Konfigurationsbeispiel für die IEEE 802.1x Multi-Domain Authentication auf Cisco Catalyst Layer 3 Fixed Configuration Switches

Inhalt

Einführung

Die Multi-Domain Authentication ermöglicht es einem IP-Telefon und einem PC, sich auf demselben Switch-Port zu authentifizieren, während sie sie in den entsprechenden Sprach- und Daten-VLANs platzieren. In diesem Dokument wird erläutert, wie Sie IEEE 802.1x Multi-Domain Authentication (MDA) auf fest konfigurierten Cisco Catalyst Layer-3-Switches konfigurieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Wie wirkt RADIUS?
- Catalyst Switching- und ACS-Bereitstellungsleitfaden
- Benutzerhandbuch für Cisco Secure Access Control Server 4.1
- Überblick über das Cisco Unified IP-Telefon

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switches der Serie 3560 mit Cisco IOS® Softwareversion 12.2(37)SE1**Hinweis:** Die Unterstützung für die Multi-Domain Authentication ist nur ab Cisco IOS Software Release 12.2(35)SE verfügbar.
- 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.
- Cisco Unified IP-Telefon 7970G mit SCCP-Firmware Version 8.2(1)
- Cisco Unified IP-Telefon 7961G mit SCCP-Firmware Version 8.2(2)
- Media Covergence Server (MCS) mit Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)sr2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Verwandte Produkte

Diese Konfiguration kann auch mit den folgenden Hardware-Komponenten verwendet werden:

- Cisco Catalyst Switches der Serie 3560-E
- Cisco Catalyst Switches der Serie 3750
- Cisco Catalyst Switches der Serie 3750-E

Hinweis: Der Cisco Catalyst Switch der Serie 3550 unterstützt keine 802.1x-Multi-Domain-Authentifizierung.

Konventionen

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

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.

802.1x besteht aus drei Hauptkomponenten. Jede dieser Komponenten wird als "Port Access Entity (PAE)" bezeichnet.

- Supplicant (Komponente): Client-Gerät, das Netzwerkzugriff anfordert, z. B. IP-Telefone und angeschlossene PCs
- Authenticator - Netzwerkgerät, das die Autorisierungsanfragen für Komponenten vereinfacht, z. B. Cisco Catalyst 3560
- Authentifizierungsserver - Ein RADIUS (Remote Authentication Dial-in User Server), der den Authentifizierungsdienst bereitstellt, z. B. Cisco Secure Access Control Server

Die Cisco Unified IP-Telefone enthalten außerdem eine 802.1X-Komponente. Mit dieser Komponente können Netzwerkadministratoren die Verbindung von IP-Telefonen mit den LAN-Switch-Ports steuern. Die erste Version der 802.1X-Komponente des IP-Telefons implementiert die EAP-MD5-Option für die 802.1X-Authentifizierung. Bei einer Konfiguration mit mehreren Domänen müssen das IP-Telefon und der angeschlossene PC unabhängig den Zugriff auf das Netzwerk anfordern, indem ein Benutzername und ein Kennwort festgelegt werden. Das Authentifizierungsgerät kann Informationen von den RADIUS-Attributen verlangen. Attribute geben zusätzliche Autorisierungsinformationen an, z. B. ob der Zugriff auf ein bestimmtes VLAN für einen Supplicant zulässig ist. Diese Attribute können anbieterspezifisch sein. Cisco verwendet das RADIUS-Attribut `cisco-av-pair`, um dem Authentifizierer (Cisco Catalyst 3560) mitzuteilen, dass ein Supplicant (IP Phone) für das Sprach-VLAN zugelassen ist.

Konfiguration

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen 802.1x-Multi-Domain-Authentifizierungsfunktion.

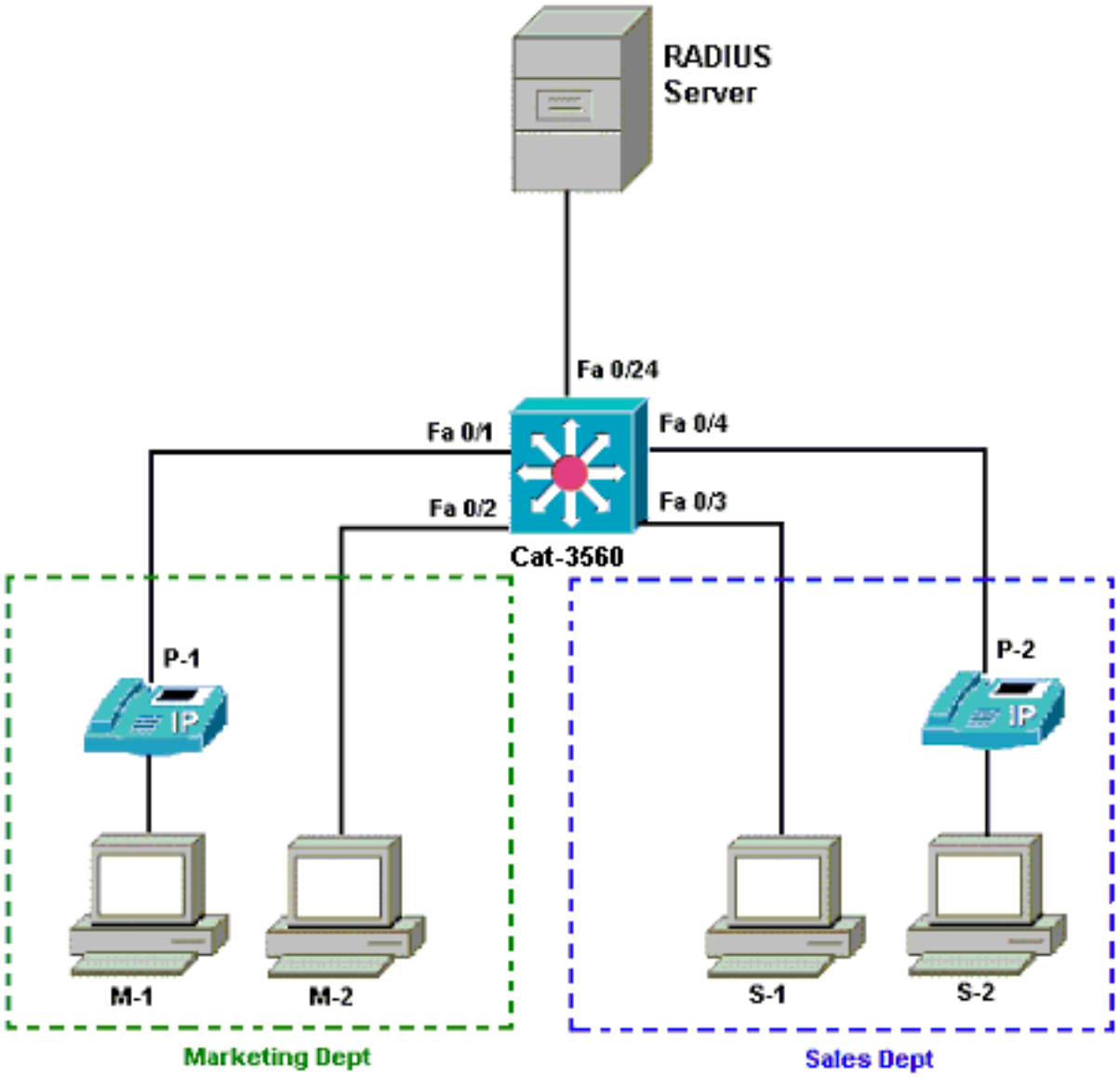
Für diese Konfiguration sind folgende Schritte erforderlich:

- Konfigurieren Sie den Catalyst Switch für die 802.1x-Multi-Domain-Authentifizierung.
- Konfigurieren Sie den RADIUS-Server.
- Konfigurieren der PC-Clients für die Verwendung der 802.1x-Authentifizierung.
- Konfigurieren Sie die IP-Telefone für die Verwendung der 802.1x-Authentifizierung.

