

IEEE 802.1x-verificatie op Cisco Catalyst Layer 3 Vaste Configuration-Switches - Configuratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie van de Catalyst Switch voor 802.1x multi-domein verificatie](#)

[De RADIUS-server configureren](#)

[Configuratie van de PC Clients om 802.1x verificatie te gebruiken](#)

[Configuratie van de IP-telefoons die gebruikt moeten worden 802.1x-verificatie](#)

[Verifiëren](#)

[PC-clients](#)

[IP-telefoons](#)

[Layer 3 Switch](#)

[Problemen oplossen](#)

[IP-telefoonverificatie mislukt](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Met multi-domein verificatie kunnen een IP-telefoon en een PC op dezelfde switch poort worden geauthentiseerd terwijl deze op juiste spraak- en datapoorten worden geplaatst. Dit document legt uit hoe u IEEE 802.1x multi-domein verificatie (MDA) kunt configureren op Cisco Catalyst Layer 3 vaste configuratie-switches.

[Voorwaarden](#)

[Vereisten](#)

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- [Hoe werkt RADIUS?](#)
- [Catalyst-switching- en ACS-implementatiegids](#)
- [Gebruikershandleiding voor Cisco Secure Access Control Server 4.1](#)
- [Een overzicht van de Cisco Unified IP-telefoon](#)

[Gebruikte componenten](#)

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

- Cisco Catalyst 3560 Series Switch met Cisco IOS-software release 12.2(37)SE1 **Opmerking:** Ondersteuning voor multi-domein verificatie is alleen beschikbaar bij Cisco IOS-software release 12.2(35)SE en hoger.
- 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-klienten die 802.1x-verificatie ondersteunen **Opmerking:** Dit voorbeeld gebruikt Microsoft Windows XP-clients.
- Cisco Unified IP-telefoon 7970G met SCCP firmware versie 8.2(1)
- Cisco Unified IP-telefoon 7961G met SCCP firmware versie 8.2(2)
- Media Convergence Server (MCS) met Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2

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.

[Verwante producten](#)

Deze configuratie kan ook worden gebruikt bij deze hardware:

- Cisco Catalyst 3560-E Series Switch
- Cisco Catalyst 3750 Series Switch
- Cisco Catalyst 3750-E Series Switch

Opmerking: Cisco Catalyst 3550 Series Switch biedt geen ondersteuning voor 802.1x multi-domein verificatie.

[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 client-server gebaseerd toegangscontrole- en verificatieprotocol dat onbevoegde apparaten beperkt om via publiekelijk toegankelijke poorten aan te sluiten op een LAN. 802.1x beheerst de toegang tot het netwerk door de oprichting van twee afzonderlijke virtuele toegangspunten in elke haven. 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.

802.1x bestaat uit drie primaire componenten. Elk wordt een Port Access Entiteit (PAE) genoemd.

- Vermenigvuldig-client-apparaat dat om netwerktoegang vraagt, bijvoorbeeld IP-telefoons en aangesloten pc's
- Verificatie-netwerkapparaat dat de aanvraag voor uitgebreide toestemming vergemakkelijkt, bijvoorbeeld Cisco Catalyst 3560
- Verificatieserver-A afstandsverificatie Dial-in User Server (RADIUS), die de verificatieservice biedt, bijvoorbeeld Cisco Secure Access Control Server

De Cisco Unified IP-telefoons bevatten ook een 802.1X applicatie. Met dit getal kunnen netwerkbeheerders de connectiviteit van IP-telefoons met de LAN switch-poorten controleren. De eerste release van de IP-telefoon 802.1X-applicatie implementeert de MAP-MD5 optie voor 802.1X-verificatie. In een configuratie met meerdere domeinen, moeten de IP-telefoon en de aangesloten PC onafhankelijk om toegang tot het netwerk vragen door de specificatie van een gebruikersnaam en wachtwoord. Het Authenticator apparaat kan informatie vereisen van de RADIUS genaamd eigenschappen. Eigenschappen specificeren extra autorisatie informatie zoals of toegang tot een bepaald VLAN voor een Leverancier is toegestaan. Deze eigenschappen kunnen een specifieke verkoper zijn. Cisco gebruikt de RADIUS-eigenschap `cisco-av-paar` om de verificator (Cisco Catalyst 3560) te vertellen dat een Supplicant (IP-telefoon) op het VLAN-kanaal is toegestaan.

[Configureren](#)

In deze sectie, wordt u voorgesteld met de informatie om de 802.1x multi-domein authenticatie optie te configureren die in dit document wordt beschreven.

