IEEE 802.1x-Authentifizierung mit Catalyst 6500/6000 mit Ausführung der Cisco IOS Software - Konfigurationsbeispiel

Inhalt

Einführung

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

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 Cisco IOS Software Release 12.2(18)SXF auf der Supervisor Engine**Hinweis:** Sie benötigen die Cisco IOS Software Release 12.1(13)E oder höher, um eine Port-basierte 802.1x-Authentifizierung zu unterstützen.
- 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 in den 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 er alle vom Switch oder vom LAN angebotenen Services bereitstellt. Bis zur Authentifizierung des Geräts lässt die 802.1x-Zugriffskontrolle nur EAPOL-Datenverkehr (Extensible Authentication Protocol over LAN) über den Port zu, mit dem das Gerät verbunden ist. Nach erfolgreicher Authentifizierung kann normaler Datenverkehr den Port passieren.

Hinweis: Wenn der Switch EAPOL-Pakete von dem Port empfängt, der nicht für die 802.1x-Authentifizierung konfiguriert ist, oder wenn der Switch die 802.1x-Authentifizierung nicht unterstützt, werden die EAPOL-Pakete verworfen und nicht an Upstream-Geräte weitergeleitet.

Konfigurieren

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

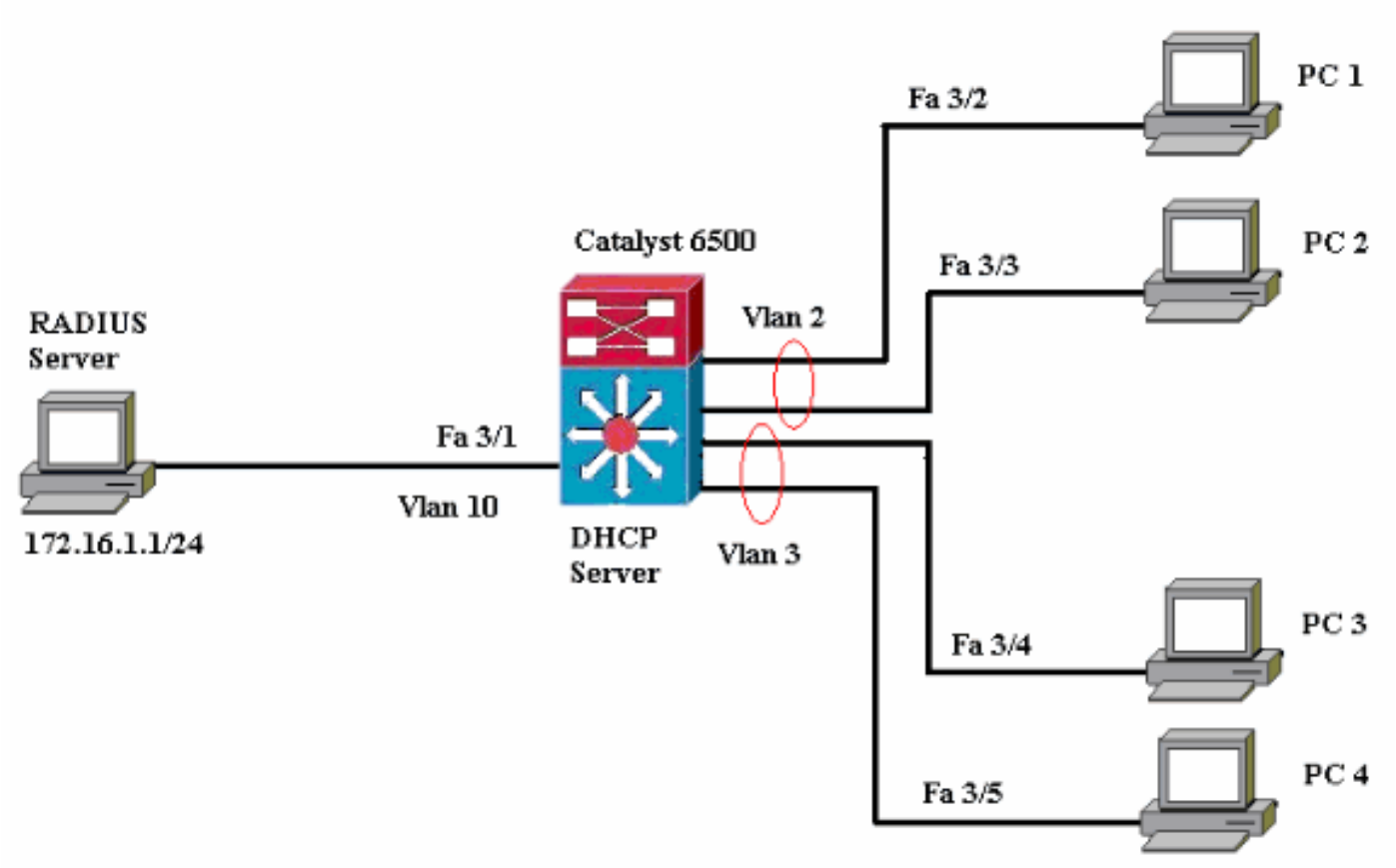
Für diese Konfiguration sind folgende Schritte erforderlich:

- Konfigurieren Sie den Catalyst Switch für die 802.1x-Authentifizierung.

- Konfigurieren Sie den RADIUS-Server.
- Konfigurieren der PC-Clients für die Verwendung der 802.1x-Authentifizierung.

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. Er fordert Identitätsinformationen vom Client an, verifiziert diese Informationen mit dem RADIUS-Server und leitet eine Antwort an den Client weiter. 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 authentifizierten Netzwerkzugriff anfordern. Die 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.