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

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



- RADIUS server (RADIUS-Server): Dieser Server führt die eigentliche Authentifizierung des Clients aus. 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 Cisco ACS auf einem Media Covergence Server (MCS) für die Authentifizierung und VLAN-Zuweisung installiert und konfiguriert. Der MCS ist außerdem der TFTP-Server und der Cisco Unified Communications Manager (Cisco CallManager) für die IP-Telefone.
- Switch - Dieser Befehl 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 3560-Switch 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. Hierzu wird die authentifizierte Benutzeridentität dem DHCP-Erkennungsprozess hinzugefügt. Die Ports FastEthernet 0/1 und 0/4 sind die einzigen für die 802.1x-Multi-Domain-Authentifizierung konfigurierten Ports. Die Ports FastEthernet 0/2 und 0/3 befinden sich im standardmäßigen 802.1x-Einzelhost-Modus. Port FastEthernet 0/24 wird mit dem RADIUS-Server verbunden.**Hinweis:** Wenn Sie einen externen DHCP-Server verwenden, vergessen Sie nicht, den Befehl **ip helper-address** auf der SVI (VLAN)-Schnittstelle

hinzuzufügen, in der sich der Client befindet, der auf den DHCP-Server zeigt.

- Clients - Dies sind Geräte, z. B. IP-Telefone oder Workstations, die den Zugriff auf das LAN und die Switch-Services anfordern und auf Anfragen vom Switch reagieren. Hier werden Clients konfiguriert, um die IP-Adresse von einem DHCP-Server zu erhalten. Die Geräte M-1, M-2, S-1 und S-2 sind Workstation-Clients, die Zugriff auf das Netzwerk anfordern. P-1 und P-2 sind die IP-Telefon-Clients, die Zugriff auf das Netzwerk anfordern. M-1, M-2 und P-1 sind Client-Geräte in der Marketingabteilung. S-1, S-2 und P-2 sind Client-Geräte in der Vertriebsabteilung. Die IP-Telefone P-1 und P-2 sind für dasselbe Sprach-VLAN (VLAN 3) konfiguriert. Die Workstations M-1 und M-2 werden nach erfolgreicher Authentifizierung so konfiguriert, dass sie sich im selben Daten-VLAN (VLAN 4) befinden. Nach erfolgreicher Authentifizierung sind die Workstations S-1 und S-2 ebenfalls so konfiguriert, dass sie sich im selben Daten-VLAN (VLAN 5) befinden.**Hinweis:** Sie können die dynamische VLAN-Zuweisung von einem RADIUS-Server nur für die Datengeräte verwenden.

Konfigurieren des Catalyst Switches für die 802.1x-Multi-Domain-Authentifizierung

Diese Switch-Beispielkonfiguration umfasst:

- Aktivieren der 802.1x-Multi-Domain-Authentifizierung an den Switch-Ports
- Konfiguration des RADIUS-Servers
- DHCP-Serverkonfiguration für IP-Adresszuweisung
- Inter-VLAN-Routing für Verbindungen zwischen Clients nach Authentifizierung

Unter Verwenden der Multidomain-Authentifizierung finden Sie weitere Informationen zu den Richtlinien zum Konfigurieren von MDA.

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

Hinweis: Hier wird nur die entsprechende Konfiguration angezeigt.