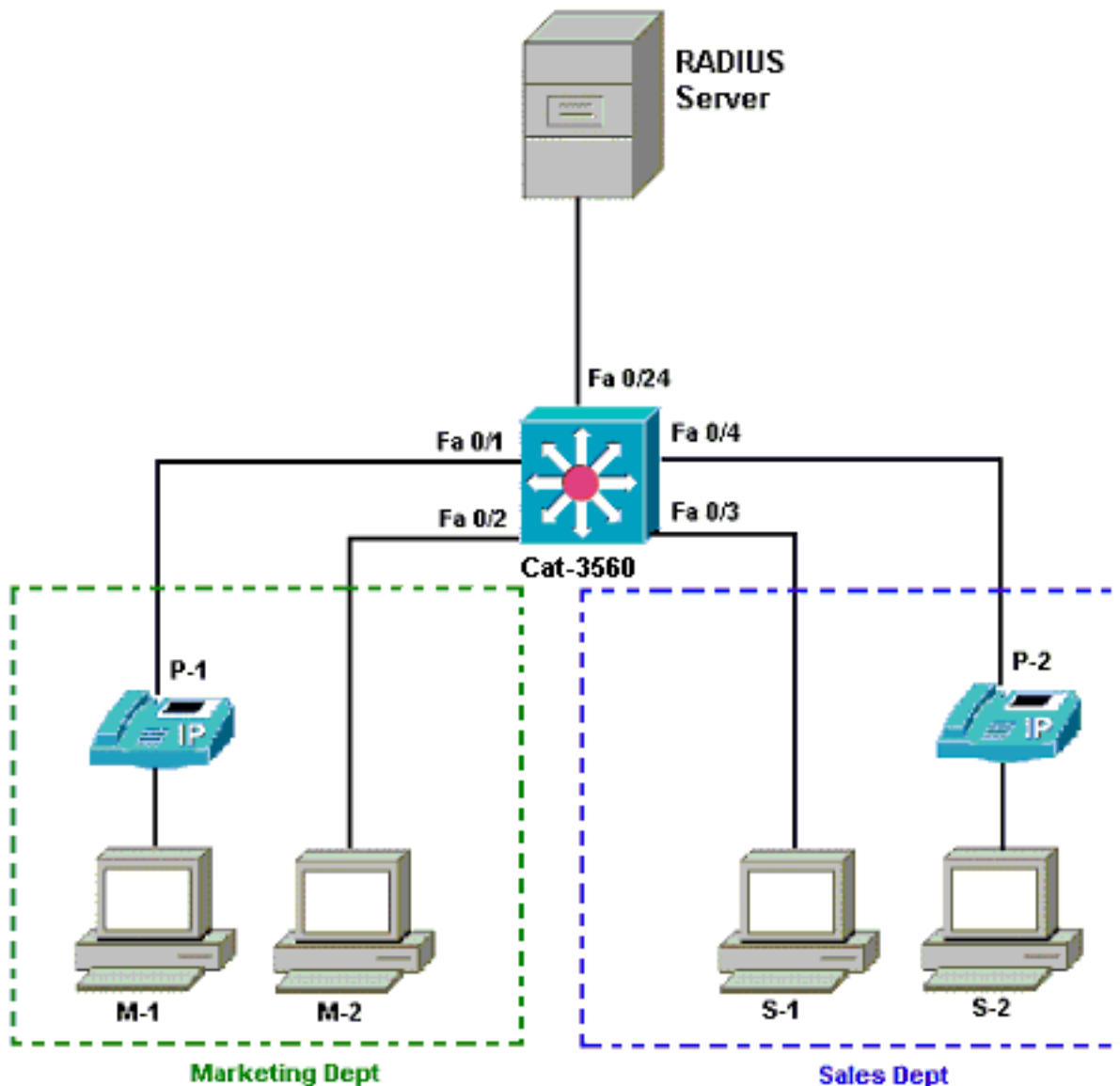
Voor deze configuratie zijn de volgende stappen vereist:

- [Configureer de Catalyst Switch voor 802.1x multi-domein verificatie.](#)
- [Configureer de RADIUS-server.](#)
- [Configureer de PC-clients met de 802.1x-verificatie.](#)
- [Configureer de IP-telefoons om 802.1x-verificatie te gebruiken.](#)

N.B.: Gebruik het [Opdrachtupgereedschap](#) ([alleen geregistreeerde](#) klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

[Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd:



- RADIUS server-Dit 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 Cisco ACS geïnstalleerd en geconfigureerd op een Media Coverage Server (MCS) voor verificatie en VLAN-toewijzing. MCS is ook de TFTP-server en Cisco Unified Communications Manager (Cisco CallManager) voor de IP-telefoons.
- Switch-Dit regelt de fysieke toegang tot het netwerk gebaseerd op 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 Catalyst 3560 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 categorieën eindgebruikers. Om dit te doen, voegt het de geauthenteerde gebruikersidentiteit in het DHCP-zoekproces toe. Port Fast Ethernet 0/1 en 0/4 zijn de enige poorten die zijn geconfigureerd voor 802.1x multi-domein verificatie. Poorten Fast Ethernet 0/2 en 0/3 zijn in de standaard 802.1x single host-modus. Port FastEthernet 0/24 sluit zich aan op de RADIUS-server.**Opmerking:** Als u een externe DHCP-server gebruikt, vergeet dan niet de opdracht `ip helper-adres` op de SVI (VLAN)-interface toe te voegen, waarin de client verblijft, wat op de DHCP-server wijst.