Konfigurieren des Catalyst Switches für die 802.1x-Authentifizierung

Diese Switch-Beispielkonfiguration umfasst:

- Aktivieren der 802.1x-Authentifizierung auf FastEthernet-Ports
- Anleitung zum Verbinden eines RADIUS-Servers mit VLAN 10 hinter dem FastEthernet-Port 3/1.
- Eine DHCP-Serverkonfiguration für zwei IP-Pools, einer für Clients in VLAN 2 und der andere für Clients in VLAN 3.
- Inter-VLAN-Routing für Verbindungen zwischen Clients nach der Authentifizierung.

Richtlinien zur Konfiguration der 802.1x-Authentifizierung finden Sie unter 802.1x Port-Based Authentication Guidelines and Restrictions (Richtlinien und Einschränkungen für die Port-basierte Authentifizierung).

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

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
```

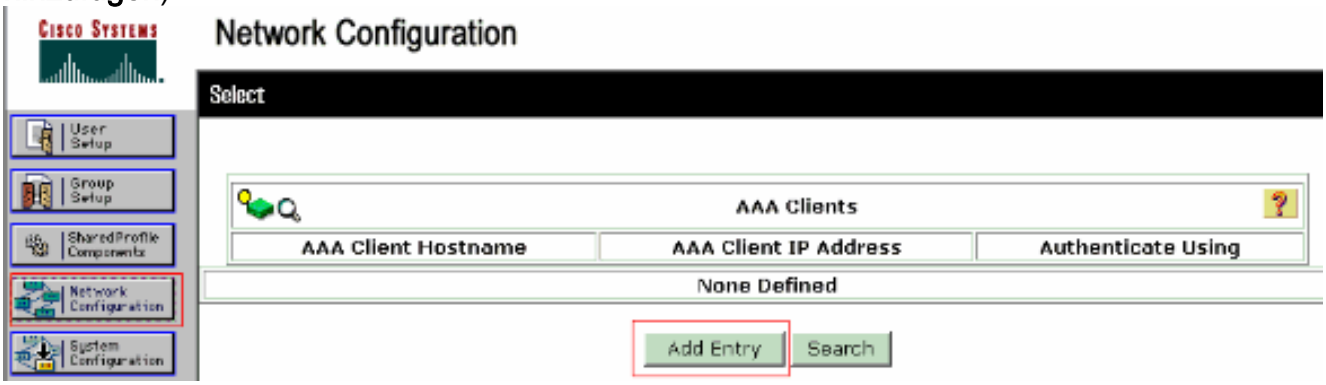
```
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