Cat. 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
```

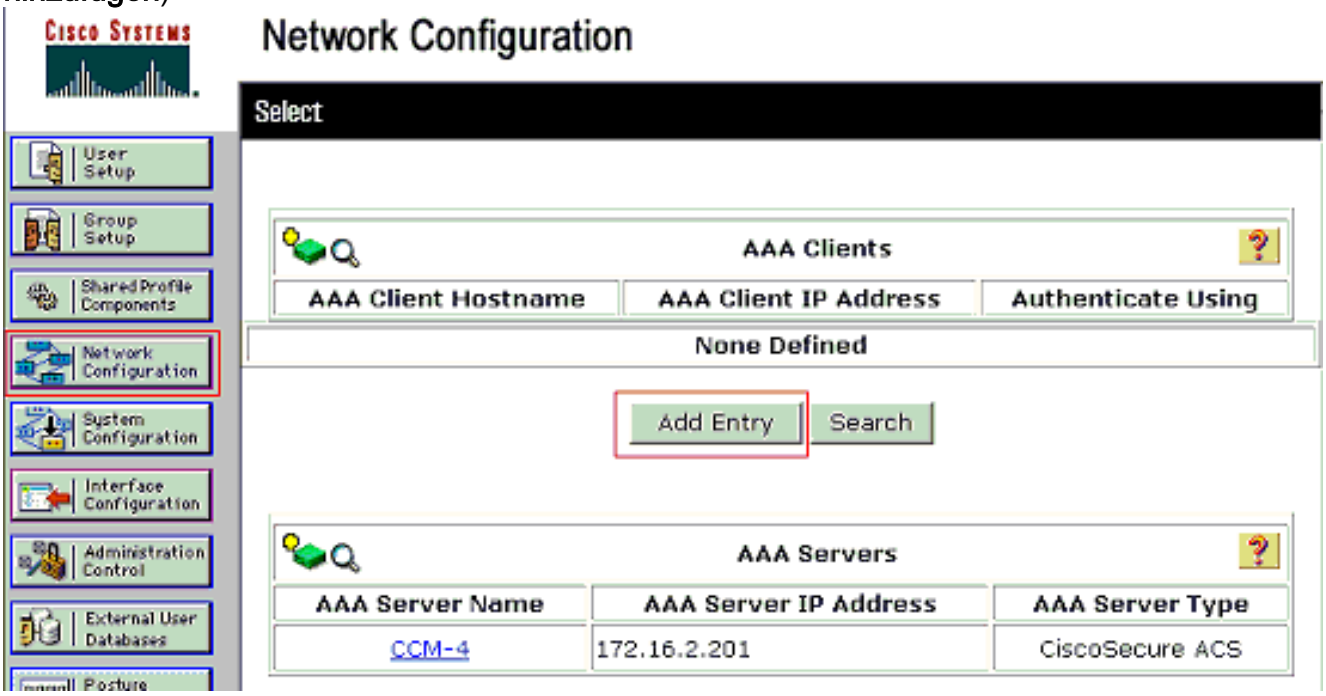
```
!--- This pool assigns ip address for IP Phones. !---
Option 150 is for the TFTP server. Cat-3560(dhcp-
config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
!--- This pool assigns ip address for PC clients in
Marketing 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
```

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

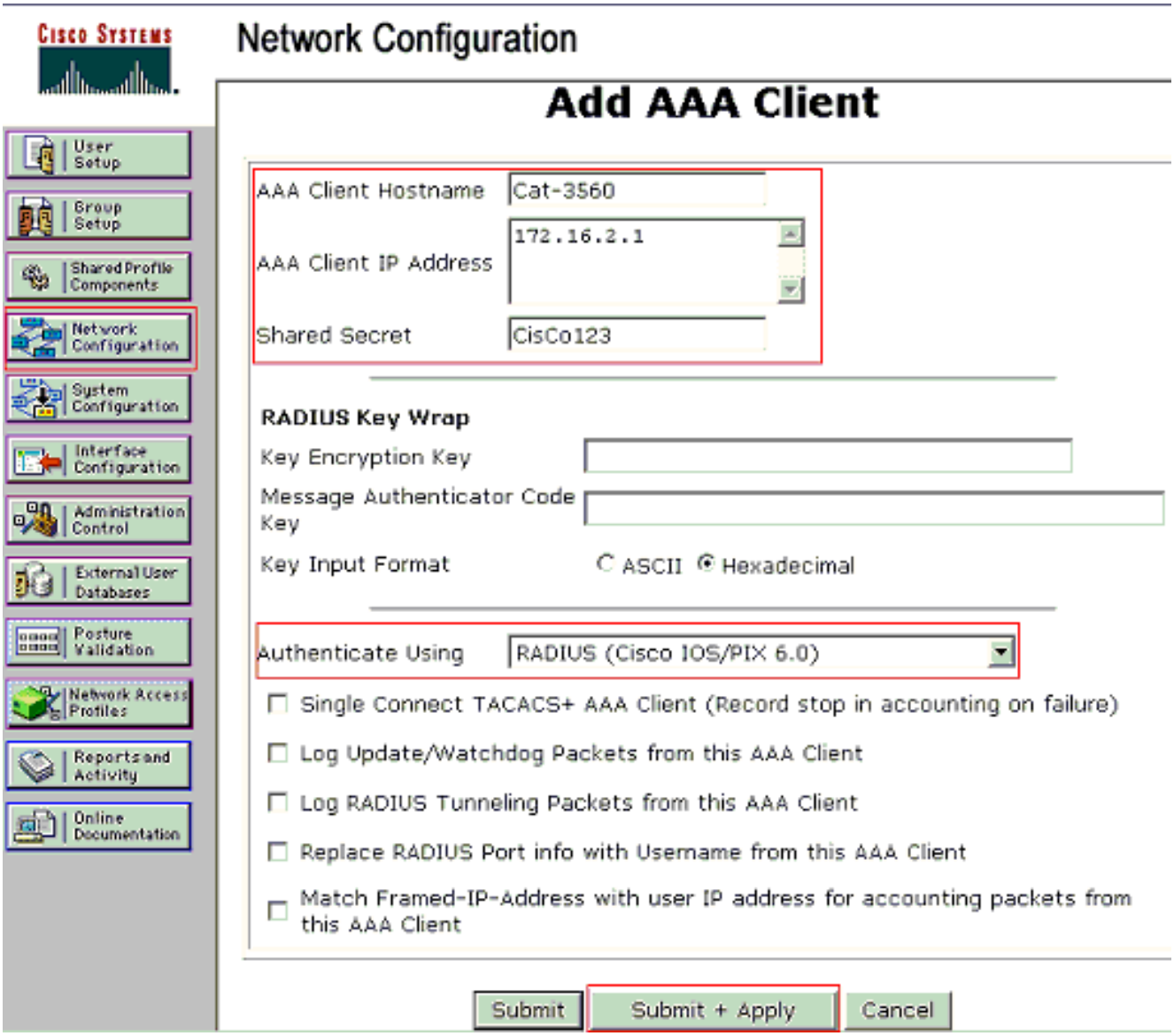
Konfigurieren des RADIUS-Servers

Der RADIUS-Server ist mit der statischen IP-Adresse 172.16.2.201/24 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 (**Cat-3560**).IP-Adresse des AAA-Clients = IP-Adresse der Verwaltungsschnittstelle des Switches (**172.16.2.1**).Shared Secret = auf dem Switch konfigurierter RADIUS-Schlüssel (**CisCo123**).**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.Authentifizierung mit = **RADIUS (Cisco IOS/PIX 6.0)**.**Hinweis:** Cisco Attribute-Value (AV) pair-Attribut ist unter dieser Option verfügbar.
4. Klicken Sie auf **Senden + Übernehmen**, um diese Änderungen wirksam zu machen, wie im folgenden Beispiel
   gezeigt:



Gruppeneinrichtung

In dieser Tabelle finden Sie Informationen zum Konfigurieren des RADIUS-Servers für die Authentifizierung.

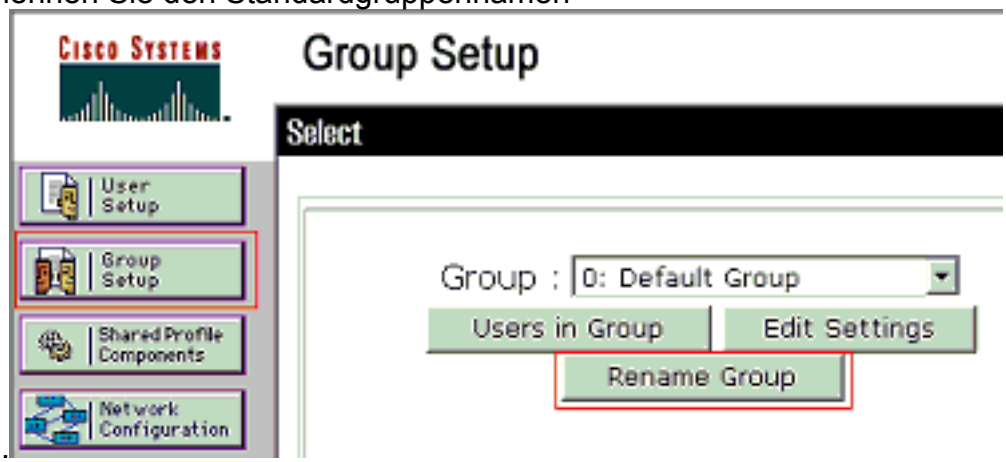
"Slot0:"	Abb.	Gruppe	Benutzer	Kennwort	VLAN	DHCP-Pool
M-1	Marketing	Marketing	mkt-manager	Cisco	MARKETING	Marketing
M-2	Marketing	Marketing	mkt-personal	Cisco	MARKETING	Marketing
S-2	Vertrieb	Vertrieb	Vertriebsleiter	Cisco	VERTRIEB	Vertrieb
S-1	Vertrie	Vertrie	Verkau	Cisco	VERT	Vert

	b	b	fspersonal		RIEB	rieb
P-1	Marketing	IP-Telefone	CP-7970G-SEP001759E7492C	P1cisco	SPRACHE	IP-Telefone
P-2	Vertrieb	IP-Telefone	CP-7961G-SEP001A2F80381F	P2cisco	SPRACHE	IP-Telefone

