

IEEE 802.1x-Authentifizierung mit Catalyst 6500/6000 mit CatOS-Software - Konfigurationsbeispiel

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren des Catalyst Switches für die 802.1x-Authentifizierung](#)

[Konfigurieren des RADIUS-Servers](#)

[Konfigurieren der 802.1x-Authentifizierung für PC-Clients](#)

[Überprüfen](#)

[PC-Clients](#)

[Catalyst 6500](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird erläutert, wie IEEE 802.1x auf einem Catalyst 6500/6000 konfiguriert wird, der im Hybrid-Modus (CatOS auf der Supervisor Engine und Cisco IOS® Software auf der MSFC) sowie auf einem RADIUS-Server (Remote Authentication Dial-In User Service) für Authentifizierung und VLAN-Zuweisung ausgeführt wird.

[Voraussetzungen](#)

[Anforderungen](#)

Die Leser dieses Dokuments sollten folgende Themen kennen:

- [Installationsanleitung für Cisco Secure ACS für Windows 4.1](#)
- [Benutzerhandbuch für Cisco Secure Access Control Server 4.1](#)
- [Wie wirkt RADIUS?](#)
- [Catalyst Switching- und ACS-Bereitstellungsleitfaden](#)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst 6500 mit CatOS Software Release 8.5(6) auf der Supervisor Engine und Cisco IOS Software Release 12.2(18)SXF auf der MSFC **Hinweis:** Sie benötigen CatOS 6.2 oder höher, um die 802.1x-Port-basierte Authentifizierung zu unterstützen. **Hinweis:** Nach der Authentifizierung des 802.1x-Hosts vor Softwareversion 7.2(2) wird dieser einem im NVRAM konfigurierten VLAN hinzugefügt. Mit der Softwareversion 7.2(2) und höheren Versionen kann ein 802.1x-Host nach der Authentifizierung seine VLAN-Zuweisung vom RADIUS-Server erhalten.
- In diesem Beispiel wird der Cisco Secure Access Control Server (ACS) 4.1 als RADIUS-Server verwendet. **Hinweis:** Vor der Aktivierung von 802.1x auf dem Switch muss ein RADIUS-Server angegeben werden.
- PC-Clients, die 802.1x-Authentifizierung unterstützen. **Hinweis:** In diesem Beispiel werden Microsoft Windows XP-Clients verwendet.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Der IEEE 802.1x-Standard definiert ein Client-Server-basiertes Zugriffskontroll- und Authentifizierungsprotokoll, das verhindert, dass nicht autorisierte Geräte über öffentlich zugängliche Ports mit einem LAN verbunden werden. 802.1x steuert den Netzwerkzugriff, indem an jedem Port zwei getrennte virtuelle Access Points erstellt werden. Ein Access Point ist ein unkontrollierter Port, der andere ist ein kontrollierter Port. Der gesamte Datenverkehr über den einzelnen Port ist für beide Access Points verfügbar. 802.1x authentifiziert jedes Benutzergerät, das an einen Switch-Port angeschlossen ist, und weist den Port einem VLAN zu, bevor alle vom Switch oder vom LAN angebotenen Services verfügbar gemacht werden. Bis zur Authentifizierung des Geräts lässt die 802.1x-Zugriffskontrolle nur EAP-Datenverkehr (Extensible Authentication Protocol) über LAN (EAPOL) über den Port zu, mit dem das Gerät verbunden ist. Nach erfolgreicher Authentifizierung kann normaler Datenverkehr den Port passieren.

Konfigurieren

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der 802.1x-Funktion, die in diesem Dokument beschrieben wird.