!--- Output suppressed. !--- All active ports are in
VLAN 1 (except 3/1) before authentication.
```

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

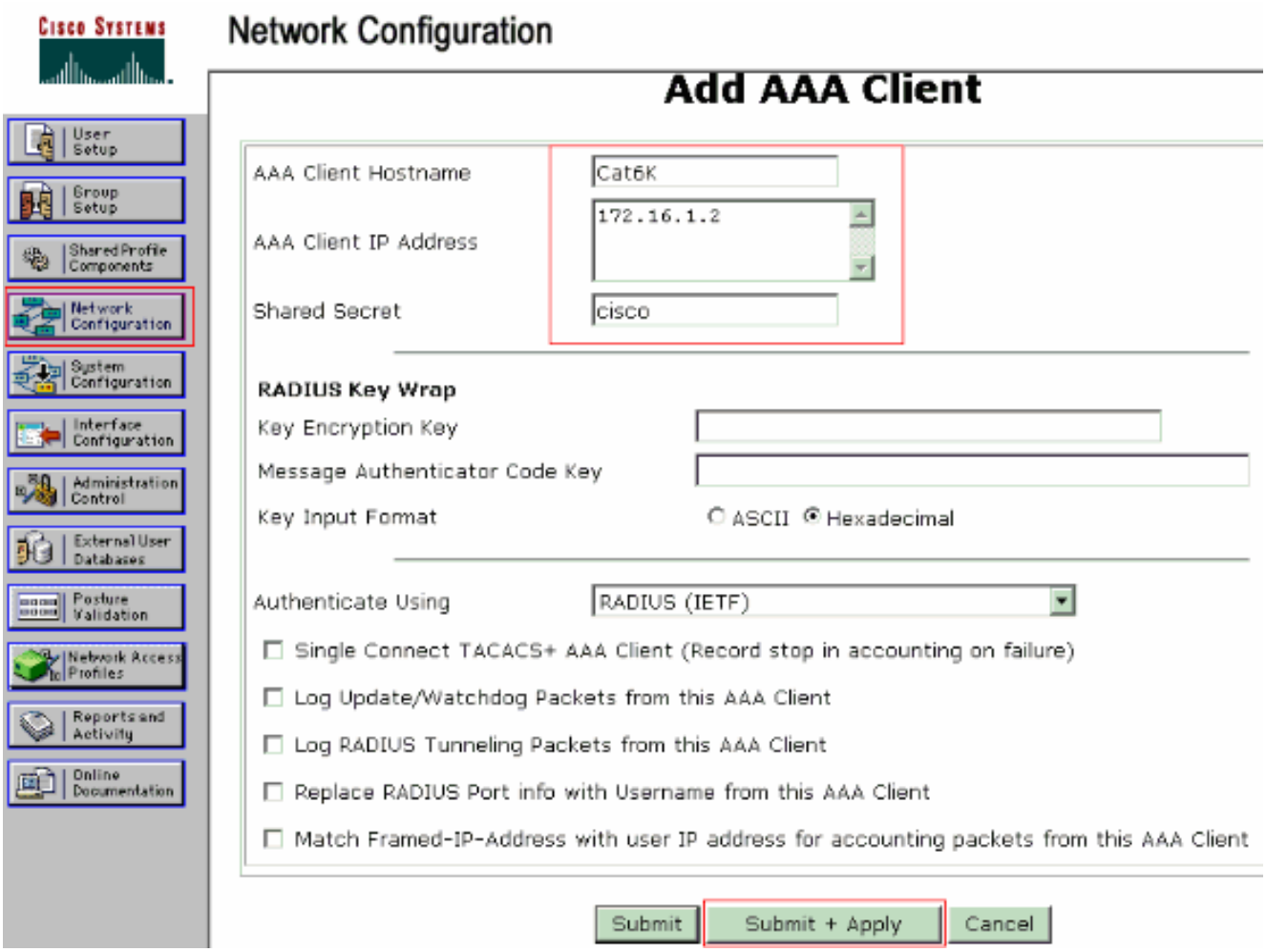
Konfigurieren des RADIUS-Servers

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. Klicken Sie im ACS-Administrationsfenster auf **Network Configuration** (Netzwerkkonfiguration), um einen AAA-Client zu konfigurieren.
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 = IP-Adresse der Verwaltungsschnittstelle des Switches (**172.16.1.2**).Shared Secret = auf dem Switch konfigurierter RADIUS-Schlüssel (**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:

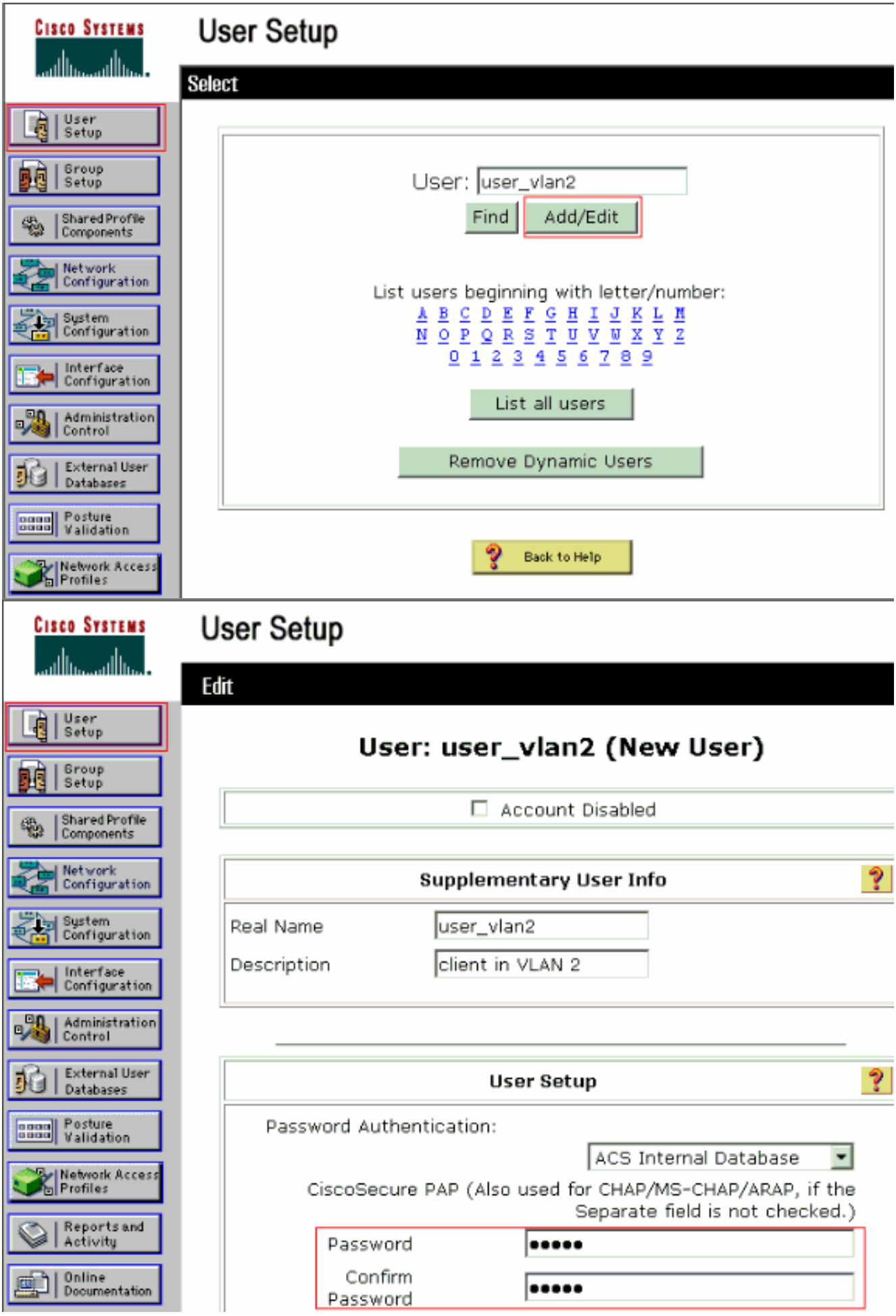


Führen Sie diese Schritte aus, um den RADIUS-Server für die Authentifizierung, VLAN- und IP-Adresszuweisung zu konfigurieren.

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

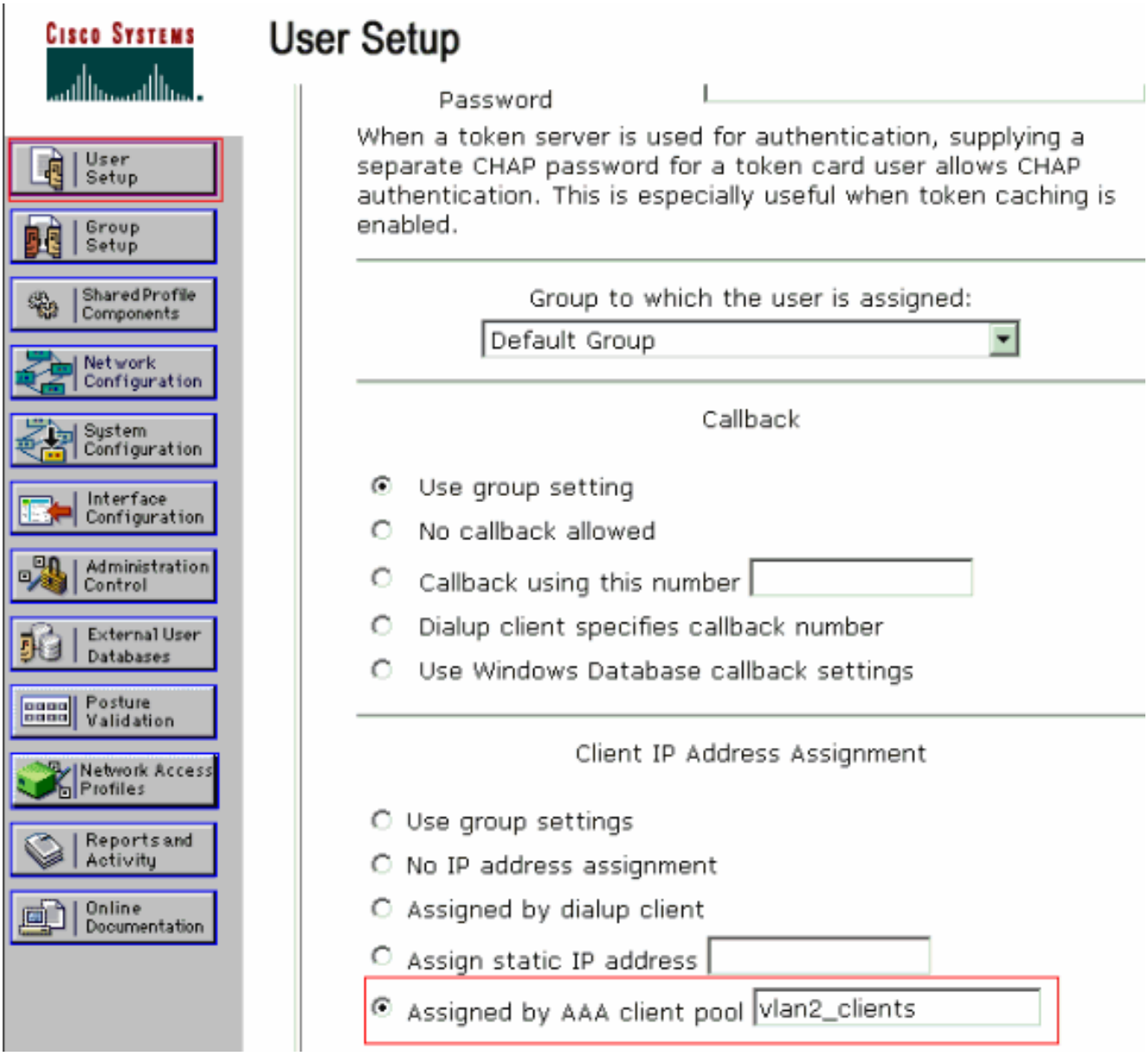