Erstellen Sie Gruppen für Clients, die mit VLANs 3 (VOICE), 4 (MARKETING) und 5 (VERTRIEB) verbunden sind. Hier werden Gruppen **IP-Telefone**, **Marketing** und **Vertrieb** erstellt.

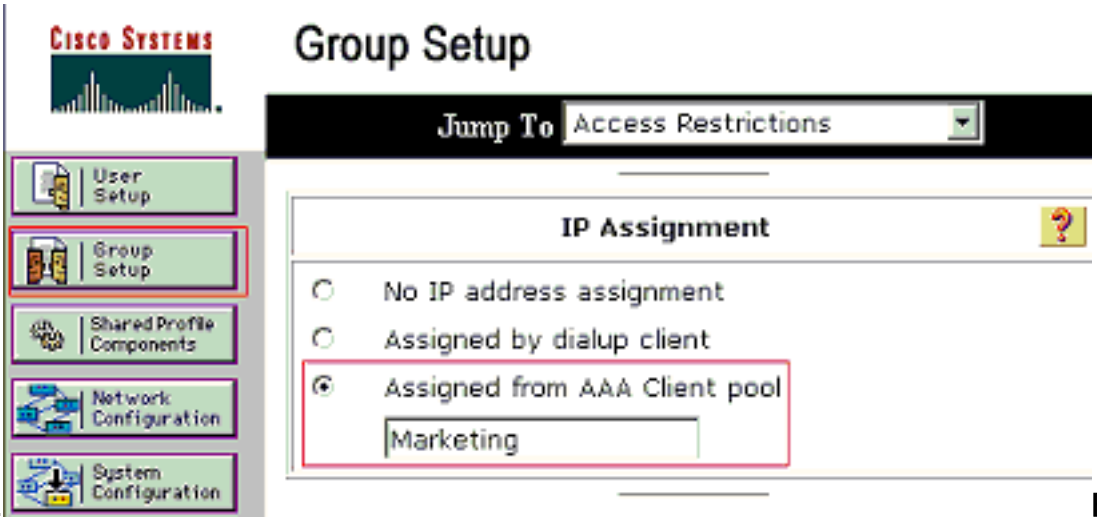
Hinweis: Dies ist die Konfiguration der Gruppen **Marketing** und **IP-Telefone**. Führen Sie für die **Sales**-Gruppenkonfiguration die Schritte für die **Marketing-**Gruppe aus.

1. Um eine Gruppe zu erstellen, wählen Sie **Group Setup (Gruppeneinrichtung) aus,** und benennen Sie den Standardgruppennamen um.



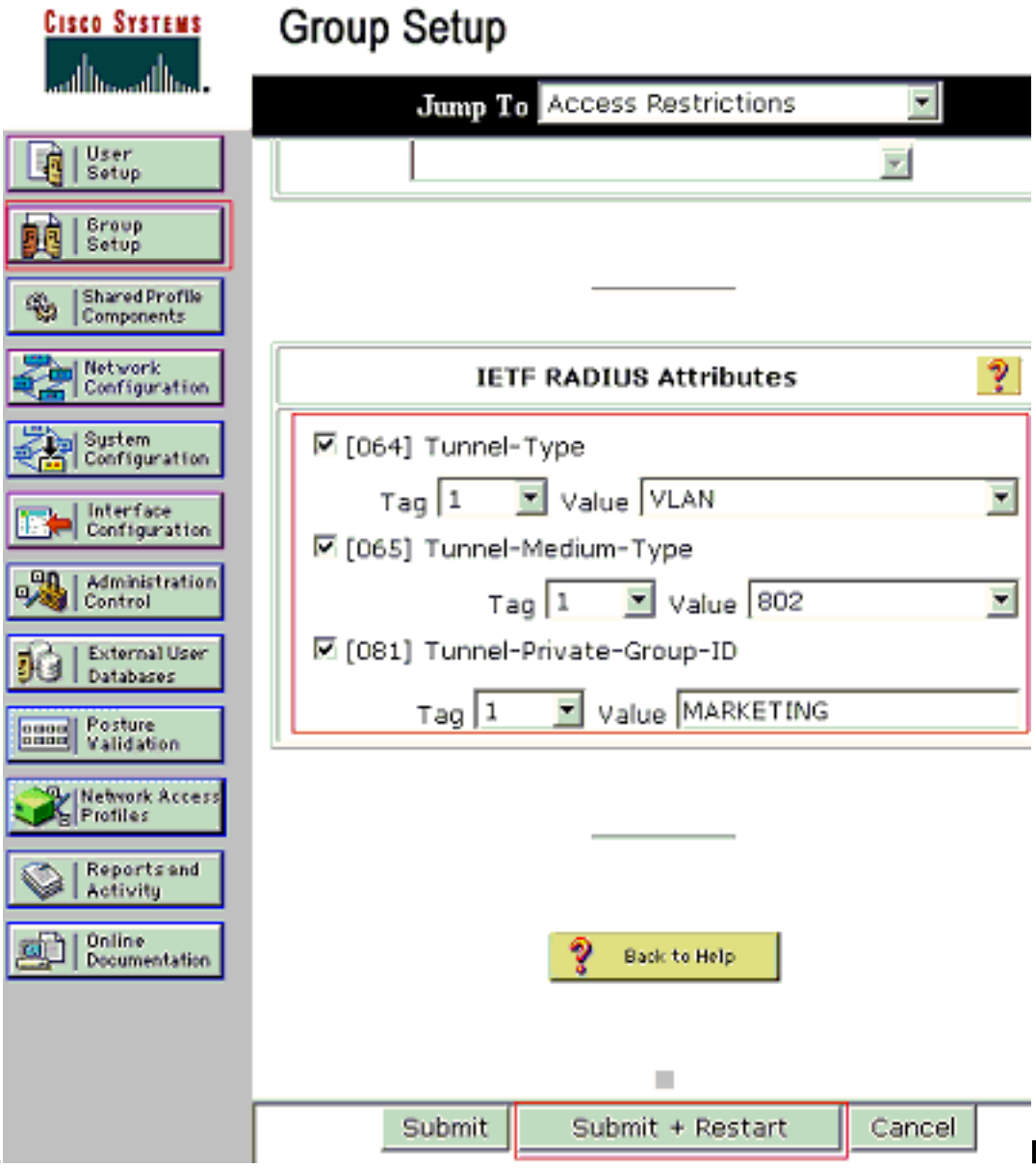
2. Um eine Gruppe zu konfigurieren, wählen Sie die Gruppe aus der Liste aus, und klicken Sie auf **Einstellungen bearbeiten.**

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



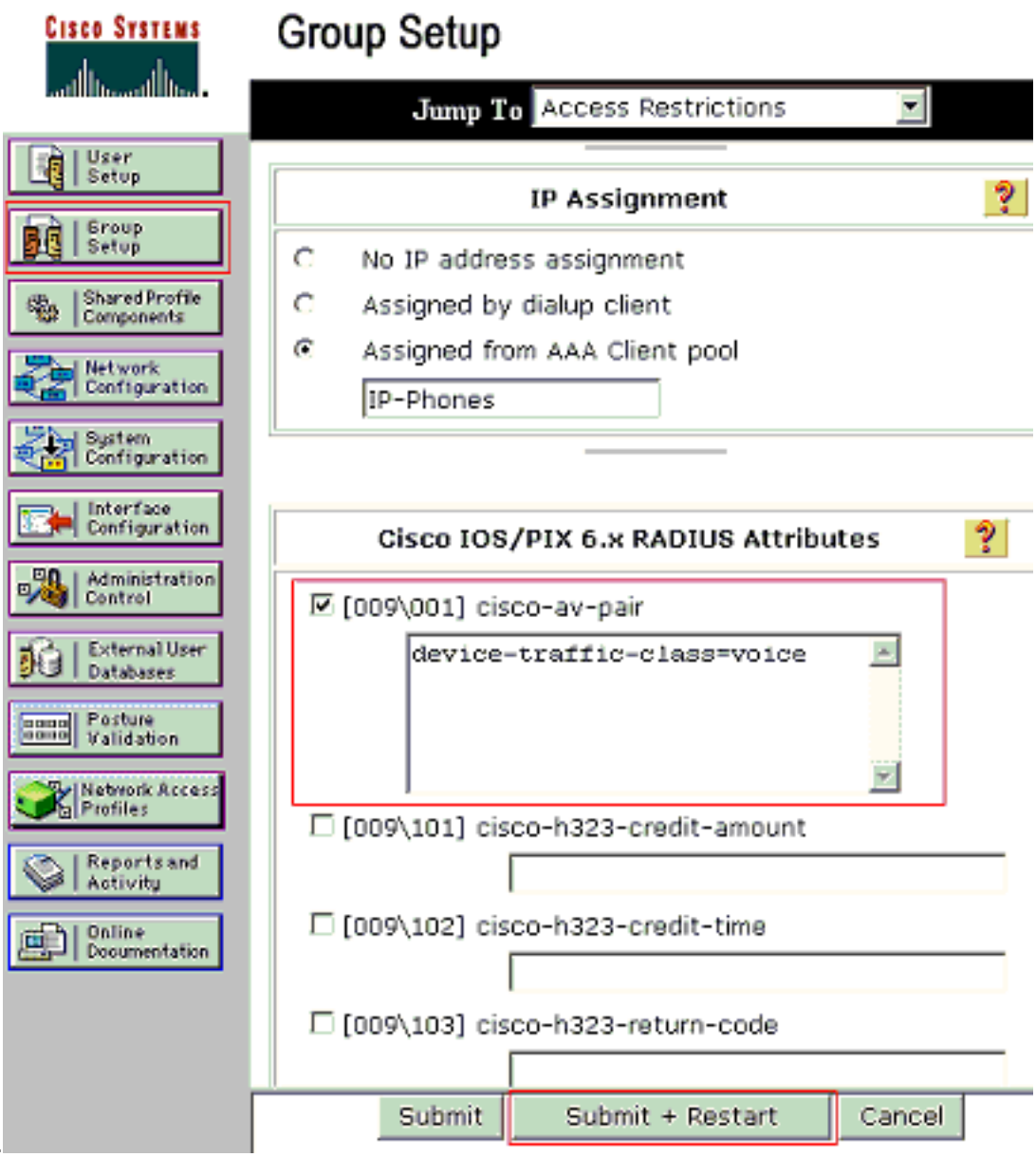
ein.**Hinweis:** Wählen Sie diese Option aus, und geben Sie den Namen des AAA-Client-IP-Pools in das Feld ein, nur wenn diesem Benutzer die IP-Adresse zugewiesen werden soll, die von einem IP-Adresspool auf dem AAA-Client konfiguriert wurde.**Hinweis:** Bei Gruppenkonfiguration von **IP-Telefonen** überspringen Sie den nächsten Schritt, Schritt 4, und fahren Sie mit Schritt 5 fort.

4. Definieren Sie die IETF-Attribute (Internet Engineering Task Force) **64**, **65** und **81** und klicken Sie dann auf **Senden + Neu starten**.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:** 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. 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, wird der Client dem Zugriffs-VLAN des Ports zugewiesen. Wenn Sie das Attribut **81** für die dynamische VLAN-Zuweisung definiert haben und der Port ein Switch-Port im Zugriffsmodus ist, müssen Sie auf dem Switch den Befehl **a** für den **standardmäßigen Gruppenradius** des Autorisierungsnetzwerks 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.**Hinweis:** Der nächste Schritt gilt nur für die Gruppe **IP-Telefone**.