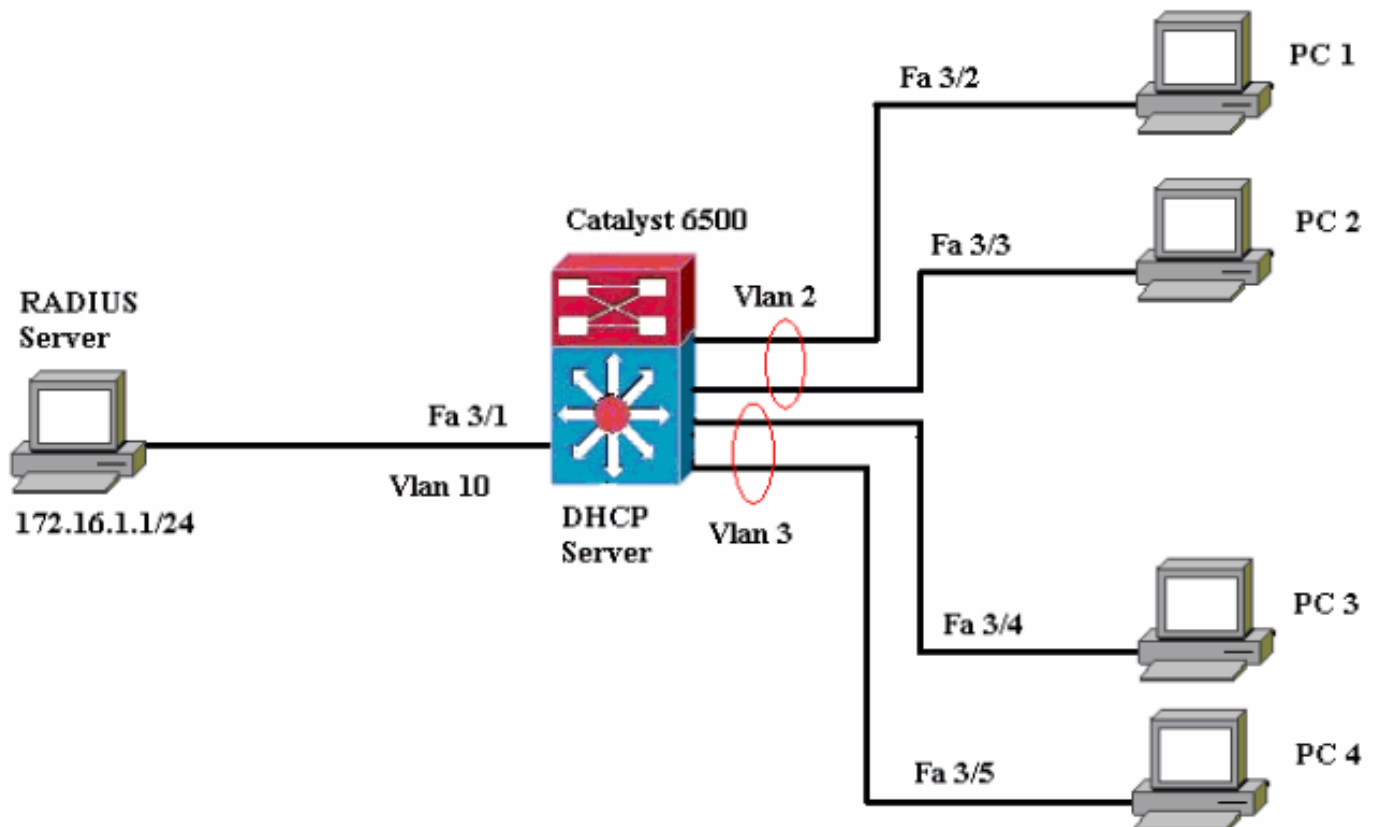
Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Für diese Konfiguration sind folgende Schritte erforderlich:

- [Konfigurieren des Catalyst Switches für die 802.1x-Authentifizierung](#)
- [Konfigurieren des RADIUS-Servers](#)
- [Konfigurieren der 802.1x-Authentifizierung für PC-Clients](#)

