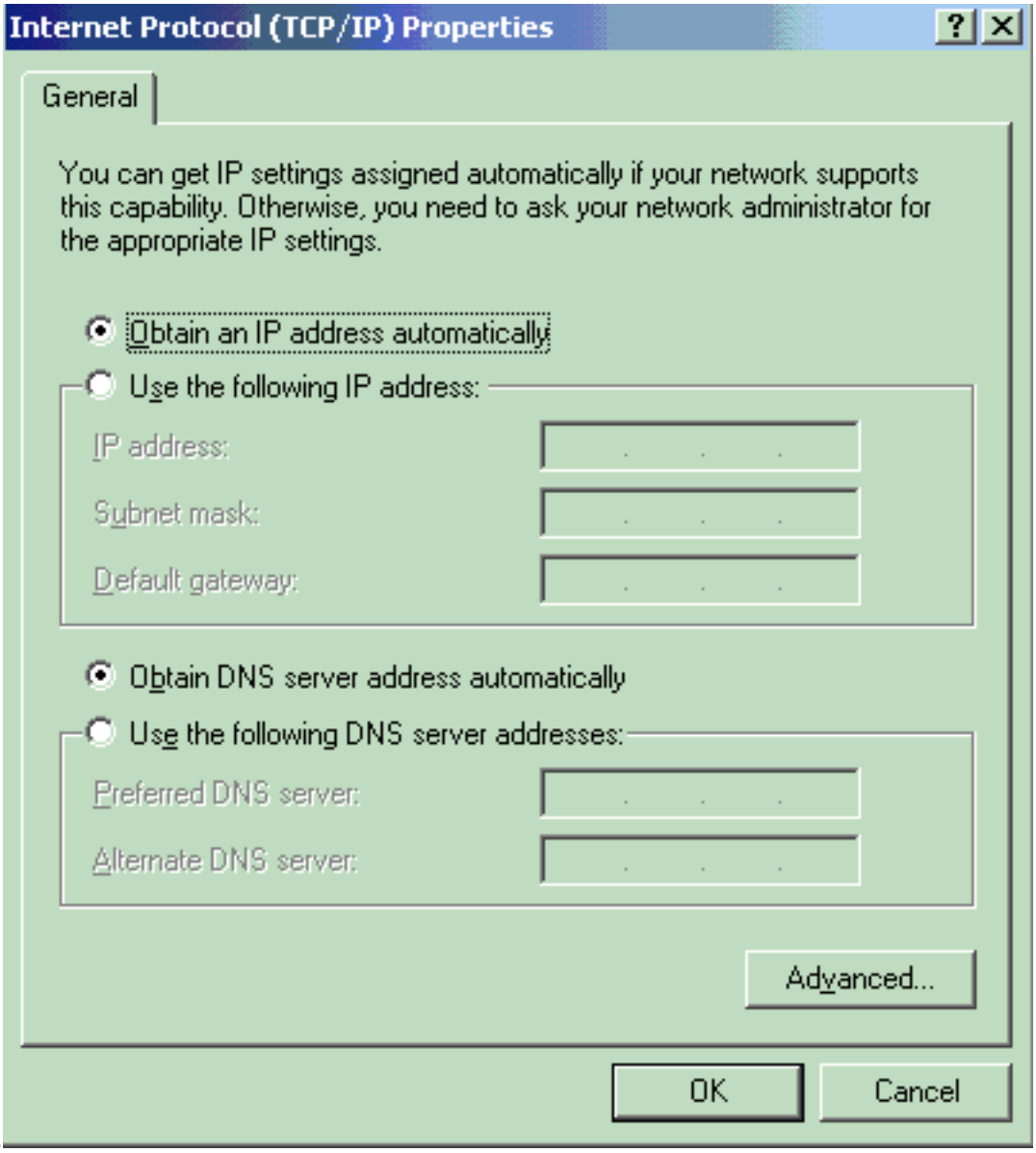
Dit voorbeeld is specifiek voor de Microsoft Windows XP Extensible Authentication Protocol (EAP) over LAN-client (EAPOL):

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 cliënten te vormen om het IP adres van een server van DHCP te verkrijgen.