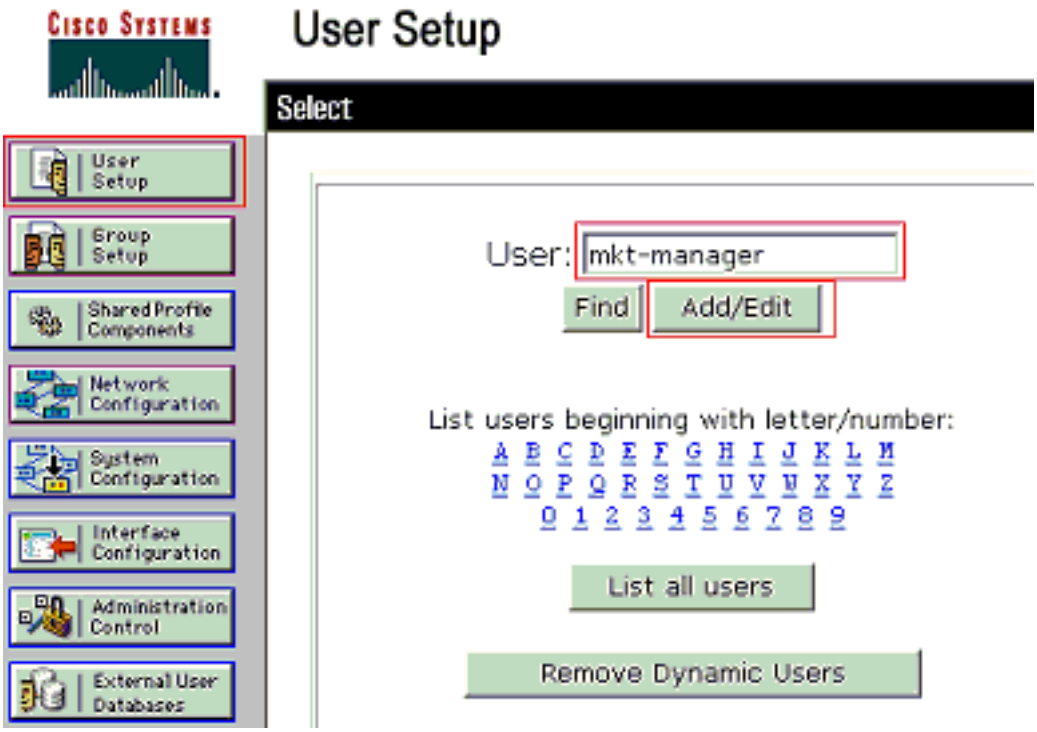
5. Konfigurieren Sie den RADIUS-Server so, dass er ein Cisco Attribute-Value (AV)-Paar-Attribut sendet, um ein Sprachgerät zu autorisieren. Andernfalls behandelt der Switch das Sprachgerät als Datengerät. Definieren Sie ein Cisco Attribute-Value (AV)-Paarattribut mit dem Wert *device-traffic-class=voice* und klicken Sie auf **Senden + Neu**

starten. 

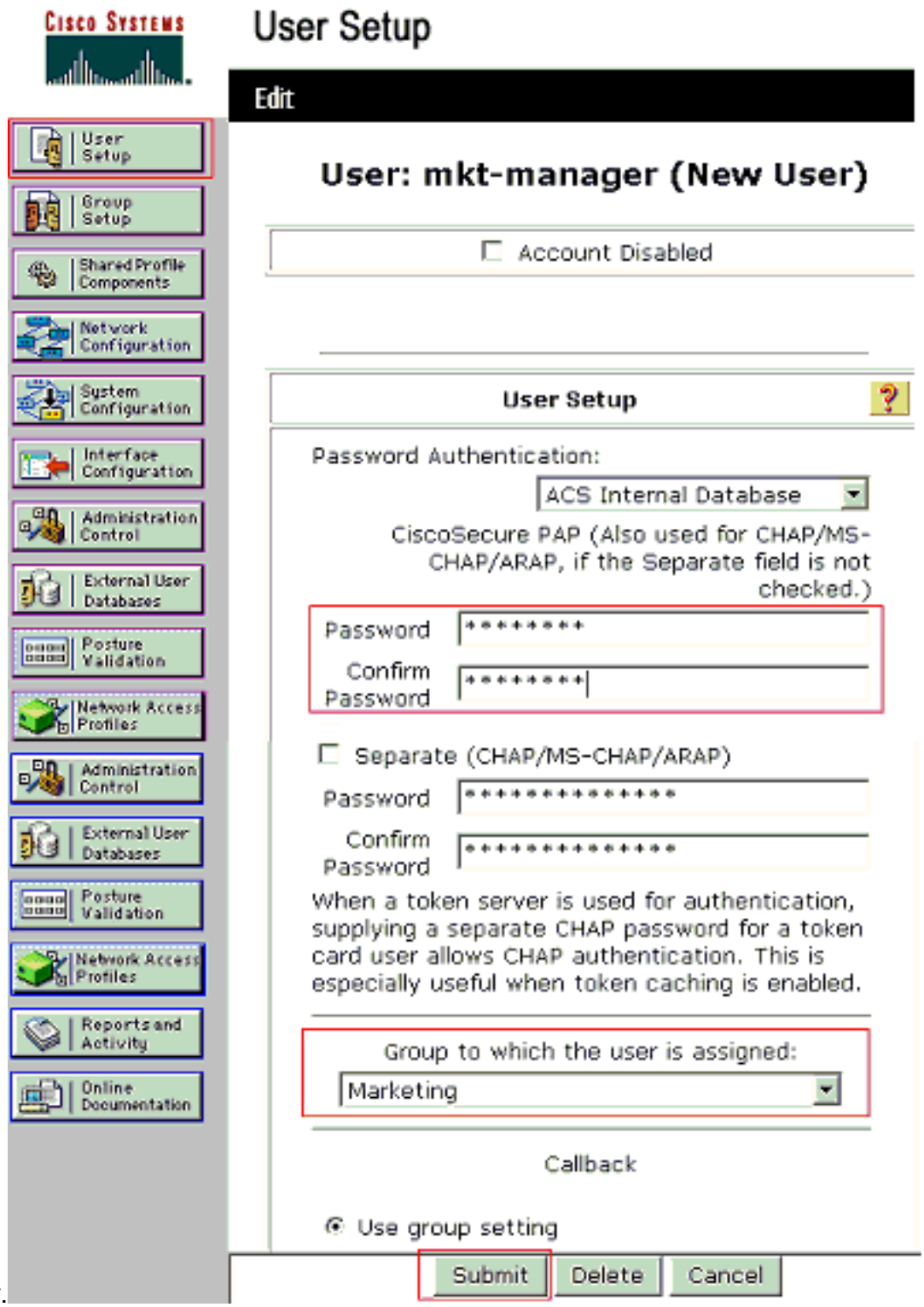
Benutzereinrichtung

Führen Sie diese Schritte aus, um einen Benutzer hinzuzufügen und zu konfigurieren.

1. Um Benutzer hinzuzufügen und zu konfigurieren, wählen Sie **User Setup (Benutzereinrichtung)**. Geben Sie den Benutzernamen ein, und klicken Sie auf **Hinzufügen/Bearbeiten.**

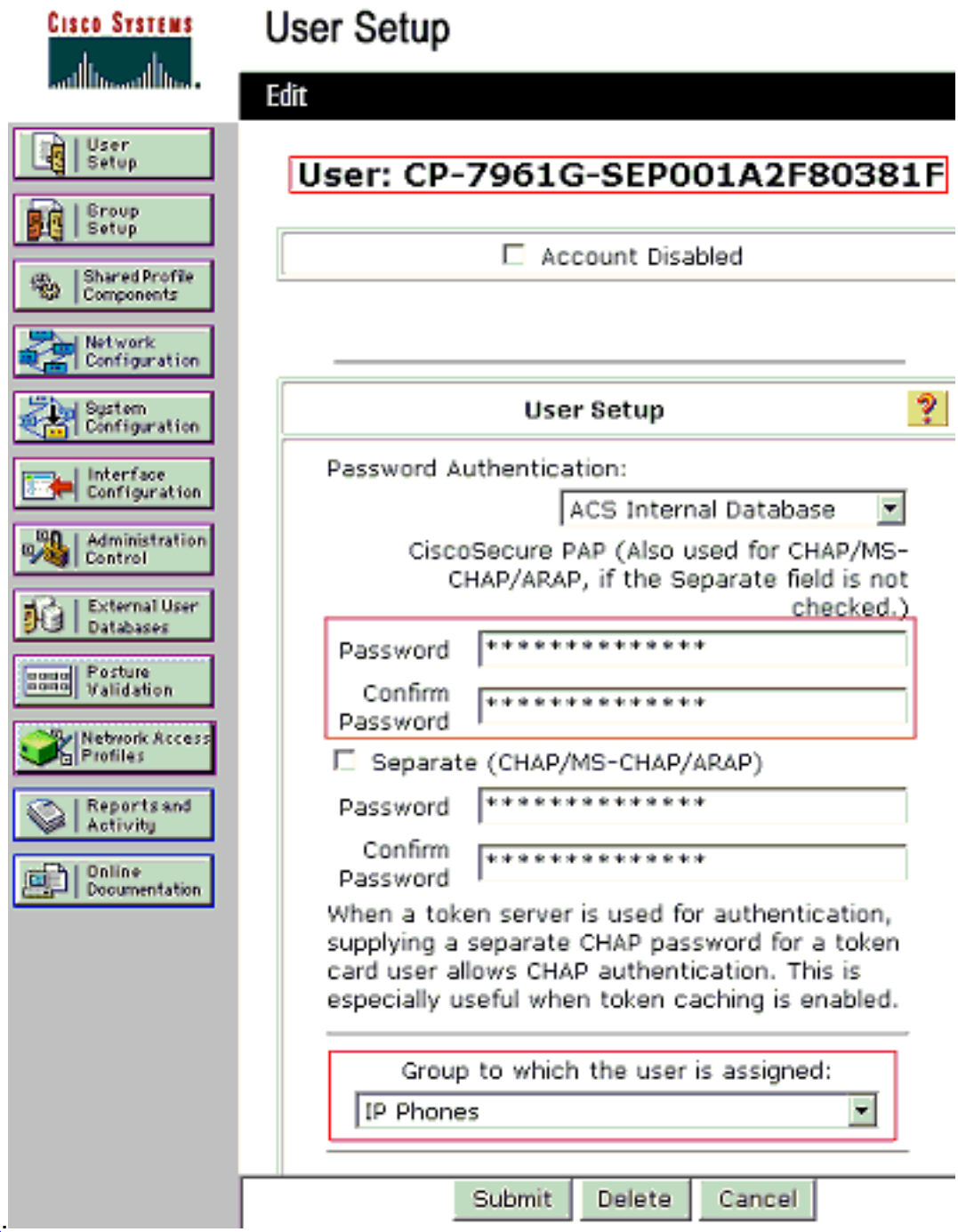


2. Definieren Sie den Benutzernamen, das Kennwort und die Gruppe für den



Benutzer.

3. Das IP-Telefon verwendet seine Geräte-ID als Benutzernamen und den geheimen Schlüssel als Kennwort für die Authentifizierung. Diese Werte müssen auf dem RADIUS-Server übereinstimmen. Erstellen Sie für die IP-Telefone P-1 und P-2 Benutzernamen, die mit ihrer Geräte-ID und dem Kennwort identisch sind, die mit dem konfigurierten gemeinsamen geheimen Schlüssel übereinstimmen. Weitere Informationen zur Geräte-ID und zum Shared Secret auf einem IP-Telefon finden Sie im Abschnitt [Konfigurieren der IP-Telefone für die Verwendung der 802.1x-]



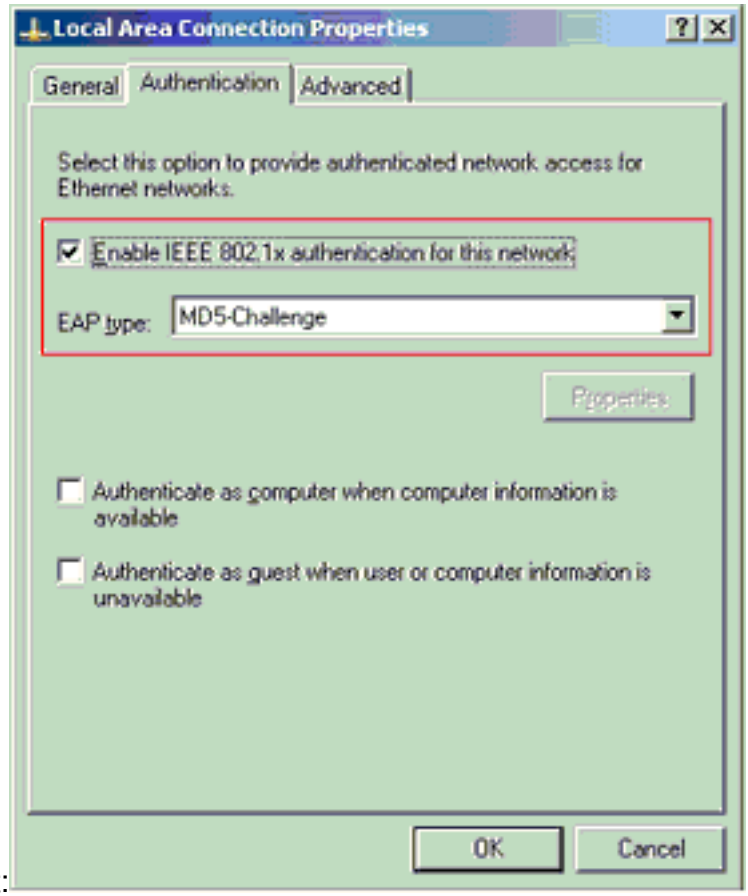
Authentifizierung.

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

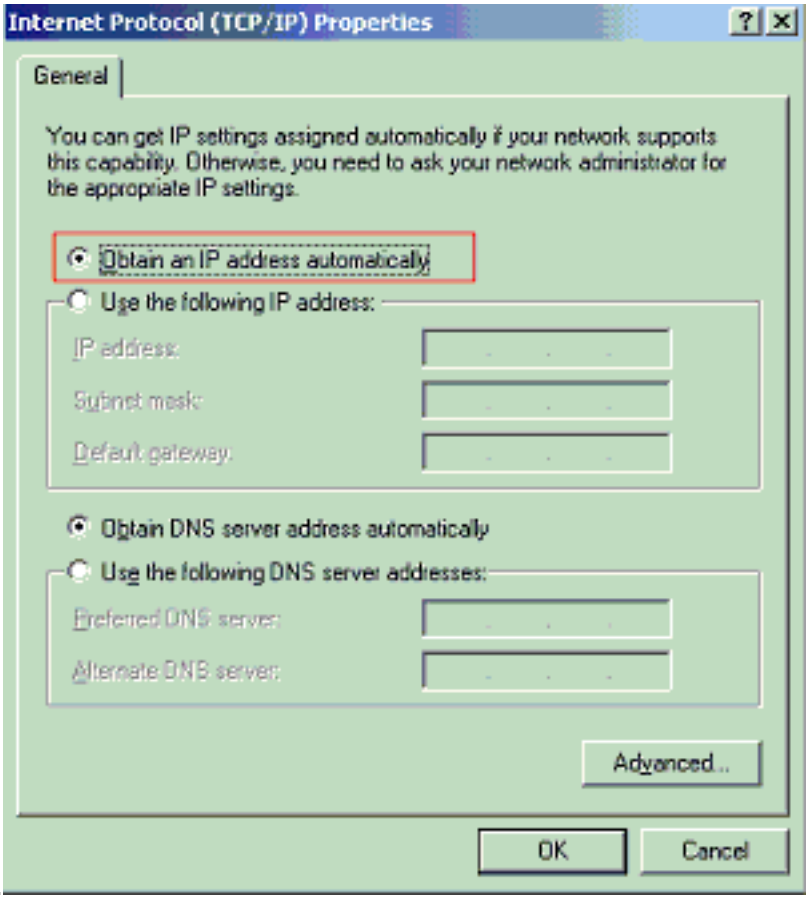
gezeigt:



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.



Konfigurieren der 802.1x-Authentifizierung für die IP-Telefone

Führen Sie diese Schritte aus, um die IP-Telefone für die 802.1x-Authentifizierung zu konfigurieren.