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



- RADIUS server (RADIUS-Server): Führt die eigentliche Authentifizierung des Clients durch. Der RADIUS-Server validiert die Identität des Clients und benachrichtigt den Switch, ob der Client für den Zugriff auf das LAN und die Switch-Services autorisiert ist. Hier wird der RADIUS-Server für die Authentifizierung und VLAN-Zuweisung konfiguriert.
- Switch - Steuert den physischen Zugriff auf das Netzwerk basierend auf dem Authentifizierungsstatus des Clients. Der Switch fungiert als Vermittler (Proxy) zwischen dem Client und dem RADIUS-Server, der Identitätsinformationen vom Client anfordert, diese Informationen mit dem RADIUS-Server verifiziert und eine Antwort an den Client weiterleitet. Hier wird der Catalyst Switch der Serie 6500 auch als DHCP-Server konfiguriert. Die 802.1x-Authentifizierungsunterstützung für das Dynamic Host Configuration Protocol (DHCP) ermöglicht es dem DHCP-Server, die IP-Adressen den verschiedenen Endbenutzerklassen zuzuweisen, indem die authentifizierte Benutzeridentität dem DHCP-Erkennungsvorgang hinzugefügt wird.
- Clients - Die Geräte (Workstations), die Zugriff auf das LAN und die Switch-Services anfordern und auf Anfragen vom Switch reagieren. Hier sind die PCs 1 bis 4 die Clients, die einen authentifzierten Netzwerkzugriff anfordern. PCs 1 und 2 verwenden dieselben Anmeldeinformationen wie VLAN 2. Ebenso verwenden PCs 3 und 4 eine

Anmeldeinformationen für VLAN 3. PC-Clients sind so konfiguriert, dass sie die IP-Adresse von einem DHCP-Server erhalten. **Hinweis:** Bei dieser Konfiguration wird jedem Client, der die Authentifizierung nicht durchführt, oder jedem anderen nicht 802.1x-fähigen Client, der eine Verbindung mit dem Switch herstellt, der Netzwerkzugriff verweigert, indem er diese unter Verwendung der Authentifizierungsfehler und der Gast-VLAN-Funktionen in ein ungenutztes VLAN (VLAN 4 oder 5) verschiebt.

Konfigurieren des Catalyst Switches für die 802.1x-Authentifizierung

Diese Switch-Beispielkonfiguration umfasst:

- Aktivieren Sie die 802.1x-Authentifizierung und die zugehörigen Funktionen auf FastEthernet-Ports.
- Verbinden Sie den RADIUS-Server hinter dem FastEthernet-Port 3/1 mit dem VLAN 10.
- DHCP-Serverkonfiguration für zwei IP-Pools, einer für Clients in VLAN 2 und einer für Clients in VLAN 3.
- Inter-VLAN-Routing für Verbindungen zwischen Clients nach der Authentifizierung.

Die Richtlinien zur Konfiguration der 802.1x-Authentifizierung finden Sie in den [Authentifizierungskonfigurationsrichtlinien](#).

Hinweis: Stellen Sie sicher, dass der RADIUS-Server immer hinter einem autorisierten Port eine Verbindung herstellt.

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
successssful 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.
Spanntree 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