Hinweis: Hier wird die Benutzerkonfiguration für Clients angezeigt, die nur mit VLAN 2 verbunden sind. Für Benutzer, die eine Verbindung zu VLAN 3 herstellen, gehen Sie wie folgt vor.

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



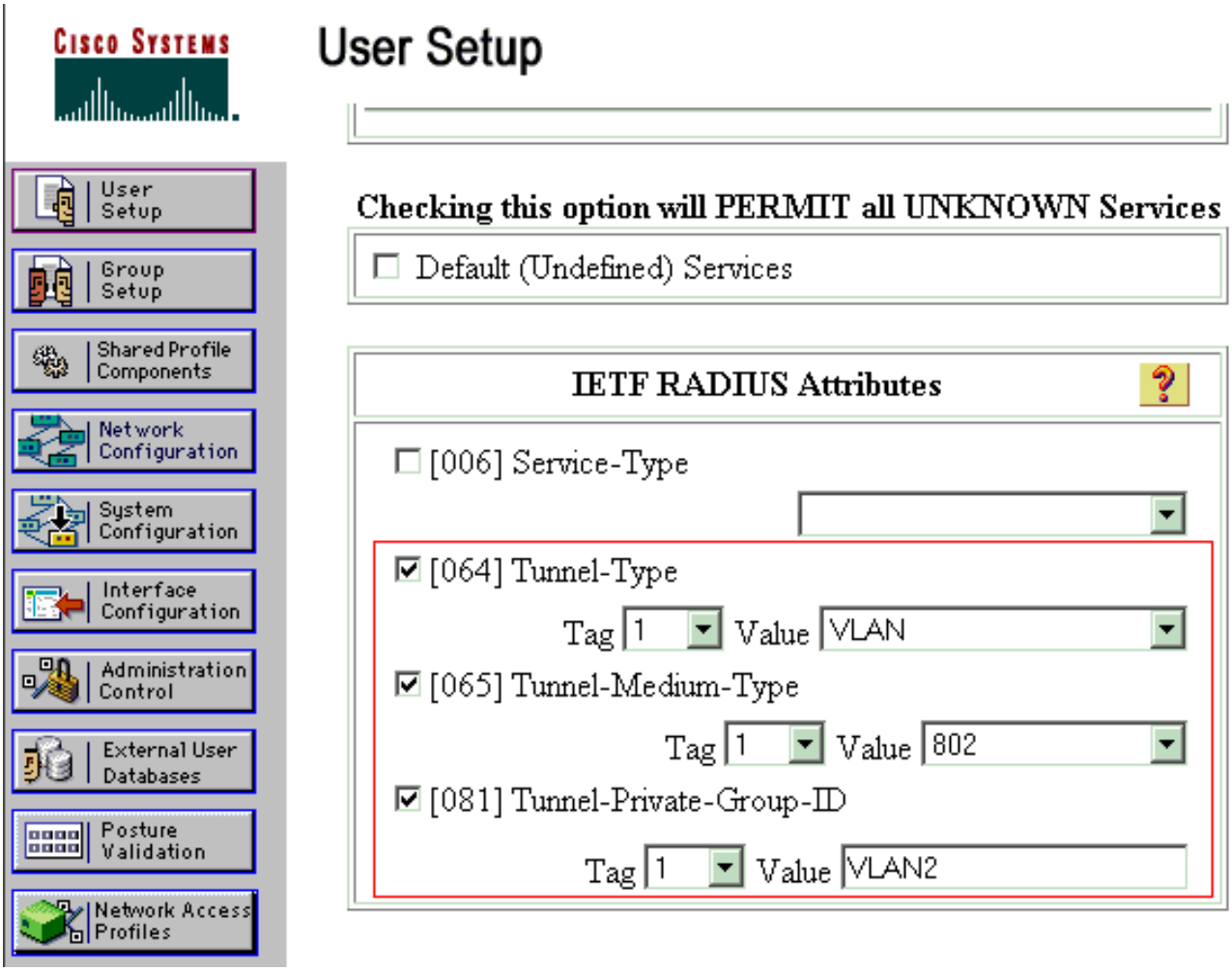
2. Definieren Sie die Client-IP-Adressenzuweisung als **vom AAA-Clientpool zugewiesen**. Geben Sie den Namen des auf dem Switch für VLAN 2-Clients konfigurierten IP-Adresspools

ein.



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 gezeigt. Catalyst ignoriert alle anderen Tags als 1. Um einen Benutzer einem bestimmten VLAN zuzuweisen, müssen Sie außerdem das Attribut **81** mit einem VLAN-*Namen* oder einer VLAN-*Nummer* definieren, die dem Attribut entspricht.**Hinweis:** Wenn Sie den VLAN-*Namen* verwenden, sollte dieser genau mit dem im Switch konfigurierten identisch sein.