- Clients-deze apparaten zijn bijvoorbeeld IP-telefoons of werkstations, die om toegang tot de LAN- en switch-services verzoeken en op verzoeken van de switch reageren. Hier worden de clients ingesteld om het IP-adres van een DHCP-server te bereiken. De apparaten M-1, M-2, S-1 en S-2 zijn de client voor het werkstation die om toegang tot het netwerk verzoekt. P-1 en P-2 zijn de IP-telefoonklanten die om toegang tot het netwerk verzoeken. M-1, M-2 en P-1 zijn clientapparaten in de marketingafdeling. S-1, S-2 en P-2 zijn clientapparaten in de verkoopafdeling. IP-telefoons P-1 en P-2 worden geconfigureerd om in dezelfde spraak-VLAN (VLAN 3) te zijn. Werkstations M-1 en M-2 worden geconfigureerd om in dezelfde gegevens VLAN (VLAN 4) te zijn na een succesvolle verificatie. Werkstations S-1 en S-2 worden ook geconfigureerd om in hetzelfde data-VLAN (VLAN 5) te zijn na een succesvolle verificatie. **Opmerking:** U kunt de dynamische VLAN-toewijzing alleen voor de gegevensapparaten gebruiken vanaf een RADIUS-server.

Configuratie van de Catalyst Switch voor 802.1x multi-domein verificatie

Deze configuratie van de switch omvat:

- Hoe u 802.1x multi-domeinverificatie op de poorten van de switch kunt inschakelen
- Configuratie van RADIUS-servers
- DHCP-serverconfiguratie voor IP-adrestoewijzing
- Routing tussen VLAN's om connectiviteit tussen klanten te hebben na verificatie

Raadpleeg [Multidomein-verificatie gebruiken](#) voor meer informatie over de richtlijnen voor het configureren van MDA.

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

Opmerking: hier wordt alleen de relevante configuratie weergegeven.

Kat-3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
!--- Sets the hostname for the switch. Cat-
3560(config)#vlan 2
Cat-3560(config-vlan)#name SERVER
Cat-3560(config-vlan)#vlan 3
Cat-3560(config-vlan)#name VOICE
Cat-3560(config-vlan)#vlan 4
Cat-3560(config-vlan)#name MARKETING
Cat-3560(config-vlan)#vlan 5
Cat-3560(config-vlan)#name SALES
Cat-3560(config-vlan)#vlan 6
Cat-3560(config-vlan)#name GUEST_and_AUTHFAIL
!--- VLAN should already exist in the switch for a
successful authentication. Cat-3560(config-vlan)#exit
Cat-3560(config)#interface vlan 2
Cat-3560(config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for the RADIUS Server.
Cat-3560(config-if)#interface vlan 3
Cat-3560(config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for IP Phone clients in
```

```

VLAN 3. Cat-3560(config-if)#interface vlan 4
Cat-3560(config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
4. Cat-3560(config-if)#interface vlan 5
Cat-3560(config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560(config-if)#no shut
!--- This is the gateway address for PC clients in VLAN
5. Cat-3560(config-if)#exit
Cat-3560(config)#ip routing
!--- Enables IP routing for interVLAN routing. Cat-
3560(config)#interface range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#shut
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
!--- This is a dedicated VLAN for the RADIUS server.
Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 ,
fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
!--- You must configure the voice VLAN for the IP phone
when the !--- host mode is set to multidomain. !---
Note: If you use a dynamic VLAN in order to assign a
voice VLAN !--- on an MDA-enabled switch port, the voice
device fails authorization.

Cat-3560(config-if-range)#dot1x port-control auto
!--- Enables IEEE 802.1x authentication on the port.
Cat-3560(config-if-range)#dot1x host-mode multi-domain
!--- Allow both a host and a voice device to be !---
authenticated on an IEEE 802.1x-authorized port. Cat-
3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
!--- The guest VLAN and restricted VLAN features only
apply to the data devices !--- on an MDA enabled port.
Cat-3560(config-if-range)#dot1x reauthentication
!--- Enables periodic re-authentication of the client.
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
!--- Set the number of seconds between re-authentication
attempts. Cat-3560(config-if-range)#dot1x auth-fail max-
attempts 2
!--- Specifies the number of authentication attempts to
allow !--- before a port moves to the restricted VLAN.
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
!--- By default a 802.1x authorized port allows only a
single client. Cat-3560(config-if-range)#dot1x guest-
vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
!--- This pool assigns ip address for IP Phones. !---

```

```

Option 150 is for the TFTP server. Cat-3560(dhcp-
config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- This pool assigns ip address for PC clients in
Marketing Dept. Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
!--- This pool assigns ip address for PC clients in
Sales Dept. Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1
Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group
radius
!--- Method list should be default. Otherwise dot1x does
not work. Cat-3560(config)#aaa authorization network
default group radius
!--- You need authorization for dynamic VLAN assignment
to work with RADIUS. Cat-3560(config)#radius-server host
172.16.2.201 key Cisco123
!--- The key must match the key used on the RADIUS
server. Cat-3560(config)#dot1x system-auth-control
!--- Globally enables 802.1x. Cat-3560(config)#interface
range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

```

VLAN Name	Status	Ports

1 default	active	Fa0/1,
Fa0/2, Fa0/3, Fa0/4		Fa0/5,
Fa0/6, Fa0/7, Fa0/8		Fa0/9,
Fa0/10, Fa0/11, Fa0/12		Fa0/13,
Fa0/14, Fa0/15, Fa0/16		Fa0/17,
Fa0/18, Fa0/19, Fa0/20		Fa0/21,
Fa0/22, Fa0/23, Gi0/1		Gi0/2
2 SERVER	active	Fa0/24
3 VOICE	active	Fa0/1,
Fa0/4		
4 MARKETING	active	
5 SALES	active	
6 GUEST_and_AUTHFAIL	active	
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

Opmerking: Gebruik het [Opdrachtupgereedschap](#) (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 172.16.2.201/24. 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.

Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry **Search**

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
CCM-4	172.16.2.201	CiscoSecure ACS

3. Configureer de AAA client-hostname, IP-adres, gedeelde geheime sleutel en type verificatie als volgt: AAA client hostname = Switch Hostname (**Cat-3560**). AAA client-IP-adres = Management interface-adres van de switch (**172.16.2.1**). Gedeeld geheim = RADIUS-toets ingesteld op de switch (**CisCo123**). **Opmerking:** Voor een correct gebruik moet de gedeelde geheime sleutel identiek zijn op de AAA-client en ACS. Toetsen zijn hoofdlettergevoelig. Verifieer het gebruik met = **RADIUS (Cisco IOS/PIX 6.0)**. **Opmerking:** het kenmerk Cisco Attribution-Value (AV) is beschikbaar onder deze optie.
4. Klik op **Indienen + Toepassen** om deze veranderingen effectief te maken, zoals dit voorbeeld toont:

CISCO SYSTEMS Network Configuration

Add AAA Client

AAA Client Hostname
 AAA Client IP Address
 Shared Secret

RADIUS Key Wrap

 Key Encryption Key
 Message Authenticator Code Key
 Key Input Format ASCII Hexadecimal

 Authenticate Using

Groepsinstallatie

Raadpleeg deze tabel om de RADIUS-server voor verificatie te configureren.

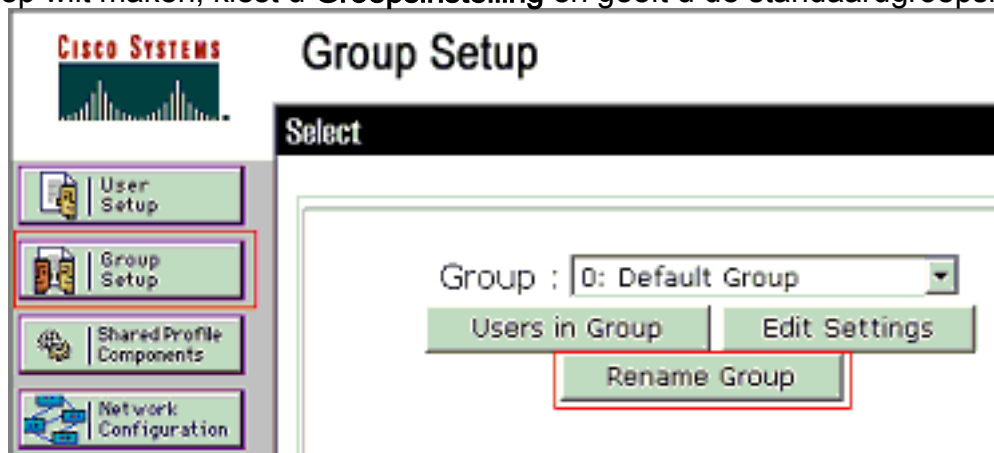
Apparaat	Dept	Groep	Gebruiker	Wachtwoord	VLAN	DH CP-pool
M-1	Marketing	Marketing	marktm anager	Cisco	MARKETING	Marketing
M-2	Marketing	Marketing	marktm edewer kers	MScisco	MARKETING	Marketing
S-2	Verkoop	Verkoop	verkoo pmana ger	SMcisco	VERK OOP	Verkoop
S-1	Verkoop	Verkoop	verkoo pperso	Cisco	VERK OOP	Verkoop

			neel			
P-1	Marketing	IP-telefoons	CP-7970G-SEP001759E7492C	P1cisco	SPRAAK	IP-telefoons
P-2	Verkoop	IP-telefoons	CP-7961G-SEP001A2F80381F	P2cisco	SPRAAK	IP-telefoons

Maak groepen voor klanten die verbinding maken met VLAN's 3 (VOICE), 4 (MARKETING) en 5 (SALES). Hier worden groepjes **IP-telefoons**, **marketing** en **verkoop** voor dit doel gemaakt.

Opmerking: Dit is de configuratie van de groepen Marketing- en IP-telefoons. Voltooi de stappen voor de **Marketing** groep voor de **verkoopgroepconfiguratie**.

1. Als u een groep wilt maken, kiest u **Groepsinstelling** en geeft u de standaardgroepsnaam een



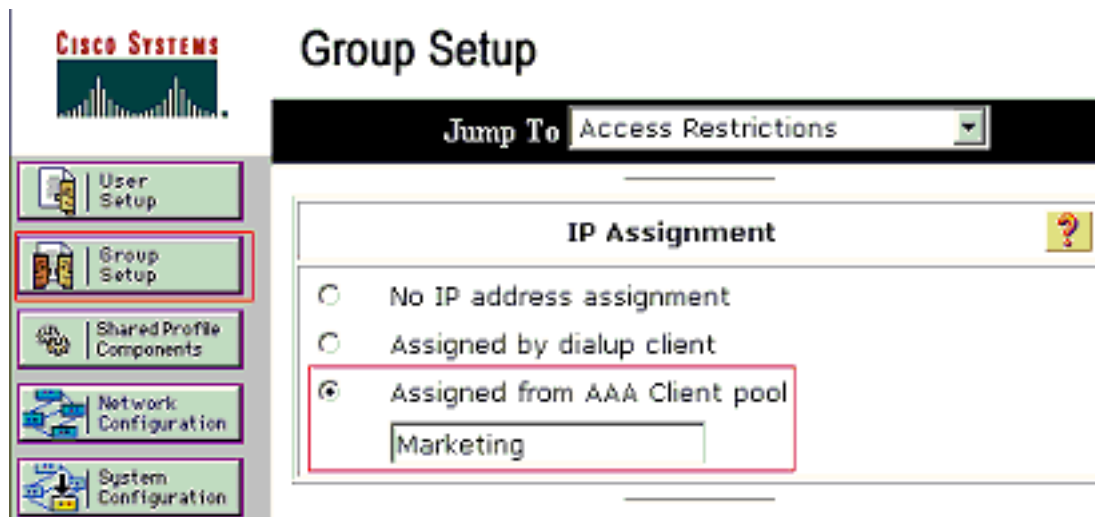
andere naam.

2. Kies de groep uit de lijst en klik op **Instellingen bewerken** om een groep te



configureren

3. Definieert de client-IP-adrestoewijzing zoals **toegewezen door AAA-clientpool**. Voer de naam in van de IP-adrespool die op de switch voor deze groepsklanten is



ingesteld.

Opme

rking: Kies deze optie en type 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. **Opmerking:** Voor groepsconfiguratie **IP-telefoons** slaat u de volgende stap over, stap 4 en gaat u naar stap 5.


4. Definiëert de eigenschappen van de Internet Engineering Task Force (IETF) **64**, **65** en **81** en klik vervolgens op **Indienen + Herstart**. 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.

Opmerk

ing: 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**. 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, wordt de client toegewezen 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 **standaard** de opdracht **van de groep** van het **autorisatie netwerk** op de switch uitvoeren. 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. **Opmerking:** de volgende stap is alleen van toepassing op de groep **IP-telefoons**.

5. Configuratie van de server van de RADIUS om een paar van Cisco toe te wijzen Attribution-Value (AV) om een stemapparaat te machtigen. Zonder dit, behandelt de switch het stemapparaat als een gegevensapparaat. Definieer Cisco Attribution-Value (AV) paareigenschap met een waarde van *device-traffic-class=voice* en klik op **Submit +**



Group Setup

Jump To Access Restrictions

- User Setup
- Group Setup**
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

IP Assignment

- No IP address assignment
- Assigned by dialup client
- Assigned from AAA Client pool

Cisco IOS/PIX 6.x RADIUS Attributes

- [009\001] cisco-av-pair
 -
- [009\101] cisco-h323-credit-amount
- [009\102] cisco-h323-credit-time
- [009\103] cisco-h323-return-code

Restart.

[Instellen gebruiker](#)

Voltooi deze stappen om een gebruiker toe te voegen en te configureren.

1. Selecteer **Gebruiker** Instellingen om gebruikers toe te voegen en te configureren. Voer de gebruikersnaam in en klik op **Toevoegen/Bewerken**



User Setup

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases

User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

2. Bepaal de naam, het wachtwoord en de groep voor de

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

User: mkt-manager (New User)

Account Disabled

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password *****
 Confirm Password *****

Separate (CHAP/MS-CHAP/ARAP)

Password *****
 Confirm Password *****

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Marketing

Callback

Use group setting

Submit Delete Cancel

gebruiker.

3. IP-telefoon gebruikt zijn apparaat-ID als de gebruikersnaam en het gedeelde geheim voor de verificatie. Deze waarden moeten overeenkomen op de RADIUS-server. Voor IP-telefoons P-1 en P-2 moeten er gebruikersnamen worden gemaakt die gelijk zijn aan hun apparaat-ID en wachtwoord, net zoals het geconfigureerde gedeelde geheim. Zie het [configureren van de IP-telefoons om het gedeelte 802.1x-verificatie te gebruiken](#) voor meer informatie over apparaat-ID en gedeeld geheim op een IP-



User: CP-7961G-SEP001A2F80381F

Account Disabled

User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password *****
 Confirm Password *****

Separate (CHAP/MS-CHAP/ARAP)

Password *****
 Confirm Password *****

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IP Phones

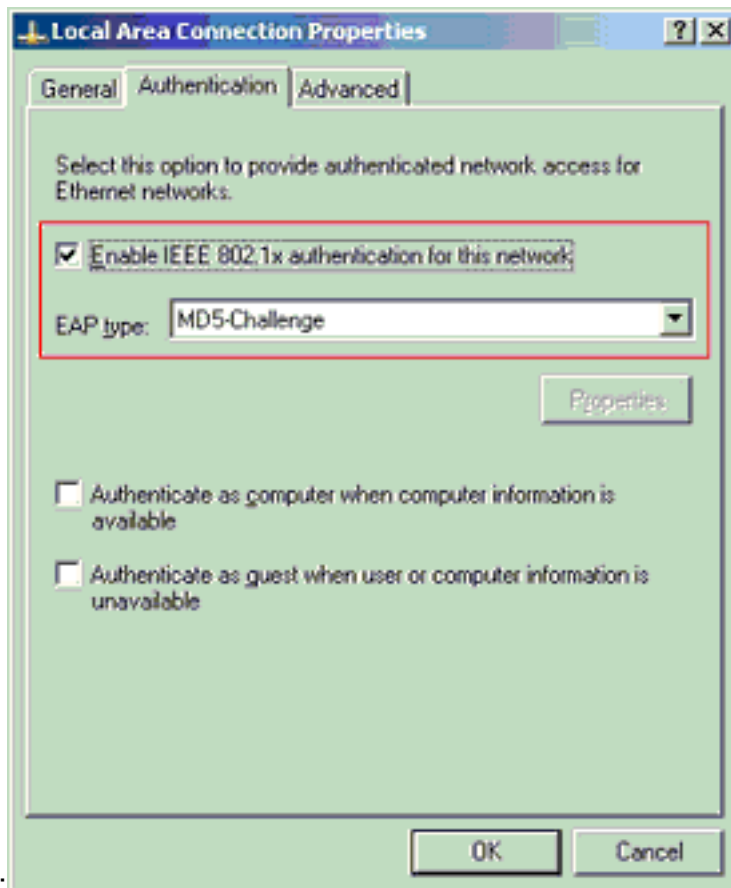
Submit Delete Cancel

telefoon.

[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):

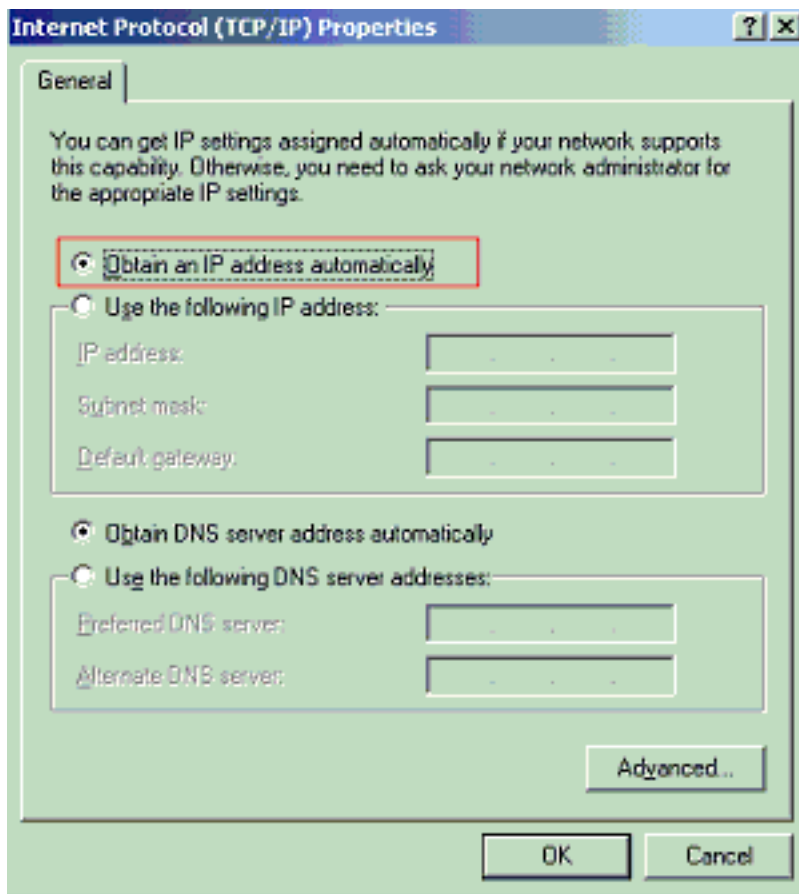
1. Kies **Start > Control Panel > Network Connections**, klik met de rechtermuisknop op uw **Local Area Connection** en kies **Properties**.
2. Controleer **pictogram in waarschuwing** op het tabblad **Algemeen**.
3. Controleer onder het tabblad **Verificatie** de **verificatie van IEEE 802.1x voor dit 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.

[Configuratie van de IP-telefoons die gebruikt moeten worden 802.1x-verificatie](#)

Voltooi deze stappen om de IP-telefoons te configureren voor 802.1x verificatie.

1. Druk op de knop **Instellingen** om toegang te krijgen tot de instellingen voor **802.1X-verificatie** en kies **Security Configuration > 802.1X-verificatie > Apparaatverificatie**.
2. Stel de optie **Apparaatverificatie** in op **Ingeschakeld**.
3. Druk op de knop **Opslaan**.
4. Kies **802.1X verificatie > EAP-MD5 > Shared Secret** om een wachtwoord op de telefoon in te stellen.
5. Voer het gedeelde geheim in en druk op **Opslaan**. **Opmerking:** het wachtwoord moet tussen zes en 32 tekens liggen, die uit een combinatie van getallen of letters bestaan. *Deze toets is niet actief hier* wordt het bericht getoond en het wachtwoord wordt niet opgeslagen als niet aan deze voorwaarde wordt voldaan. **Opmerking:** Als u 802.1X-verificatie uitschakelt of een fabrieksreset uitvoert aan de telefoon, wordt het eerder ingestelde MD5 gedeelde geheim verwijderd. **N.B.:** De andere opties, apparaten ID en velg kunnen niet worden ingesteld. ApparaatID wordt gebruikt als gebruikersnaam voor 802.1x-verificatie. Dit is een derivaat van het modelnummer van de telefoon en een uniek MAC-adres dat in deze indeling wordt weergegeven: CP-<model>-SEP-<MAC>. Bijvoorbeeld **CP-7970G-SEP001759E7492C**. Raadpleeg [802.1X verificatie-instellingen](#) voor meer informatie.

Voltooi deze stappen om de IP-telefoon te configureren om het IP-adres te verkrijgen van een DHCP-server.

1. Druk op de knop **Instellingen** om de instellingen voor de **netwerkconfiguratie** te kunnen benaderen en kies **Netwerkconfiguratie**.
2. Opties voor **netwerkconfiguratie** ontgrendelen. Druk op ****#** om de vergrendeling te

- opgeheven.** **Opmerking:** Druk niet op ****#** om de opties te ontgrendelen en druk vervolgens direct op ****#** opnieuw om de opties te vergrendelen. De telefoon interpreteert deze reeks als ****#****, die de telefoon herstelt. Als u de opties wilt vergrendelen nadat u deze hebt ontgrendeld, wacht dan ten minste 10 seconden voordat u ****#** opnieuw op de knop drukt.
3. Scrollt naar de DHCP-enabled optie en druk op de **Ja**-toets om DHCP in te schakelen.
 4. Druk op de knop **Opslaan**.

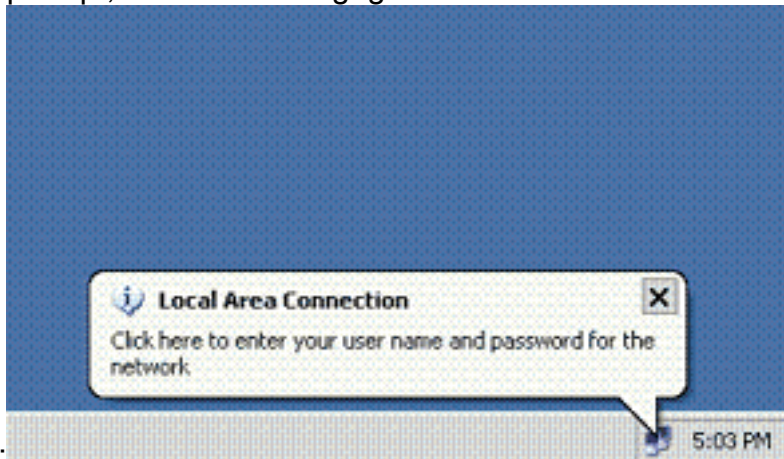
Verifiëren

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

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.

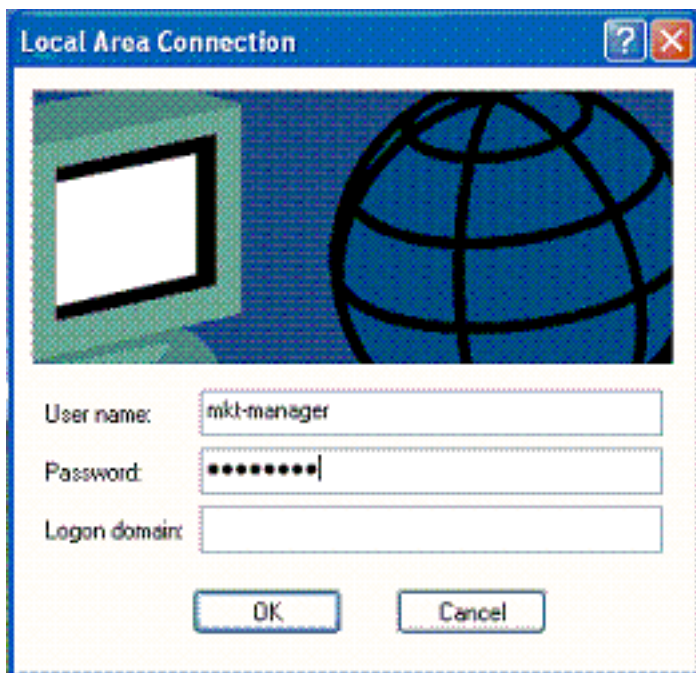
1. Klik op de prompt, die wordt weergegeven in dit



voorbeeld:

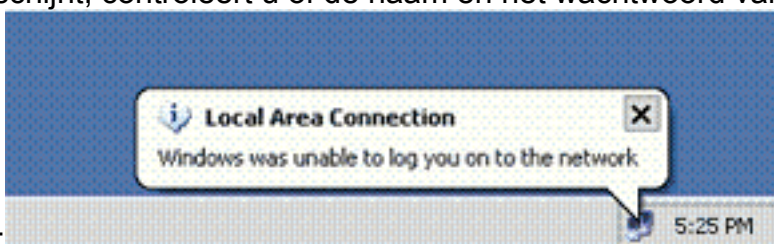
Het venster voor de gebruikersnaam en het invoeren van een wachtwoord wordt weergegeven. **Opmerking:** MDA dwingt de volgorde van de apparaatverificatie niet af. Maar, voor het beste resultaat, adviseert Cisco dat een stemapparaat voor een gegevensapparaat op een MDA enabled poort wordt authentiek verklaard.

2. Voer de gebruikersnaam en het wachtwoord



in.

- Als er geen foutmeldingen verschijnen, controleer dan de connectiviteit met de gebruikelijke methoden, zoals door toegang tot de netwerkbronnen en door ping. **N.B.:** Als deze fout verschijnt, controleert u of de naam en het wachtwoord van de gebruiker juist



zijn:

IP-telefoons

Met het menu 802.1X-verificatiestatus in de IP-telefoons kunt u de verificatiestatus controleren.

- Druk op de knop **Instellingen** om toegang te krijgen tot de 802.1X-verificatie, Real-Time switches en kies **Security Configuration > 802.1X verificatiestatus**.
- De **transactiestatus** moet worden **gemarkeerd**. Raadpleeg [802.1X Real-Time status voor verificatie](#) voor meer informatie. **Opmerking:** De authenticatiestatus kan ook worden geverifieerd via **Settings > Status > Status-berichten**.

Layer 3 Switch

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

- Zoek naar een havenstatus die **geautoriseerd aangeeft**.

```
Cat-3560#show dot1x all summary
```

Interface	PAE	Client	Status
Fa0/1	AUTH	0016.3633.339c	AUTHORIZED
		0017.59e7.492c	AUTHORIZED
Fa0/2	AUTH	0014.5e94.5f99	AUTHORIZED
Fa0/3	AUTH	0011.858D.9AF9	AUTHORIZED
Fa0/4	AUTH	0016.6F3C.A342	AUTHORIZED
		001a.2f80.381f	AUTHORIZED

Cat-3560#show dot1x interface fastEthernet 0/1 details

Dot1x Info for FastEthernet0/1

```
-----  
PAE = AUTHENTICATOR  
PortControl = AUTO  
ControlDirection = Both  
HostMode = MULTI_DOMAIN  
ReAuthentication = Enabled  
QuietPeriod = 10  
ServerTimeout = 30  
SuppTimeout = 30  
ReAuthPeriod = 60 (Locally configured)  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30  
RateLimitPeriod = 0  
Auth-Fail-Vlan = 6  
Auth-Fail-Max-attempts = 2  
Guest-Vlan = 6
```

Dot1x Authenticator Client List

```
-----  
Domain = DATA  
Supplicant = 0016.3633.339c  
  Auth SM State = AUTHENTICATED  
  Auth BEND SM State = IDLE  
Port Status = AUTHORIZED  
ReAuthPeriod = 60  
ReAuthAction = Reauthenticate  
TimeToNextReauth = 29  
Authentication Method = Dot1x  
Authorized By = Authentication Server  
Vlan Policy = 4
```

```
Domain = VOICE  
Supplicant = 0017.59e7.492c  
  Auth SM State = AUTHENTICATED  
  Auth BEND SM State = IDLE  
Port Status = AUTHORIZED  
ReAuthPeriod = 60  
ReAuthAction = Reauthenticate  
TimeToNextReauth = 15  
Authentication Method = Dot1x  
Authorized By = Authentication Server
```

Controleer de VLAN-status na succesvolle verificatie.

Cat-3560#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Gi0/1 Gi0/2
2 SERVER	active	Fa0/24
3 VOICE	active	Fa0/1, Fa0/4
4 MARKETING	active	Fa0/1, Fa0/2
5 SALES	active	Fa0/3, Fa0/4
6 GUEST_and_AUTHFAIL	active	

```
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-bindende status na een succesvolle verificatie.

```
Router#show ip dhcp binding
IP address      Hardware address   Lease expiration   Type
172.16.3.2     0100.1759.e749.2c  Aug 24 2007 06:35 AM  Automatic
172.16.3.3     0100.1a2f.8038.1f  Aug 24 2007 06:43 AM  Automatic
172.16.4.2     0100.1636.3333.9c  Aug 24 2007 06:50 AM  Automatic
172.16.4.3     0100.145e.945f.99  Aug 24 2007 08:17 AM  Automatic
172.16.5.2     0100.166F.3CA3.42  Aug 24 2007 08:23 AM  Automatic
172.16.5.3     0100.1185.8D9A.F9  Aug 24 2007 08:51 AM  Automatic
```

Het [Uitvoer Tolk](#) ([uitsluitend geregistreeerde](#) klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van de opdrachtoutput van de **show** te bekijken.

Problemen oplossen

IP-telefoonverificatie mislukt

IP-telefoonstatus geeft configuratie van IP-of registratie als 802.1x-verificatie mislukt. Voltooi deze stappen om een oplossing voor deze problemen te vinden:

- Bevestig dat de 802.1x op de IP-telefoon is ingeschakeld.
- Controleer of u het apparaat-ID op de verificatie (RADIUS) server als gebruikersnaam hebt ingevoerd.
- Bevestig dat het gedeelde geheim op de IP-telefoon is ingesteld.
- Als het gedeelde geheim is ingesteld, controleer of u hetzelfde gedeelde geheim hebt dat op de verificatieserver is ingevoerd.
- Controleer dat u de andere vereiste apparaten correct hebt ingesteld, bijvoorbeeld de switch- en de authenticatieserver.

Gerelateerde informatie

- [De IEEE 802.1x-poortgebaseerde verificatie configureren](#)
- [Configuratie van de IP-telefoon om 802.1x verificatie te gebruiken](#)
- [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](#)
- [IEEE 802.1x-verificatie met Catalyst 6500/6000 actieve Cisco IOS-softwareconfiguratie - voorbeeld](#)
- [IEEE 802.1x-verificatie met Catalyst 6500/6000-actieve CatOS-softwareconfiguratievoorbeeld](#)
- [Productondersteuningspagina's voor LAN](#)
- [Ondersteuningspagina voor LAN-switching](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)