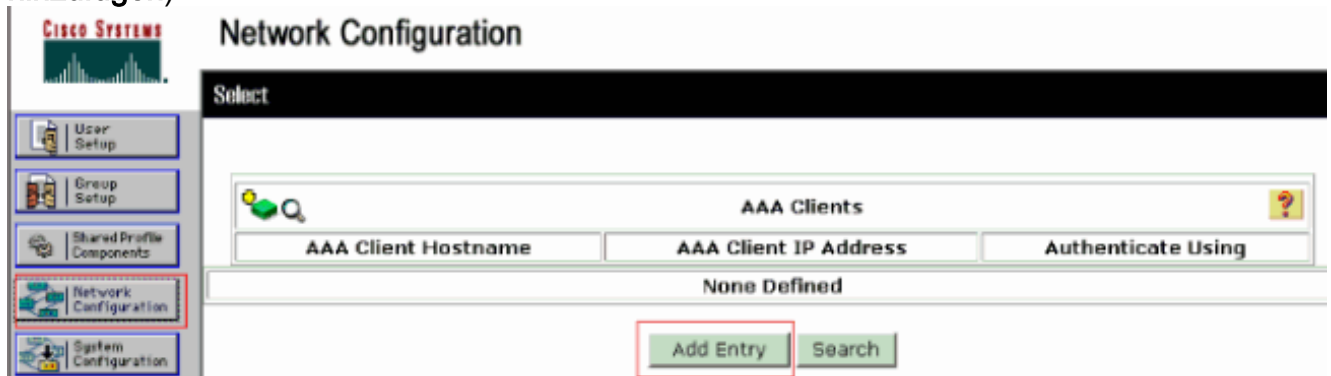
3/2-48
2 VLAN2 active 83
3 VLAN3 active 84
4 AUTHFAIL_VLAN active 85
5 GUEST_VLAN active 86
10 RADIUS_SERVER active 87
3/1
1002 fddi-default active 78
1003 token-ring-default active 81
1004 fddinet-default active 79
1005 trnet-default active 80
!--- Output suppressed. !--- All active ports will be in
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)

```


Konfigurieren des RADIUS-Servers

Der RADIUS-Server ist mit der statischen IP-Adresse 172.16.1.1/24 konfiguriert. Gehen Sie wie folgt vor, um den RADIUS-Server für einen AAA-Client zu konfigurieren:

1. Um einen AAA-Client zu konfigurieren, klicken Sie im ACS-Administrationsfenster auf **Network Configuration** (Netzwerkkonfiguration).
2. Klicken Sie im Bereich "AAA-Clients" auf **Add Entry** (Eintrag hinzufügen).



3. Konfigurieren Sie den Hostnamen, die IP-Adresse, den gemeinsamen geheimen Schlüssel und den Authentifizierungstyp des AAA-Clients wie folgt: AAA-Client-Hostname = Switch-Hostname (**Cat6K**). IP-Adresse des AAA-Clients = Management Interface (sc0) IP-Adresse des Switches (**172.16.1.2**). Shared Secret = Radius Key, der auf dem Switch konfiguriert ist (**cisco**). Authentifizierung mit = **RADIUS IETF**. **Hinweis:** Für den ordnungsgemäßen Betrieb muss der gemeinsam verwendete geheime Schlüssel auf dem AAA-Client und dem ACS identisch sein. Schlüssel beachten die Groß- und Kleinschreibung.
4. Klicken Sie auf **Senden + Übernehmen**, um diese Änderungen wirksam zu machen, wie im folgenden Beispiel gezeigt:



Network Configuration

Add AAA Client

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

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

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