Hinweis: Weitere Informationen zu diesen IETF-Attributen finden Sie in RFC 2868: RADIUS-Attribute für die Unterstützung des Tunnelprotokolls.**Hinweis:** Bei der Erstkonfiguration des ACS-Servers können die IETF-RADIUS-Attribute im **Benutzersetup** nicht angezeigt werden. Um IETF-Attribute in Benutzerkonfigurationsbildschirmen zu aktivieren, wählen Sie **Schnittstellenkonfiguration > RADIUS (IETF)** aus. Überprüfen Sie anschließend die Attribute **64**, **65** und **81** in den Spalten Benutzer und Gruppe.**Hinweis:** Wenn Sie das IETF-Attribut **81** nicht definieren und der Port ein Switch-Port im Zugriffsmodus ist, hat der Client Zuweisung zum Zugriffs-VLAN des Ports. Wenn Sie das Attribut **81** für die dynamische VLAN-Zuweisung definiert haben und der Port ein Switch-Port im Zugriffsmodus ist, müssen Sie den Befehl **einen standardmäßigen Gruppenradius für das Autorisierungsnetzwerk** auf dem Switch ausführen. Mit diesem Befehl wird der Port dem VLAN zugewiesen, das der RADIUS-Server bereitstellt. Andernfalls verschiebt 802.1x den Port nach Authentifizierung des Benutzers in den AUTORISIERTEN Status. Der Port befindet sich jedoch weiterhin im Standard-VLAN des Ports, und die Verbindung kann ausfallen. Wenn Sie das Attribut **81** definiert haben, den Port aber als gerouteten Port konfiguriert haben, wird der Zugriff verweigert. Diese Fehlermeldung wird angezeigt:

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

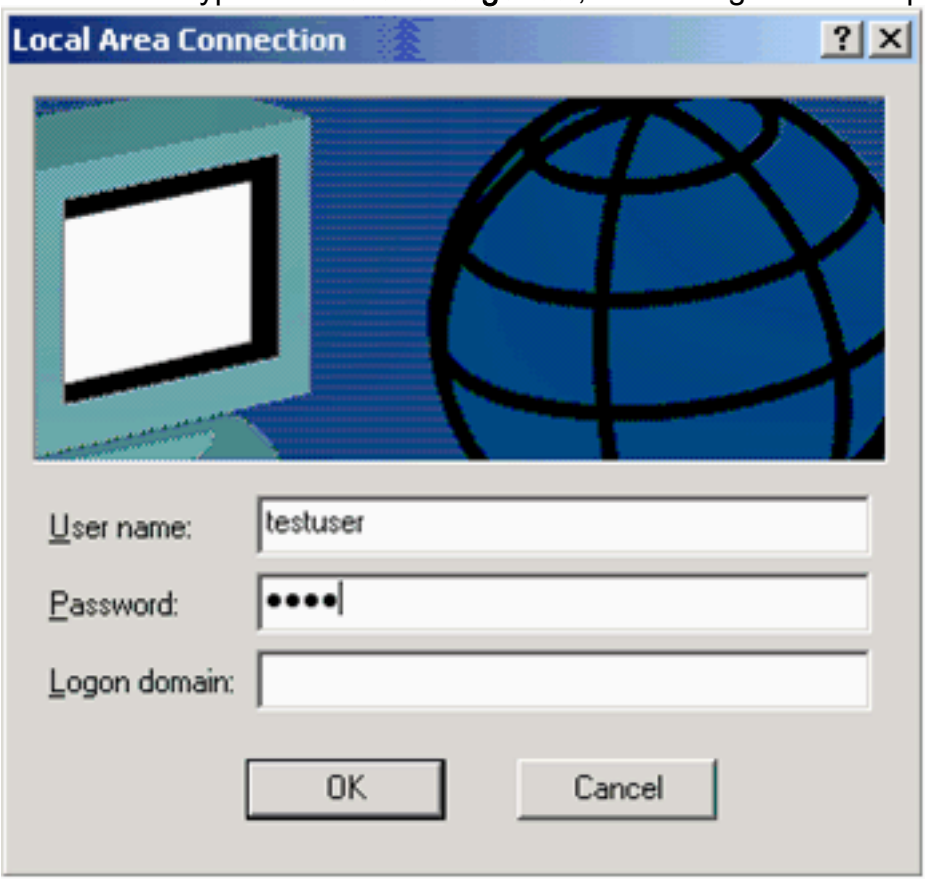
Konfigurieren der 802.1x-Authentifizierung für PC-Clients

Dieses Beispiel ist spezifisch für den EAPOL-Client (EAP over LAN) von Microsoft Windows XP:

1. Wählen Sie **Start > Systemsteuerung > Netzwerkverbindungen**, klicken Sie mit der rechten

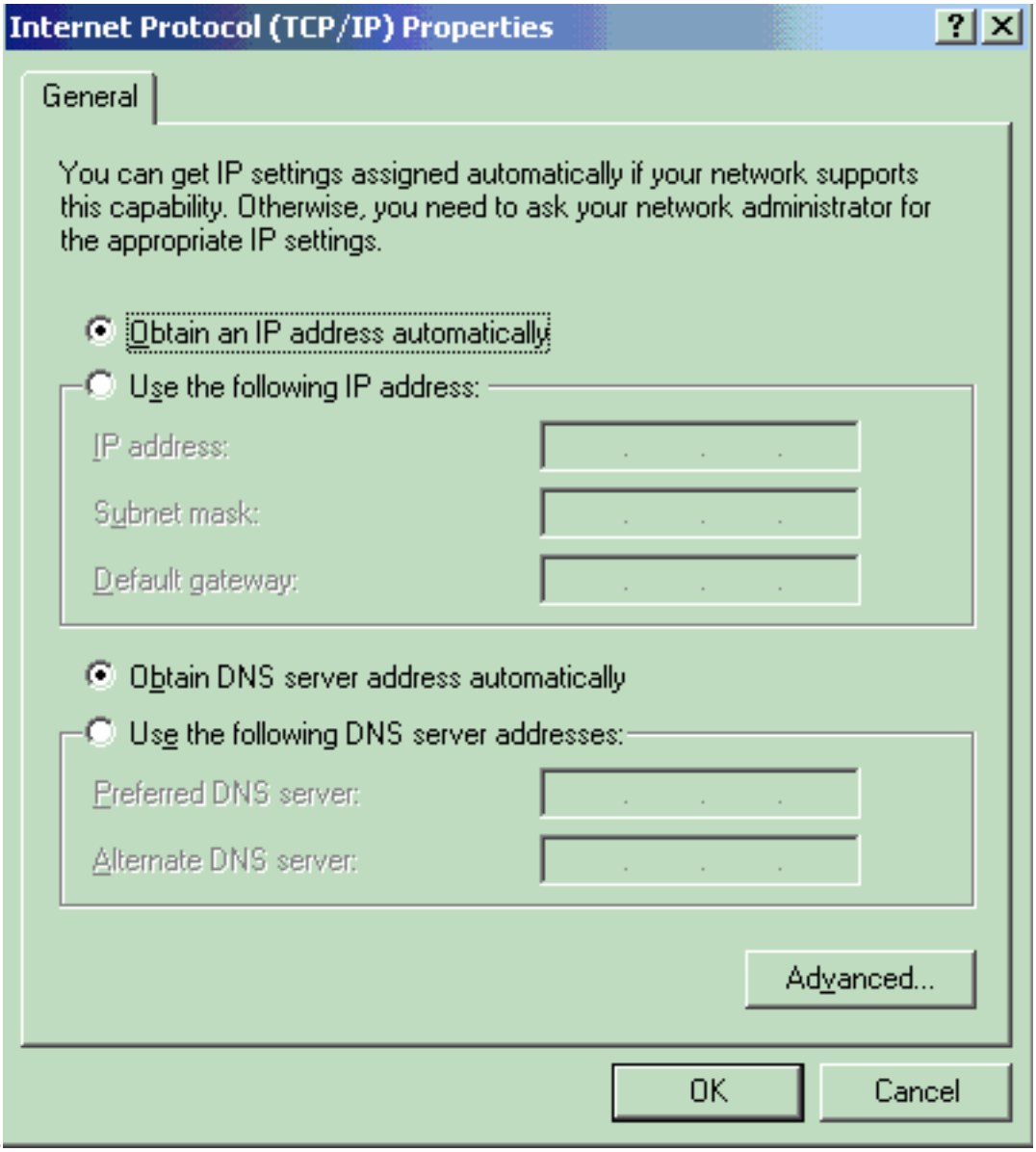
Maustaste auf Ihre **LAN-Verbindung** und wählen Sie **Eigenschaften**.

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:



Führen Sie diese Schritte aus, um die Clients so zu konfigurieren, dass sie die 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

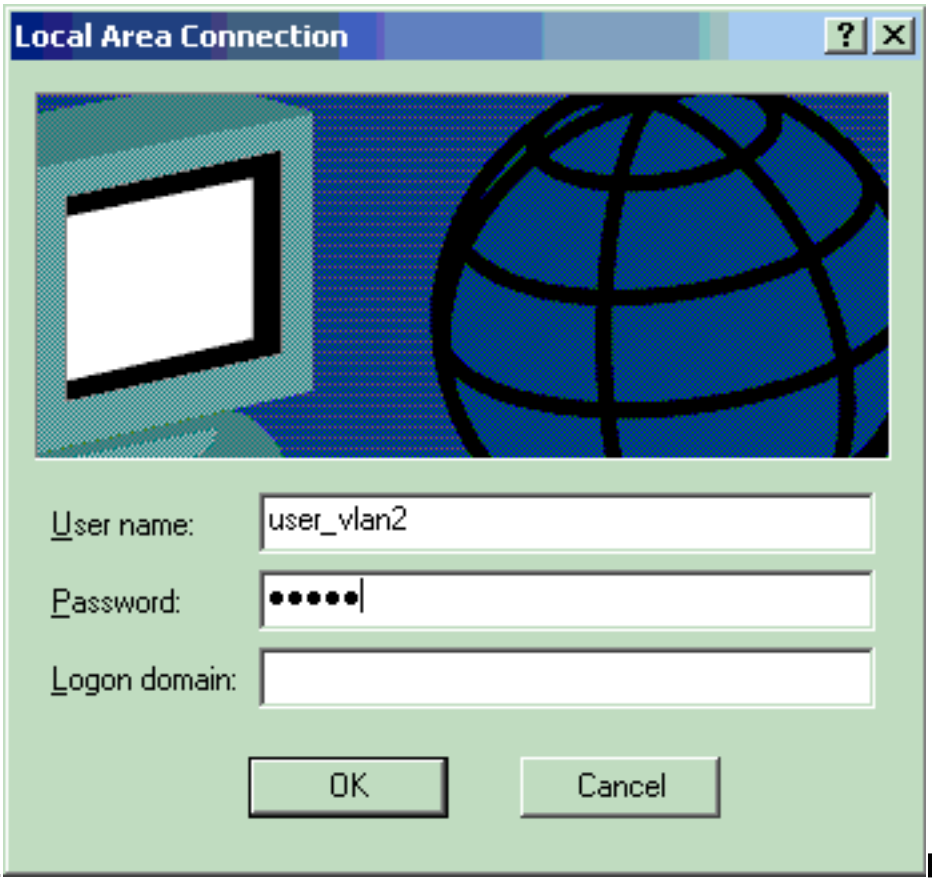
PC-Clients

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

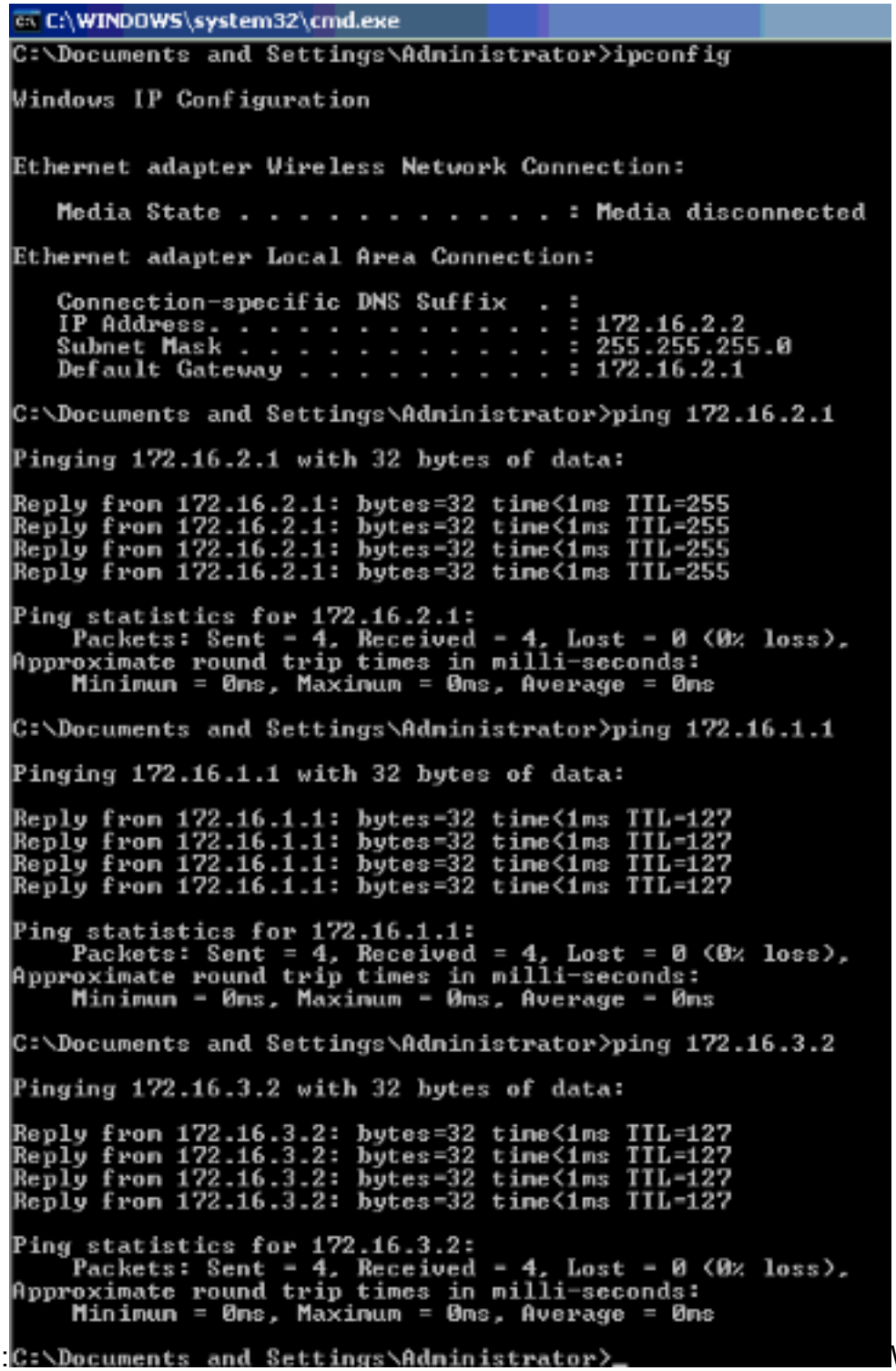
1. Klicken Sie auf die Eingabeaufforderung, die in diesem Beispiel angezeigt

wird: 

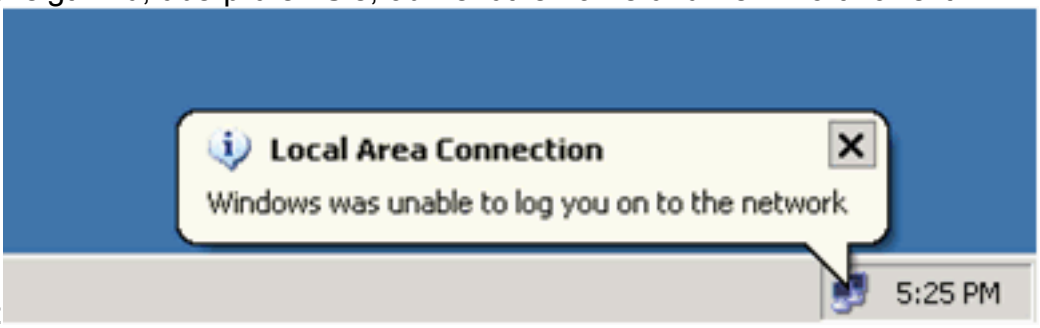
Eine QuickCard mit Benutzername und Kennwort wird angezeigt.

2. Geben Sie den Benutzernamen und das Kennwort ein. 

Hinweis: Geben Sie in PC 1 und 2 die Anmeldeinformationen für VLAN 2-Benutzer ein, und geben Sie in 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 durch **Ping**. Diese Ausgabe stammt von PC 1 und zeigt ein erfolgreiches **Ping** an PC 4



an: Wenn 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 Portstatus, der AUTORISIERT anzeigt.

```
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
```

Überprüfen Sie den VLAN-Status nach erfolgreicher Authentifizierung.

```
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. Überprüfen Sie den DHCP-Bindungsstatus nach erfolgreicher Authentifizierung.

```
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
```

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**.

Fehlerbehebung

Erfassen Sie die Ausgabe dieser **Debugbefehle**, um Fehler zu beheben:

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug dot1x events**: Ermöglicht das Debuggen von Druckanweisungen, die durch das 802.1x-Ereignisflag überwacht werden.

```
Cat6K#debug dot1x events
Dot1x events debugging is on
Cat6K#
!--- Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to
send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
   is FastEthernet3/2
00:13:36: dot1x-ev:MAC Address is 0016.3633.339c
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 6
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 15
00:13:36: dot1x-ev:Found a process thats already handling therequest for
    this id 12
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 6
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:13:36: dot1x-ev:going to send to backend on SP, length = 31
00:13:36: dot1x-ev:Sent to Bend
00:13:36: dot1x-ev:Got a Request from SP to send it to Radius with id 16
00:13:36: dot1x-ev:Found a process thats already handling therequest for
   this id 13
```

```
00:13:36: dot1x-ev:Username is user_vlan2; eap packet length = 32
00:13:36: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:13:36: dot1x-ev:Vlan name = VLAN2
00:13:37: dot1x-ev:Sending Radius SUCCESS to Backend SM -
   id 16 EAP pkt len = 4
00:13:37: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
Cat6K#
```

!--- Debug output for PC 3 connected to Fa3/4. 00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0 00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-ev:The Interface on which we got this AAA**

```
   Request is FastEthernet3/4
00:19:58: dot1x-ev:MAC Address is 0014.5e94.5f99
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 6
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 9
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 10
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 6
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA
00:19:58: dot1x-ev:going to send to backend on SP, length = 31
00:19:58: dot1x-ev:Sent to Bend
00:19:58: dot1x-ev:Got a Request from SP to send it to Radius with id 10
00:19:58: dot1x-ev:Found a process thats already handling therequest
   for this id 11
00:19:58: dot1x-ev:Username is user_vlan3; eap packet length = 32
00:19:58: dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS
00:19:58: dot1x-ev:Vlan name = 3
00:19:58: dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4
00:19:58: dot1x-ev:The process finished processing the request
   will pick up any pending requests from the queue
Cat6K#
```

- **debug radius**: Zeigt Informationen an, die RADIUS zugeordnet sind.

```
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#
```

Zugehörige Informationen

- IEEE 802.1x-Authentifizierung mit Catalyst 6500/6000 mit CatOS-Software - Konfigurationsbeispiel
- Richtlinien für die Bereitstellung von Cisco Secure ACS für Windows NT/2000-Server in einer Cisco Catalyst Switch-Umgebung
- RFC 2868: RADIUS-Attribute für die Unterstützung von Tunnelprotokollen
- Konfigurieren der Port-basierten IEEE 802.1X-Authentifizierung
- LAN-Produktunterstützung
- Unterstützung der LAN Switching-Technologie
- Technischer Support und Dokumentation - Cisco Systems