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**



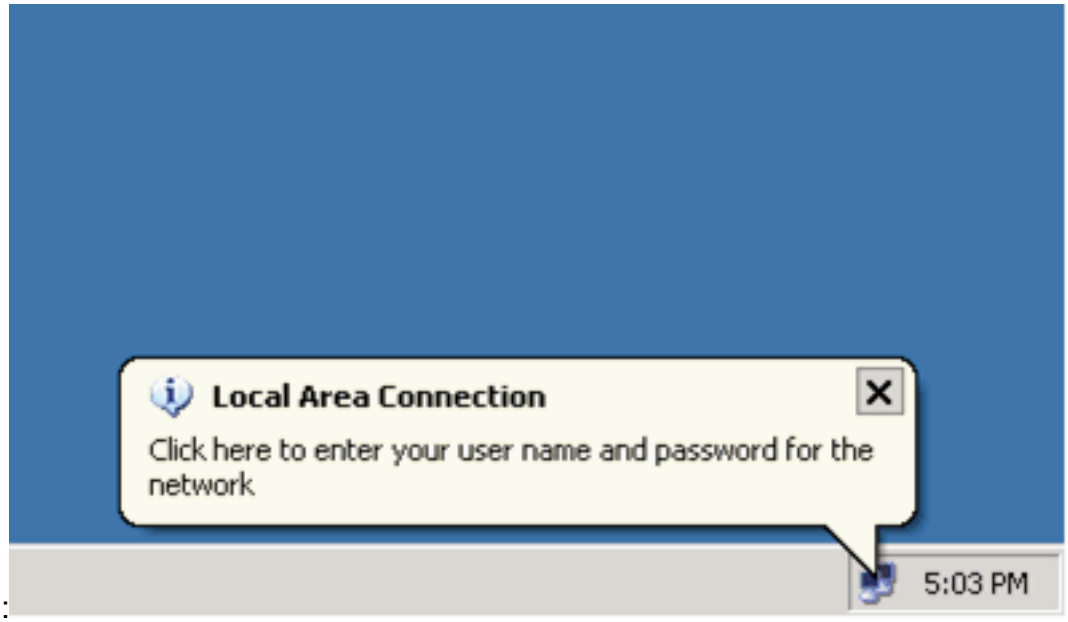
verkrijgen.