Gehen Sie wie folgt vor, um den RADIUS-Server für die Authentifizierung, VLAN- und IP-Adresszuweisung zu konfigurieren:

Für Clients, die eine Verbindung zu VLAN 2 herstellen, sowie für VLAN 3 müssen zwei Benutzernamen separat erstellt werden. Hierzu werden ein user **user_vlan2** für Clients, die mit VLAN 2 verbunden sind, und ein weiterer user **user_vlan3** für Clients, die mit VLAN 3 verbunden sind, erstellt.

Hinweis: Hier wird die Benutzerkonfiguration für Clients angezeigt, die nur mit VLAN 2 verbunden sind. Führen Sie für Benutzer, die eine Verbindung zu VLAN 3 herstellen, das gleiche Verfahren aus.

1. Um Benutzer hinzuzufügen und zu konfigurieren, klicken Sie auf **Benutzereinrichtung** und definieren Sie Benutzernamen und Kennwort.

CISCO SYSTEMS **User Setup**

Select

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](#)

CISCO SYSTEMS **User Setup**

Edit

User: user_vlan2 (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

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

Password

Confirm Password

2. Definieren Sie die Client-IP-Adressenzuweisung als vom AAA-Clientpool zugewiesen. Geben Sie den Namen des auf dem Switch für VLAN 2-Clients konfigurierten IP-Adresspools

ein.

CISCO SYSTEMS

User Setup

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:

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

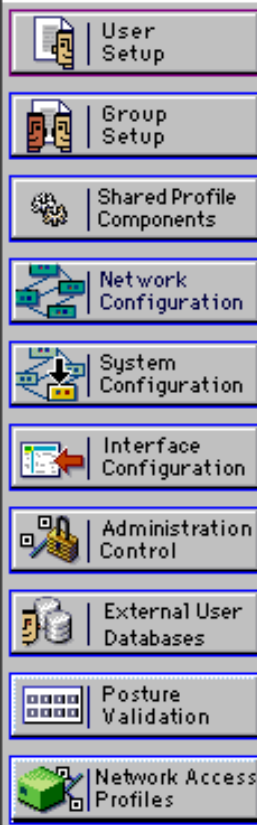
- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

Hinweis: Wählen Sie diese Option aus, und geben Sie den Namen des AAA-Client-IP-Pools in das Feld ein, nur wenn diesem Benutzer die IP-Adresse zugewiesen werden soll, die von einem IP-Adresspool auf dem AAA-Client konfiguriert wurde.

3. Definieren Sie die IETF-Attribute (Internet Engineering Task Force) 64 und 65. Stellen Sie sicher, dass die Tags der Werte auf 1 festgelegt sind, wie im folgenden Beispiel veranschaulicht wird. Catalyst ignoriert alle anderen Tags als 1. Um einen Benutzer einem bestimmten VLAN zuzuweisen, müssen Sie auch das Attribut 81 mit einem *VLAN-Namen* definieren, der *dem Namen* entspricht. **Hinweis:** Der *VLAN-Name* muss mit dem im Switch konfigurierten Namen identisch sein. **Hinweis:** VLAN-Zuordnung basierend auf *VLAN-Nummer* wird von CatOS nicht unterstützt.



User Setup



Checking this option will PERMIT all UNKNOWN Services

Default (Undefined) Services

IETF RADIUS Attributes

[006] Service-Type

[064] Tunnel-Type

Tag 1 Value VLAN

[065] Tunnel-Medium-Type

Tag 1 Value 802

[081] Tunnel-Private-Group-ID

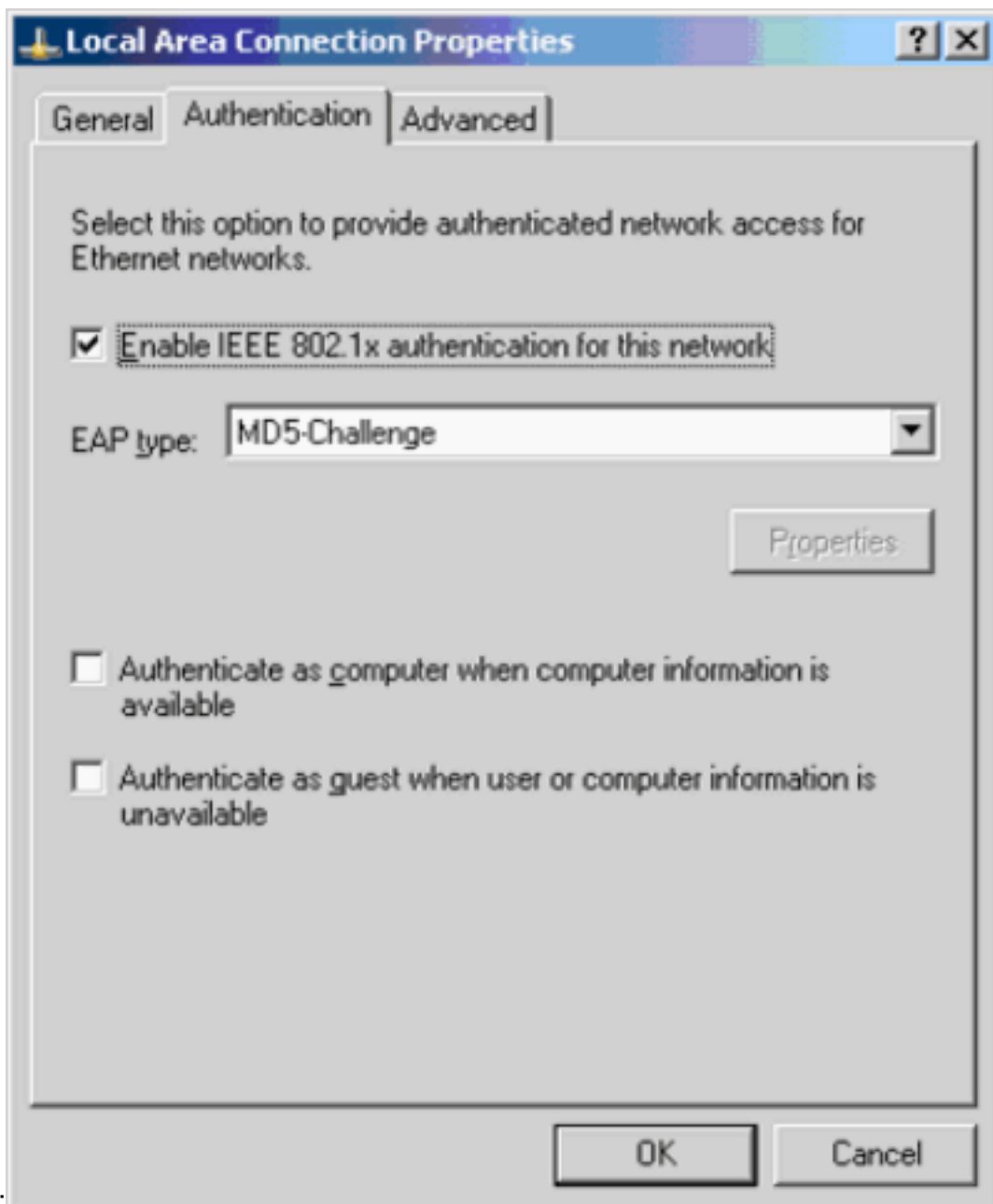
Tag 1 Value VLAN2

Siehe [RFC 2868: RADIUS Attributes for Tunnel Protocol Support](#) für weitere Informationen zu diesen IETF-Attributen. **Hinweis:** Bei der Erstkonfiguration des ACS-Servers können die IETF-RADIUS-Attribute im **Benutzersetup** nicht angezeigt werden. Wählen Sie **Interface configuration > RADIUS (IETF)**, um IETF-Attribute im Bildschirm für die Benutzerkonfiguration zu aktivieren. Überprüfen Sie anschließend die Attribute **64**, **65** und **81** in den Spalten Benutzer und Gruppe.

[Konfigurieren der 802.1x-Authentifizierung für PC-Clients](#)

Dieses Beispiel bezieht sich speziell auf den EAP-Client (Extensible Authentication Protocol) von Microsoft Windows XP. Gehen Sie wie folgt vor:

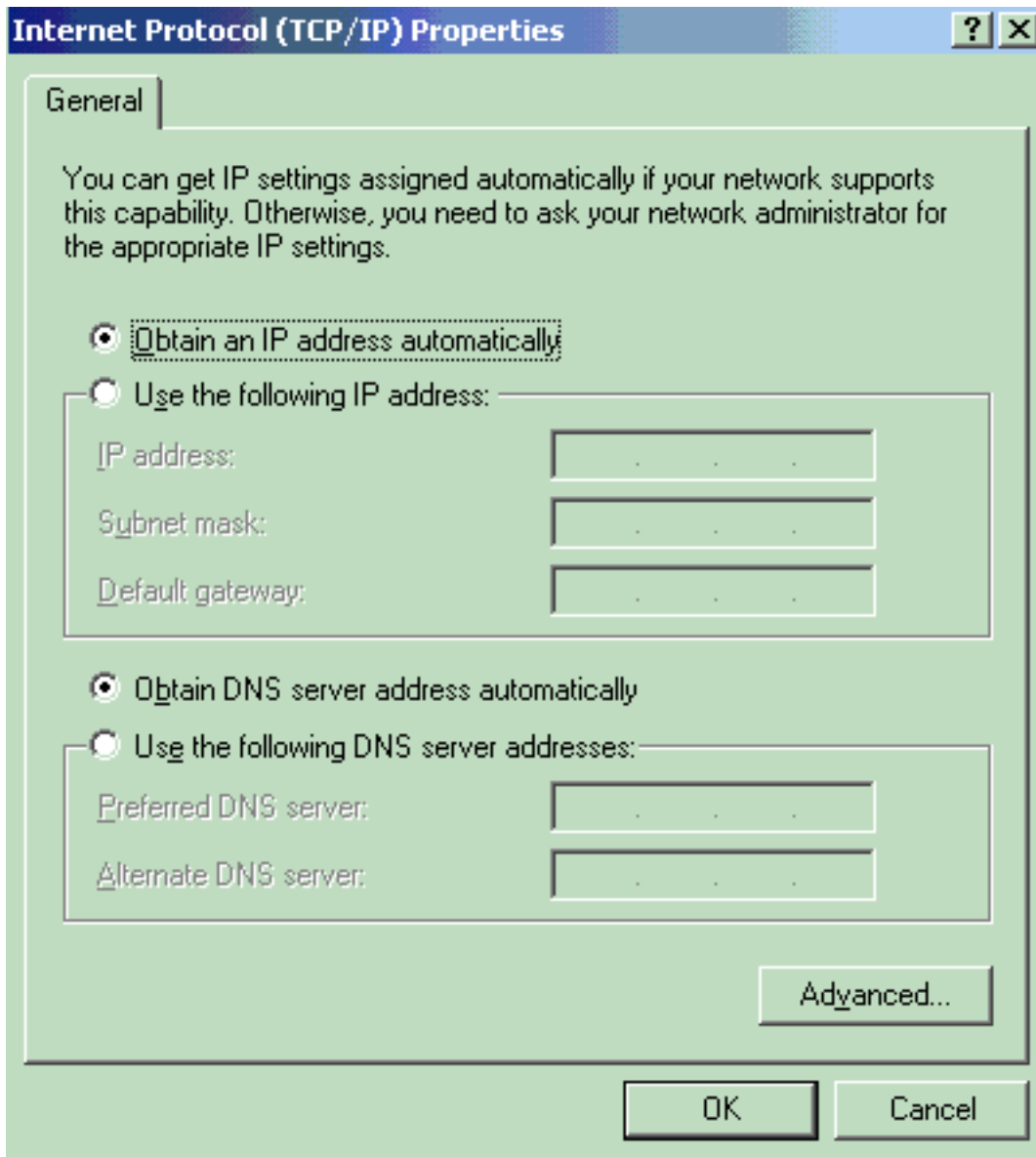
1. Wählen Sie **Start > Systemsteuerung > Netzwerkverbindungen**, klicken Sie mit der rechten Maustaste auf Ihre **LAN-Verbindung** und wählen Sie **Eigenschaften**.
2. Aktivieren Sie **unter** der Registerkarte Allgemein die **Option Symbol im Benachrichtigungsbereich anzeigen**.
3. Aktivieren Sie auf der Registerkarte Authentifizierung die Option **IEEE 802.1x-Authentifizierung für dieses Netzwerk aktivieren**.
4. Legen Sie den EAP-Typ auf **MD5-Challenge fest**, wie im folgenden Beispiel



gezeigt:

Gehen Sie wie folgt vor, um die Clients so zu konfigurieren, dass sie eine IP-Adresse von einem DHCP-Server beziehen:

1. Wählen Sie **Start > Systemsteuerung > Netzwerkverbindungen**, klicken Sie mit der rechten Maustaste auf Ihre **LAN-Verbindung** und wählen Sie **Eigenschaften**.
2. Klicken Sie auf der Registerkarte Allgemein auf **Internetprotokoll (TCP/IP)** und anschließend auf **Eigenschaften**.
3. Wählen Sie **IP-Adresse automatisch beziehen**



aus.

Überprüfen

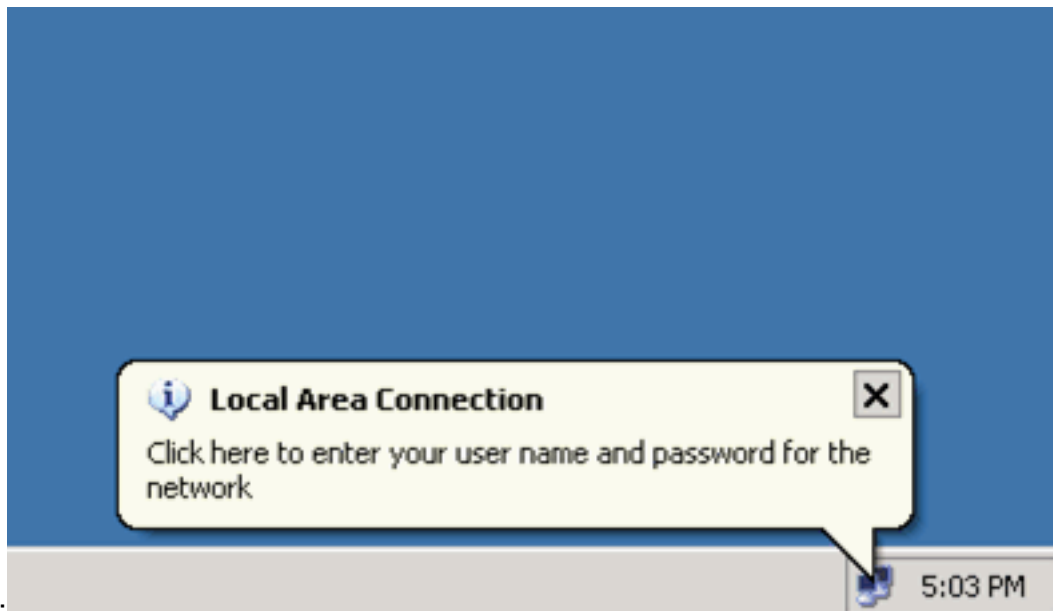
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

PC-Clients

Wenn Sie die Konfiguration korrekt abgeschlossen haben, zeigen die PC-Clients eine Popup-Aufforderung zur Eingabe von Benutzername und Kennwort an.

1. Klicken Sie auf die Eingabeaufforderung, die in diesem Beispiel angezeigt



wird:

Es wird eine

Eingabe-Fenster für Benutzername und Kennwort angezeigt.

2. Geben Sie den Benutzernamen und das Kennwort



ein.

Hinweis: Geben Sie in PC 1 und 2 die Anmeldeinformationen für VLAN 2-Benutzer ein. Geben Sie auf PC 3 und PC 4 die Anmeldeinformationen für VLAN 3 ein.

3. Wenn keine Fehlermeldungen angezeigt werden, überprüfen Sie die Verbindung mit den üblichen Methoden, z. B. durch Zugriff auf die Netzwerkressourcen und mit dem **Ping**-Befehl. Dies ist eine Ausgabe von PC 1, die einen erfolgreichen **Ping** an PC 4 anzeigt:

```
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
```

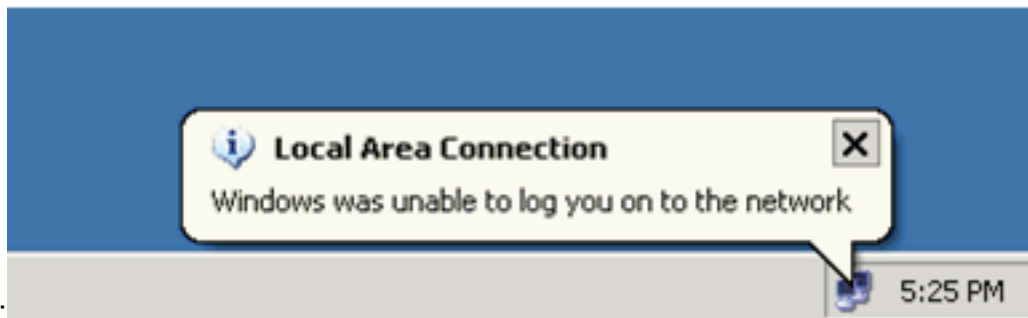
```
Ping statistics for 172.16.3.2:
```

```
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>_
```

We

nn dieser Fehler angezeigt wird, überprüfen Sie, ob Benutzername und Kennwort korrekt



sind:

Catalyst 6500

Wenn Kennwort und Benutzername korrekt angezeigt werden, überprüfen Sie den 802.1x-Portstatus auf dem Switch.

1. Suchen Sie nach einem Port-Status, der autorisiert anzeigt.

```
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
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

Überprüfen Sie den VLAN-Status nach erfolgreicher Authentifizierung.

```
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	

2. Überprüfen Sie nach erfolgreicher Authentifizierung den DHCP-Bindungsstatus vom Routing-Modul (MSFC).

```
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

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [IEEE 802.1x-Authentifizierung mit Catalyst 6500/6000 mit Ausführung der Cisco IOS Software - Konfigurationsbeispiel](#)
- [Catalyst Switching- und ACS-Bereitstellungsleitfaden](#)
- [RFC 2868: RADIUS-Attribute für die Unterstützung von Tunnelprotokollen](#)
- [Konfigurieren der 802.1x-Authentifizierung](#)
- [Support-Seiten für LAN-Produkte](#)
- [Support-Seite für LAN-Switching](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)