1. Drücken Sie die **Einstellungstaste**, um auf die **802.1X-Authentifizierungseinstellungen** zuzugreifen, und wählen Sie **Sicherheitskonfiguration > 802.1X-Authentifizierung > Geräteauthentifizierung aus**.
2. Legen Sie die Option **Geräteauthentifizierung** auf **Aktiviert fest**.
3. Drücken Sie die programmierbare Taste **Speichern**.
4. Wählen Sie **802.1X Authentication > EAP-MD5 > Shared Secret (802.1X-Authentifizierung > EAP-MD5 > Shared Secret** (Gemeinsamer geheimer Schlüssel), um ein Kennwort für das Telefon festzulegen.
5. Geben Sie den freigegebenen geheimen Schlüssel ein, und drücken Sie **Save (Speichern)**.**Hinweis:** Das Kennwort muss zwischen sechs und 32 Zeichen lang sein und aus einer beliebigen Kombination von Zahlen oder Buchstaben bestehen. `Dieser Schlüssel ist nicht aktiv, wenn` eine Nachricht angezeigt wird und das Kennwort nicht gespeichert wird, wenn diese Bedingung nicht erfüllt ist.**Hinweis:** Wenn Sie die 802.1X-Authentifizierung deaktivieren oder auf dem Telefon ein Zurücksetzen auf die Werkseinstellungen vornehmen, wird der zuvor konfigurierte, freigegebene MD5-geheime Schlüssel gelöscht.**Hinweis:** Die anderen Optionen, Geräte-ID und Bereich, können nicht konfiguriert werden. Die Geräte-ID wird als Benutzername für die 802.1x-Authentifizierung verwendet. Es handelt sich um eine Ableitung der Modellnummer und der eindeutigen MAC-Adresse des Telefons, die in diesem Format angezeigt wird: CP-<model>-SEP-<MAC>. Beispielsweise **CP-7970G-SEP001759E7492C**. Weitere Informationen finden Sie unter 802.1X-Authentifizierungseinstellungen.

Führen Sie diese Schritte aus, um das IP-Telefon so zu konfigurieren, dass es die IP-Adresse von einem DHCP-Server bezieht.

1. Drücken Sie die **Einstellungstaste**, um auf die **Netzwerkkonfigurationseinstellungen** zuzugreifen, und wählen Sie **Netzwerkkonfiguration aus**.
2. Entsperren Sie die **Netzwerkkonfigurationsoptionen**. Drücken Sie zum Entsperren die Taste **#.**Hinweis:** Drücken Sie nicht **#**, um die Optionen zu entsperren, und drücken Sie sofort **# erneut, um die Optionen zu sperren. Das Telefon interpretiert diese Sequenz als **#**, die das Telefon zurücksetzt. Um Optionen nach dem Entsperren zu sperren, warten Sie mindestens 10 Sekunden, bevor Sie **# erneut drücken.
3. Navigieren Sie zur Option DHCP Enabled (DHCP aktiviert), und drücken Sie die programmierbare Taste **Yes (Ja)**, um DHCP zu aktivieren.
4. Drücken Sie die programmierbare Taste **Speichern**.

Überprüfung

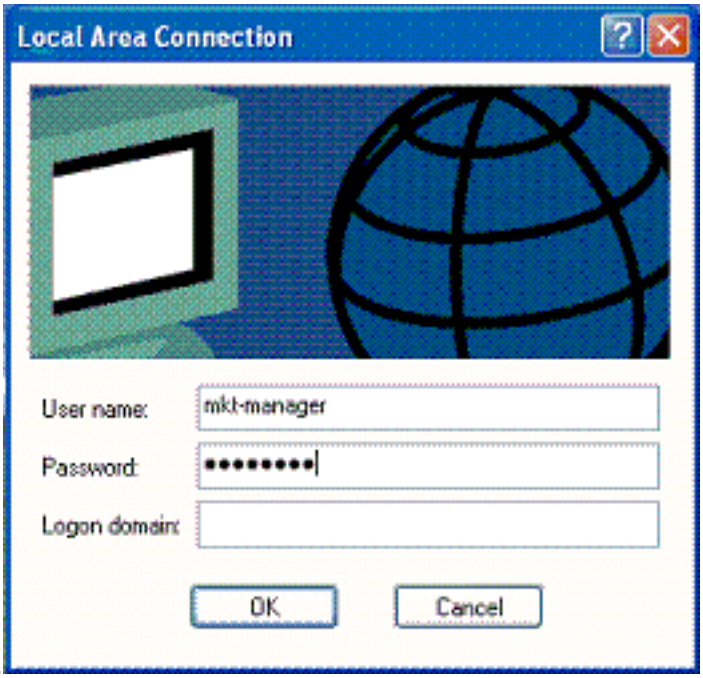
In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

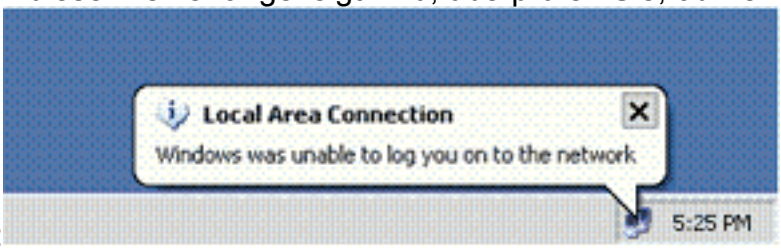
PC-Clients

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.**Hinweis:** MDA erzwingt nicht die Reihenfolge der Geräteauthentifizierung. Für optimale Ergebnisse empfiehlt Cisco jedoch, dass ein Sprachgerät authentifiziert wird, bevor ein Datengerät an einem MDA-fähigen Port angeschlossen wird.
2. Geben Sie den Benutzernamen und das Kennwort

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**.**Hinweis:** Wenn dieser Fehler angezeigt wird, überprüfen Sie, ob Benutzername und Kennwort korrekt sind: 

IP-Telefone

Über das Menü "802.1X Authentication Status" (Authentifizierungsstatus) der IP-Telefone kann der Authentifizierungsstatus überwacht werden.

1. Drücken Sie die **Einstellungstaste**, um auf die 802.1X-Authentifizierungs-Echtzeit-Statistiken zuzugreifen, und wählen Sie **Sicherheitskonfiguration > 802.1X-Authentifizierungsstatus aus**.
2. Der **Transaktionsstatus** sollte **authentifiziert** werden. Weitere Informationen finden Sie unter Echtzeit-Status der 802.1X-Authentifizierung.**Hinweis:** Der Authentifizierungsstatus kann auch unter **Einstellungen > Status > Statusmeldungen** überprüft werden.

Layer-3-Switch

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.

```
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
```

Überprüfen Sie den VLAN-Status nach erfolgreicher Authentifizierung.

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

```
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
```

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

IP-Telefon-Authentifizierung fehlgeschlagen

Der Status des IP-Telefons zeigt die `Konfiguration der IP` oder die `Registrierung` an, wenn die 802.1x-Authentifizierung fehlschlägt. Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Bestätigen Sie, dass 802.1x auf dem IP-Telefon aktiviert ist.
- Stellen Sie sicher, dass die Geräte-ID als Benutzername auf dem Authentifizierungsserver (RADIUS) eingegeben ist.
- Bestätigen Sie, dass der gemeinsame geheime Schlüssel auf dem IP-Telefon konfiguriert ist.
- Wenn der gemeinsame geheime Schlüssel konfiguriert ist, stellen Sie sicher, dass auf dem Authentifizierungsserver derselbe geheime Schlüssel eingegeben ist.
- Überprüfen Sie, ob Sie die anderen erforderlichen Geräte, z. B. den Switch und den Authentifizierungsserver, ordnungsgemäß konfiguriert haben.

Zugehörige Informationen

- Konfigurieren der Port-basierten IEEE 802.1x-Authentifizierung
- Konfigurieren des IP-Telefons für die 802.1x-Authentifizierung
- 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
- IEEE 802.1x-Authentifizierung mit Catalyst 6500/6000 mit Ausführung der Cisco IOS Software - Konfigurationsbeispiel
- IEEE 802.1x-Authentifizierung mit Catalyst 6500/6000 mit CatOS-Software - Konfigurationsbeispiel
- Support-Seiten für LAN-Produkte
- Support-Seite zum Thema LAN-Switching
- Technischer Support und Dokumentation für Cisco Systeme