Verifiëren

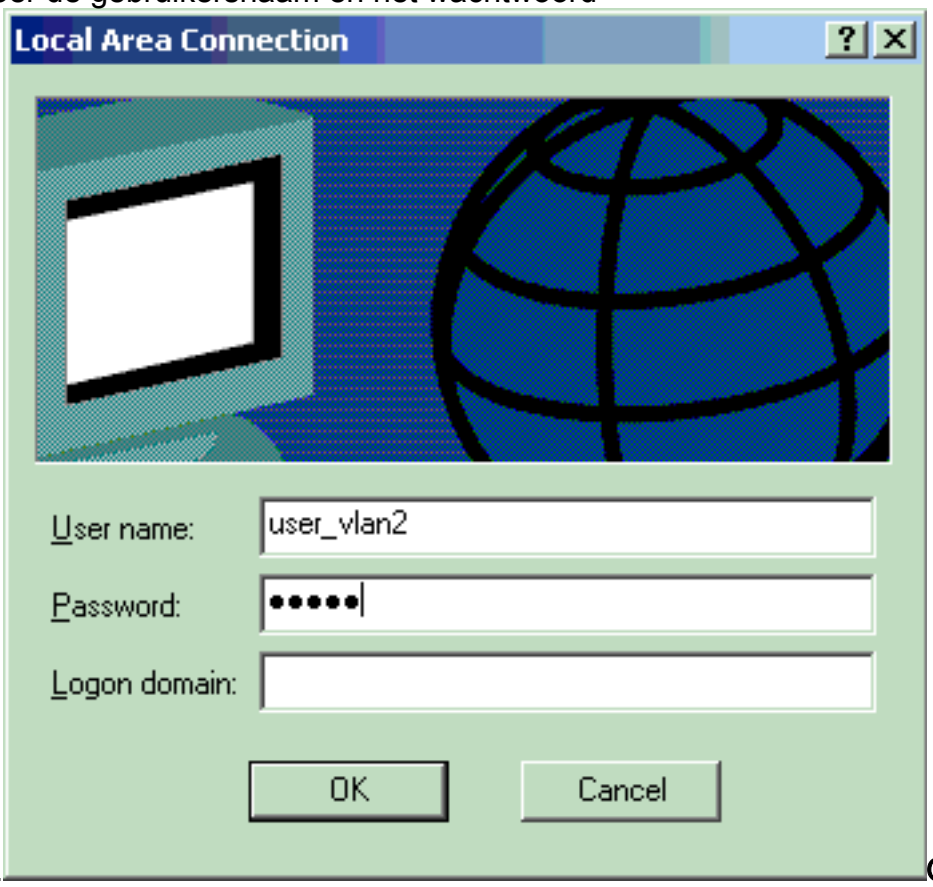
PC-clients

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

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

voorbeeld: 

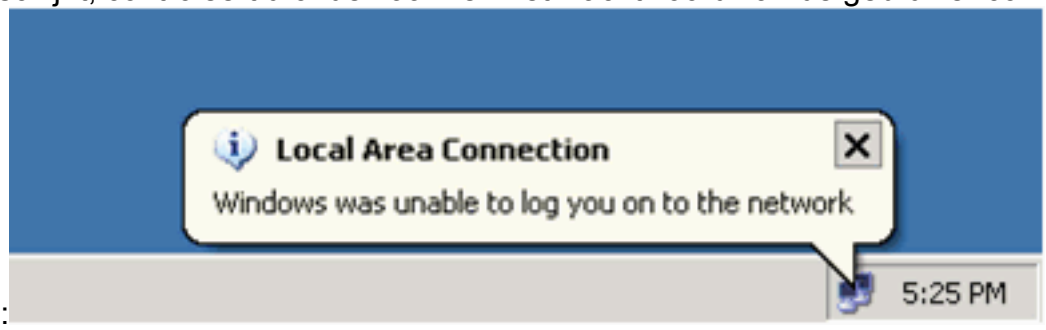
Het venster voor de gebruikersnaam en het invoeren van een wachtwoord wordt weergegeven.

2. Voer de gebruikersnaam en het wachtwoord in. 

Opmerking: Voer in PC 1 en 2 VLAN 2 gebruikersreferenties in en in PC 3 en 4 VLAN 3 gebruikersreferenties in.
3. Als er geen foutmeldingen verschijnen, controleer dan de connectiviteit met de gebruikelijke methoden, zoals door toegang tot de netwerkbronnen en door **ping**. Deze uitvoer komt van PC 1, en toont een succesvol **pingelen** aan 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: Als deze fout verschijnt, controleert u of de naam en het wachtwoord van de gebruiker correct zijn:



Catalyst 6500

Als het wachtwoord en de gebruikersnaam correct lijken te zijn, controleert u de 802.1x-

poortstatus op de switch.

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

```
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
```

Controleer de VLAN-status na succesvolle verificatie.

```
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. Controleer de DHCP-bindingsstatus van de volgende succesvolle verificatie.

```
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
```

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

Problemen oplossen

Verzamel de uitvoer van deze opdrachten **debug** om problemen op te lossen:

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten gebruikt.

- **debug dot1x gebeurtenissen**—hiermee kan het fouilleren van afdrukverklaringen worden beveiligd met de vlag van de punt1x gebeurtenissen.

```
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 straal**—informatie die bij RADIUS is gekoppeld.

```
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#
```

Gerelateerde informatie

- IEEE 802.1x-verificatie met Catalyst 6500/6000-actieve CatOS-softwareconfiguratievoorbeeld
- Richtsnoeren voor de implementatie van Cisco Secure ACS voor Windows NT/2000-servers in een Cisco Catalyst Switch-omgeving
- RFC 2868: RADIUS-kenmerken voor tunnelprotocolondersteuning
- De IEEE 802.1X-poortgebaseerde verificatie configureren
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems