

Konfigurationsbeispiel für VLANs auf Aironet Access Points

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Netzwerkdiagramm](#)

[Konfigurieren](#)

[Konfigurieren des nativen VLANs auf dem WAP](#)

[Konfigurieren von VLANs für Gastbenutzer und Admin-Benutzer am WAP](#)

[Konfigurieren des Catalyst Switches](#)

[Konfigurieren des Routers](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Fehlerbehebungsverfahren](#)

[Befehle zur Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel, das zeigt, wie VLANs auf Cisco Aironet Access Points (APs) mithilfe der Kommandozeile (CLI) konfiguriert werden.

Voraussetzungen

Anforderungen

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

- Kenntnis der grundlegenden Konfiguration von Aironet APs
- Kenntnis der Konfiguration des Aironet 802.11a/b/g Client-Adapters mit dem Aironet Desktop-Utility
- Grundkenntnisse der Konfiguration von Cisco Catalyst Switches und Cisco Routern

Verwendete Komponenten

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

- Aironet AP der Serie 1240AG mit Cisco IOS[®] Softwareversion 12.4(3g)JA1
- Aironet 802.11a/b/g Client-Adapter
- Aironet Desktop-Dienstprogramm, das Firmware Version 2.5 ausführt
- Catalyst 2950-Switch mit Cisco IOS-Software, Version 12.1(19)EA1
- 2800 ISR-Router mit Cisco IOS Software, Version 12.4(11)T

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.

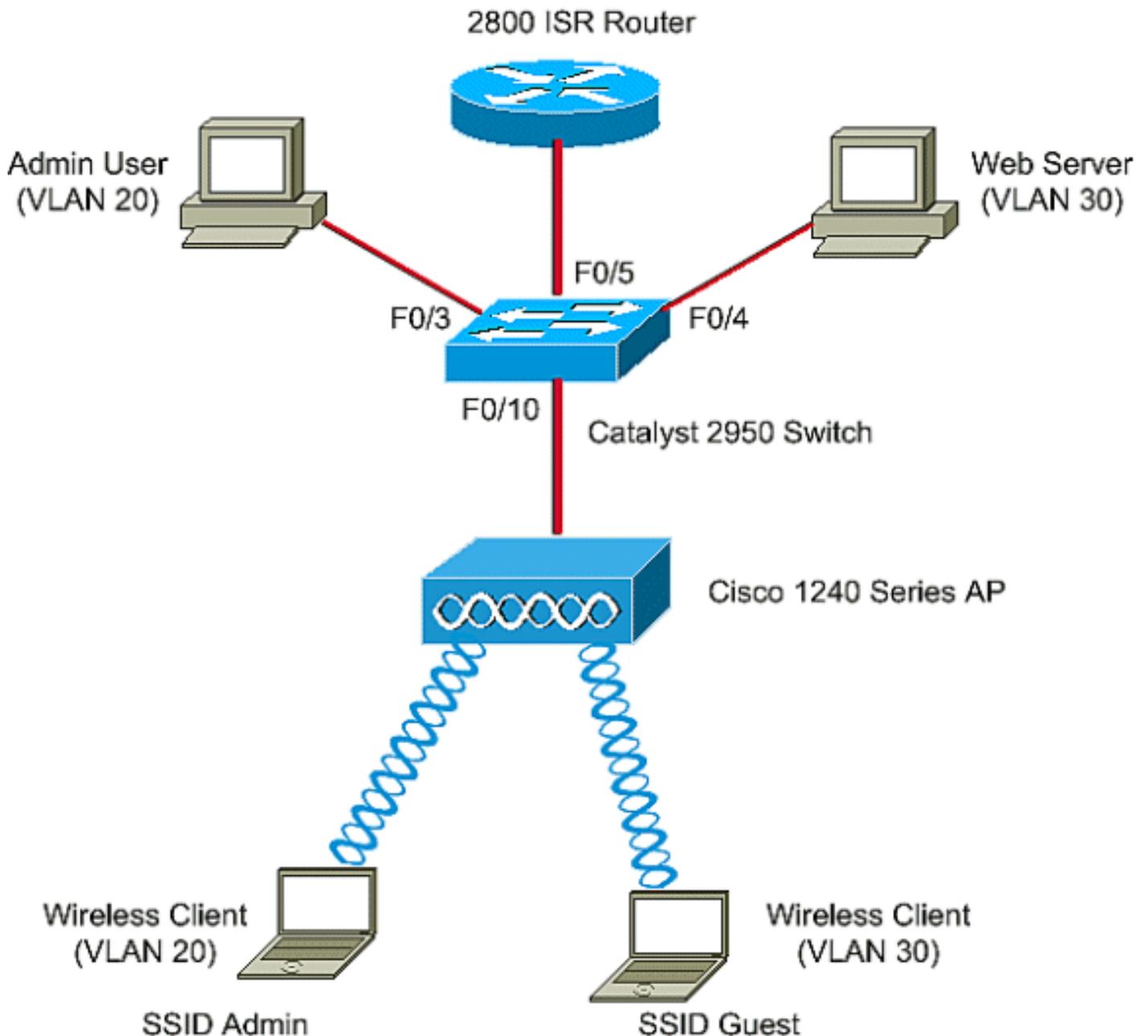
Konventionen

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

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.

Ein AP der Serie Aironet 1200 verfügt über drei VLANs: VLAN 2, VLAN 20 und VLAN 30. Die Konfiguration in diesem Dokument verwendet VLAN 2 als natives VLAN, VLAN 20 für die Administration (Admin) und VLAN 30 für Gastbenutzer. Wireless-Benutzer, die der Admin-Abteilung angehören, müssen eine Verbindung zum WAP herstellen und mit den Admin-Abteilungsbenutzern im kabelgebundenen Netzwerk (in VLAN 20) verbunden werden können. Die Wireless-Gastbenutzer müssen eine Verbindung zu einem Webserver herstellen können, der sich auf dem kabelgebundenen Segment des VLAN 30 befindet. Ein Catalyst 2950-Switch verbindet den Access Point mit dem kabelgebundenen Netzwerk. Ein 2800 ISR-Router ist mit demselben Switch verbunden und fungiert als DHCP-Server für Wireless-Clients, die zu VLAN 20 und VLAN 30 gehören. Der Router muss Clients aus ihrem jeweiligen Subnetz IP-Adressen zuweisen. Sie müssen den Access Point, den Catalyst-Switch und den Router für die Implementierung dieser Konfiguration konfigurieren.



Im Folgenden finden Sie eine Liste der IP-Adressen, die für die Geräte im Dokument verwendet werden. Alle IP-Adressen verwenden die /24-Subnetzmaske.

- AP Bridge-Group Virtual Interface (BVI) IP-Adresse (VLAN 2) - 172.16.1.20
- Der Wireless-Client (SSID Admin), der mit VLAN 20 verbunden ist, erhält vom DHCP-Server des Routers eine IP-Adresse aus dem Subnetz 172.16.2.0.
- Der Wireless-Client (SSID Guest), der eine Verbindung zu VLAN 30 herstellt, erhält vom DHCP-Server des Routers eine IP-Adresse aus dem Subnetz 172.16.3.0.
- Admin-Benutzer im kabelgebundenen Netzwerk im VLAN 20-172.16.2.60 (Statische IP)
- Webserver im VLAN 30-172.16.3.60 (statische IP)
- Schnittstelle des Routers in VLAN 2-172.16.1.1
- Schnittstelle des Routers in VLAN 20-172.16.2.1
- Schnittstelle des Routers in VLAN 30-172.16.3.1

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

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

Um den Access Point für die Verbindung mit einem bestimmten VLAN zu konfigurieren, müssen Sie den Service Set Identifier (SSID) für die Erkennung des VLAN konfigurieren. Ein VLAN wird entweder durch eine VLAN-ID oder einen Namen identifiziert. Wenn Sie die SSID auf einem WAP so konfigurieren, dass sie eine bestimmte VLAN-ID oder einen bestimmten VLAN-Namen erkennt, können Sie eine Verbindung zum VLAN herstellen. Nach Herstellen der Verbindung werden die Wireless-Clients, die mit dem WAP verbunden sind und die spezielle SSID verwenden, diesem VLAN zugewiesen. Da Sie bis zu 16 SSIDs auf einem WAP konfigurieren können, können Sie 16 VLANs auf einem WAP erstellen. Um VLANs auf APs zu konfigurieren und Verbindungen herzustellen, müssen Sie die folgenden Schritte ausführen:

1. [Konfigurieren Sie das native VLAN auf dem WAP.](#)
2. [Konfigurieren Sie VLANs für die Gastbenutzer und die Admin-Benutzer des APs.](#)
3. [Konfigurieren Sie den Catalyst Switch.](#)
4. [Konfigurieren des Routers](#)

[Konfigurieren des nativen VLANs auf dem WAP](#)

Das VLAN, mit dem der Access Point selbst und andere Infrastrukturgeräte wie der Switch, mit dem der Access Point verbunden ist, werden als natives VLAN bezeichnet. Das native VLAN des Access Points unterscheidet sich in der Regel von anderen VLANs, die auf dem Access Point konfiguriert wurden. Es handelt sich um die **BVI-Schnittstelle**, die für die Verwaltung des Access Points verwendet wird, dem eine IP-Adresse im nativen VLAN-Subnetz zugewiesen wird. Der Datenverkehr, z. B. der Verwaltungsverkehr, der an den und vom Access Point selbst gesendet wird, übernimmt das native VLAN und ist nicht markiert. Der gesamte nicht getaggte Datenverkehr, der an einem IEEE 802.1Q (dot1q)-Trunk-Port empfangen wird, wird mit dem für den Port konfigurierten nativen VLAN weitergeleitet. Wenn ein Paket über eine VLAN-ID verfügt, die mit der nativen VLAN-ID des sendenden Ports identisch ist, sendet der Switch das Paket ohne Tag. Andernfalls sendet der Switch das Paket mit einem Tag.

Führen Sie folgende Befehle im globalen Konfigurationsmodus des AP aus, um ein natives VLAN auf einem WAP zu konfigurieren:

```
AccessPoint<config>#interface fastethernet 0.2
AccessPoint<config-subif>#encapsulation dot1q 2 native
!--- Configure the encapsulation as dot1q and assign VLAN 2 as the native VLAN !--- on the Fast
Ethernet interface. AccessPoint<config-subif>#exit
AccessPoint<config>#interface dot11radio 0.2
AccessPoint<config-subif>#encapsulation dot1q 2 native
!--- Configure the encapsulation as dot1q and assign VLAN 2 as the native VLAN !--- on the radio
interface. AccessPoint<config-subif>#end
```

[Konfigurieren von VLANs für Gastbenutzer und Admin-Benutzer am WAP](#)

Hier müssen Sie zwei VLANs konfigurieren, eines für die Gastbenutzer und das andere für die Benutzer der Admin-Abteilung. Sie müssen die SSID auch den spezifischen VLANs zuordnen. In diesem Beispiel wird Folgendes konfiguriert:

- VLAN 20 für die Admin-Abteilung und verwendet SSID **Admin**
- VLAN 30 für Gastbenutzer und verwendet SSID **Guest**

Um diese VLANs zu konfigurieren, geben Sie die folgenden Befehle im globalen Konfigurationsmodus ein:

```
AccessPoint#configure terminal
```

```
!--- Enter global configuration mode. AccessPoint(config)#interface dot11radio 0
!--- Enter radio interface configuration mode. AccessPoint(config-if)#ssid Admin
!--- Configure the SSID "Admin". AccessPoint(config-if-ssid)#vlan 20
!--- Assign VLAN 20 to the SSID. AccessPoint(config-if-ssid)#authentication open
!--- Configure open authentication for the SSID. AccessPoint(config-if-ssid)#end
```

```
AccessPoint(config) interface fastethernet 0.20
```

```
!--- Enter subinterface mode on the Fast Ethernet interface. AccessPoint(config-subif)
encapsulation dot1Q 20
!--- Set the encapsulation as dot1q for VLAN 20. AccessPoint(config-subif) bridge-group 20
!--- Assign the subinterface to bridge group 20. AccessPoint(config-subif) exit
```

```
AccessPoint(config) interface dot11radio 0.20
```

```
!--- Enter subinterface mode on the radio interface. AccessPoint(config-subif) encapsulation
dot1Q 20
!--- Set the encapsulation as dot1q for VLAN 20. AccessPoint(config-subif) bridge-group 20
!--- Assign the subinterface to bridge group 20. AccessPoint(config-subif) exit
```

Wiederholen Sie die gleichen Schritte, um VLAN 30 für die Admin-Benutzer zu konfigurieren:

```
AccessPoint#configure terminal
```

```
AccessPoint(config)#interface dot11radio 0
AccessPoint(config-if)#ssid Guest
AccessPoint(config-if-ssid)#vlan 30
AccessPoint(config-if-ssid)#authentication open
AccessPoint(config-if-ssid)#end
```

```
AccessPoint(config) interface fastethernet 0.30
```

```
AccessPoint(config-subif) encapsulation dot1Q 30
AccessPoint(config-subif) bridge-group 30
AccessPoint(config-subif) exit
```

```
AccessPoint(config) interface dot11radio 0.30
```

```
AccessPoint(config-subif) encapsulation dot1Q 30
AccessPoint(config-subif) bridge-group 30
AccessPoint(config-subif) exit
```

Hinweis: Dieses Dokument verwendet eine offene Authentifizierung für die SSID Admin und Guest. Die Authentifizierungstypen sind an die SSIDs gebunden, die Sie für den Access Point konfigurieren. Informationen zum Konfigurieren verschiedener Authentifizierungstypen auf dem Access Point finden Sie unter [Konfigurieren von Authentifizierungstypen](#).

[Konfigurieren des Catalyst Switches](#)

Der nächste Schritt besteht in der Konfiguration der Switch-Ports, die die APs und den Router mit dem kabelgebundenen Netzwerk verbinden. Sie sollten den Switch-Port, der mit dem AP und dem

Router verbunden ist, als Trunk-Port konfigurieren, da dieser Port den Datenverkehr aller VLANs im Wireless-Netzwerk überträgt. In diesem Beispiel sind die VLANs VLAN 20, VLAN 30 und das native VLAN 2. Wenn Sie den Switch-Port konfigurieren, der mit dem Access Point und dem Router verbunden ist, stellen Sie sicher, dass die nativen VLANs, die Sie konfigurieren, mit dem nativen VLAN auf dem Access Point und dem Router übereinstimmen. Andernfalls werden Frames verworfen. Führen Sie folgende Befehle aus der CLI des Switches aus, um den Trunk-Port am Switch zu konfigurieren:

Hinweis: In diesem Dokument wird der Catalyst 2950 Switch verwendet. Die Konfigurationen des Switch-Ports können variieren, was von dem verwendeten Switch-Modell abhängt. Wie im Diagramm gezeigt, stellt das Schnittstellenverbindungskabel 0/5 eine Verbindung zum Router her, und das Schnittstellenverbindungskabel 0/10 stellt eine Verbindung zum Access Point her.

```
Switch#configure terminal
Switch<config>#interface fastethernet 0/5
!--- Enter the interface mode for Fast Ethernet 0/5. Switch<config-if>#switchport mode trunk
!--- Configure the switch port mode to trunk mode. Switch<config-if>#switchport trunk
encapsulation dot1q
!--- Configure the encapsulation on the switch port to dot1q. Switch<config-if>#switchport trunk
native vlan 2
!--- Configure the native VLAN as VLAN 2. Switch<config-if>#switchport trunk allowed vlan add
2,20,30
!--- Configure the list of VLANs that are allowed on the trunk port. Switch<config-
if>#switchport nonegotiate
```

```
Switch#configure terminal
Switch<config>#interface fastethernet 0/10
!--- Enter the interface mode for Fast Ethernet 0/10 Switch<config-if>#switchport mode trunk
!--- Configure the switch port mode to trunk mode. Switch<config-if>#switchport trunk
encapsulation dot1q
!--- Configure the encapsulation on the switch port to dot1q. Switch<config-if>#switchport trunk
native vlan 2
!--- Configure the native VLAN as VLAN 2. Switch<config-if>#switchport trunk allowed vlan add
2,20,30
!--- Configure the list of VLANs that are allowed on the trunk port. Switch<config-
if>#switchport nonegotiate
```

Hinweis: Die auf der Cisco IOS Software basierenden Aironet Wireless-Geräte unterstützen kein Dynamic Trunking Protocol (DTP). Daher darf der Switch nicht versuchen, DTP auszuhandeln.

Konfigurieren des Routers

Der Router ist als DHCP-Server für die Wireless-Clients in VLAN 20 und VLAN 30 konfiguriert. Der Router verfügt über drei Subschnittstellen, eine für jedes VLAN 2, 20 und 30, sodass er Clients im Subnetz ihres jeweiligen VLAN IP-Adressen zuweisen und VLAN-übergreifendes Routing durchführen kann.

```
Router#configure terminal
Router<config>#interface fastethernet 0/0.2
!--- Configures a Sub-interface .2 on fastethernet 0/0 Router<config-subif>#encapsulation dot1q
2 native
!--- configures the encapsulation as dot1q and assigns VLAN 2 to the sub-interface This command
also makes VLAN 2 as the Native VLAN. Here number 2 is the VLAN-id.

Router<config-subif>#ip address 172.16.1.1 255.255.255.0
```

```

!--- Assign ip address from Native VLAN 2 subnet - 172.16.1.0 /24 to the sub-interface
Router<config-subif>#exit
Router<config>#interface fastethernet 0/0.20
!--- Configures a Sub-interface .20 on fastethernet 0/0 Router<config-subif>#encapsulation dot1q
20
!--- configures the encapsulation as dot1q and assigns VLAN 20 to the sub-interface Here number
20 is the VLAN-id.

Router<config-subif>#ip address 172.16.2.1 255.255.255.0
!--- Assign ip address from VLAN 20 subnet - 172.16.2.0 /24 to the sub-interface Router<config-
subif>#exit
Router<config>#interface fastethernet 0/0.30
!--- Configures a Sub-interface .30 on fastethernet 0/0 Router<config-subif>#encapsulation dot1q
30
!--- configures the encapsulation as dot1q and assigns VLAN 30 to the sub-interface Here number
30 is the VLAN-id.

Router<config-subif>#ip address 172.16.3.1 255.255.255.0
!--- Assign ip address from VLAN 30 subnet - 172.16.3.0 /24 Router<config-subif>#exit

```

DHCP Configuration starts here

```

Router<config>#ip dhcp excluded-address 172.16.2.1
Router<config>#ip dhcp excluded-address 172.16.3.1
!--- excluded-address command is used to exclude the specified ip addresses from the DHCP pool.
In this case router's sub-interface addresses are excluded. Router<config>#ip dhcp pool pool1
!--- Creates a DHCP pool with a name pool1 and enters the DHCP config mode router<dhcp-
config>#network 172.16.2.0 /24
!--- From this pool Clients are assigned ip addresses from 172.16.2.0 /24 Subnet i.e. from
172.16.2.2 - 172.16.2.254 router<dhcp-config>#default-router 172.16.2.1
!--- Default-gateway assigned to the client from this pool is 172.16.2.1 . Default-router is
nothing but default-gateway Router<config>#ip dhcp pool pool2
!--- Creates a DHCP pool with a name pool2 and enters the DHCP config mode router<dhcp-
config>#network 172.16.3.0 /24
!--- From this pool Clients are assigned ip addresses from 172.16.3.0 /24 Subnet i.e. from
172.16.3.2 - 172.16.3.254 router<dhcp-config>#default-router 172.16.3.1
!--- Default-gateway assigned to the client from this pool is 172.16.3.1 .

```

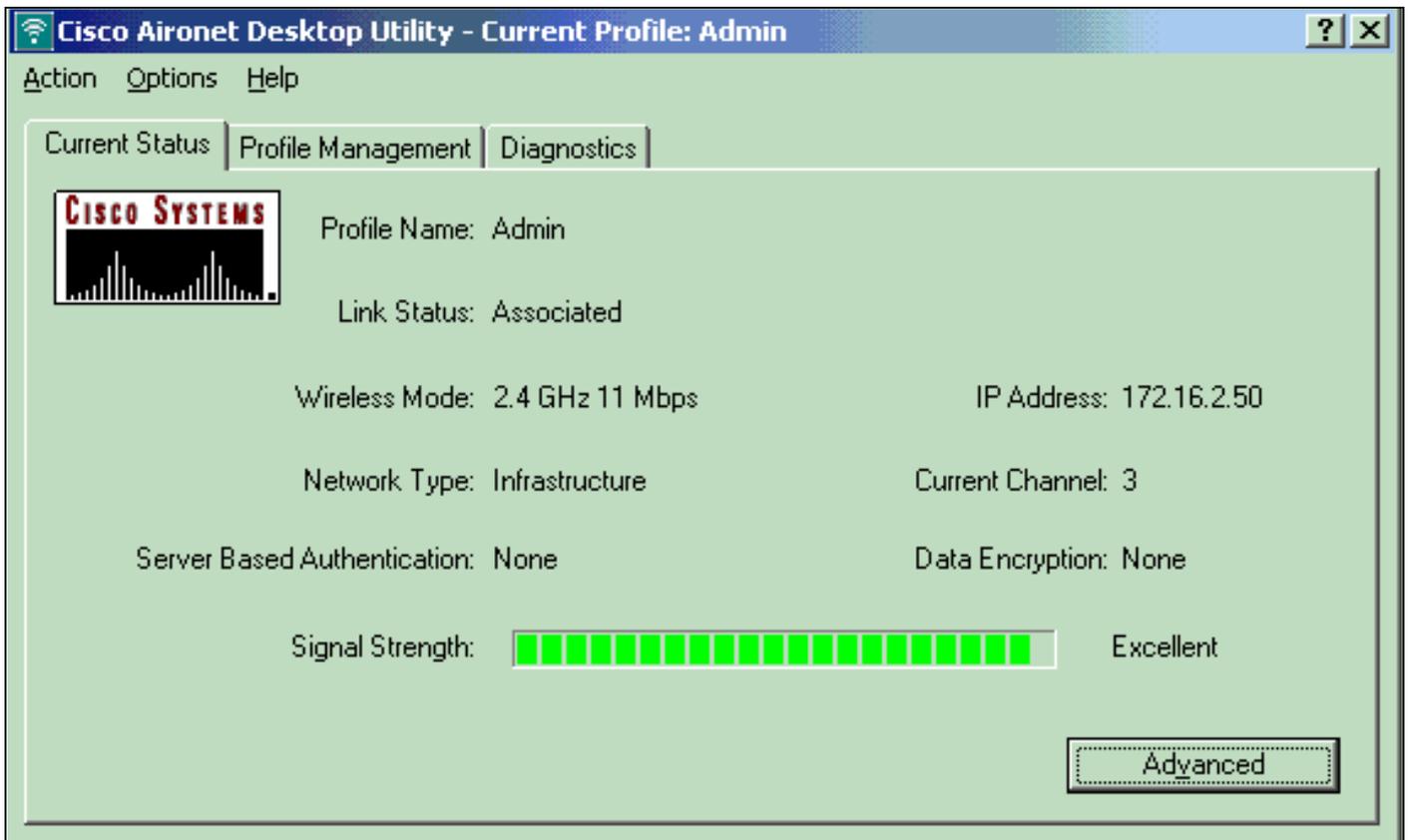
Überprüfen

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

Sie können überprüfen, ob die Konfiguration wie erwartet funktioniert. Der Wireless-Client (Admin-Benutzer), der mit SSID **Admin** konfiguriert ist, muss mit VLAN 20 verbunden werden. Derselbe Benutzer sollte eine Verbindung zum Administrator-Benutzer im kabelgebundenen Netzwerk herstellen können, das sich ebenfalls im gleichen VLAN befindet. Aktivieren Sie zur Überprüfung das Wireless-Clientprofil für den Administrator-Benutzer.

Hinweis: In diesem Dokument wird nicht erläutert, wie der Wireless-Client zum Einrichten von Profilen konfiguriert wird. Weitere Informationen zum Konfigurieren des Wireless-Client-Adapters finden Sie unter [Konfigurieren des Client-Adapters](#).

Dieses Beispielfenster zeigt, dass der Wireless-Client dem AP zugeordnet ist:



Der Befehl **show dot1 associated** (dot1-Zuordnungen anzeigen) auf dem Access Point stellt außerdem sicher, dass der Client mit VLAN 10 verbunden wird:

Hinweis: 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.

```
AccessPoint#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [Admin] :
```

MAC Address	IP address	Device	Name	Parent	State
0040.96ac.e657	172.16.2.50	CB21AG/PI21AG	Admin User	self	Assoc

Sie können den Befehl **show vlans** auf dem WAP ausführen, um die VLANs anzuzeigen, die auf dem WAP konfiguriert sind. Hier ein Beispiel:

```
AccessPoint#show vlans
```

```
Virtual LAN ID: 2 (IEEE 802.1Q Encapsulation)
```

```
vLAN Trunk Interfaces: Dot11Radio0.2
FastEthernet0.2
```

```
This is configured as native Vlan for the following interface(s) :
```

```
Dot11Radio0
FastEthernet0
```

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 1	1380	712
Other		0	63

```
0 packets, 0 bytes input
733 packets, 50641 bytes output
  Bridging      Bridge Group 1      1380      712
  Other          0                               63
```

```
1381 packets, 98016 bytes input
42 packets, 12517 bytes output
```

Virtual LAN ID: 20 (IEEE 802.1Q Encapsulation)

```
vLAN Trunk Interfaces: Dot11Radio0.20
FastEthernet0.20
```

```
Protocols Configured:  Address:      Received:      Transmitted:
  Bridging      Bridge Group 20      798           622
  Other          0                     0             19
```

```
247 packets, 25608 bytes input
495 packets, 43585 bytes output
  Bridging      Bridge Group 20      798           622
  Other          0                     0             19
```

```
552 packets, 37536 bytes input
148 packets, 21660 bytes output
```

Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation)

```
vLAN Trunk Interfaces: Dot11Radio0.30
FastEthernet0.30
```

```
Protocols Configured:  Address:      Received:      Transmitted:
  Bridging      Bridge Group 30      693           609
  Other          0                     0             19
```

```
106 packets, 13373 bytes input
517 packets, 48029 bytes output
  Bridging      Bridge Group 30      693           609
  Other          0                     0             19
```

```
605 packets, 47531 bytes input
112 packets, 15749 bytes output
```

Sie können jetzt überprüfen, ob der Wireless-Administrator-Benutzer eine Verbindung zum Administrator-Benutzer auf der kabelgebundenen Seite herstellen kann, der für dasselbe VLAN konfiguriert ist. Geben Sie den **Ping**-Befehl auf dem Wireless-Client aus. Hier ein Beispiel:

```
D:\>ping 172.16.2.60
```

```
Pinging 172.16.2.60 with 32 bytes of data:
```

```
Reply from 172.16.2.60: bytes=32 time<10ms TTL=255
```

```
Ping statistics for 172.16.2.60:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ebenso können Sie überprüfen, ob die Gastbenutzer mit VLAN 30 verbunden sind. Sie können den **Ping**-Befehl auf dem Gast-Wireless-Client ausführen, um die Verbindung zum Webserver auf

der kabelgebundenen Seite zu testen. Hier ein Beispiel:

```
D:\>ping 172.16.3.60
```

```
Pinging 172.16.3.60 with 32 bytes of data:
```

```
Reply from 172.16.3.60: bytes=32 time<10ms TTL=255
```

```
Ping statistics for 172.16.3.60:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

Fehlerbehebungsverfahren

Befolgen Sie diese Anweisungen, um eine Fehlerbehebung in Ihrer Konfiguration durchzuführen:

1. Überprüfen Sie, ob das native VLAN, das auf dem Switch-Port konfiguriert und mit dem AP verbunden ist, mit dem nativen VLAN des AP übereinstimmt. Wenn im nativen VLAN eine Diskrepanz auftritt, findet keine Verbindung über den Switch statt.
2. Stellen Sie sicher, dass alle auf der Wireless-Seite konfigurierten VLANs auf dem Switch-Port zugelassen sind, der als Trunk konfiguriert ist. Standardmäßig sind alle VLANs über den Trunk-Port zugelassen.
3. Überprüfen Sie, ob der Befehl **bridge-group** für alle VLANs außer dem nativen VLAN konfiguriert ist. Auf der Schnittstelle, die Sie als natives VLAN einrichten, müssen Sie keine Bridge-Gruppe konfigurieren. Diese Bridge-Gruppe wird automatisch in die native Schnittstelle verschoben, um die Verbindung zu BVI 1 aufrecht zu erhalten, die sowohl die Radio- als auch die Ethernet-Schnittstelle darstellt. **Achtung:** Wenn Sie den Befehl **bridge-group** konfigurieren, werden diese Befehle automatisch aktiviert:

```
bridge-group 10 subscriber-loop-control
bridge-group 10 block-unknown-source
no bridge-group 10 source-learning
no bridge-group 10 unicast-flooding
bridge-group 10 spanning-disabled
```

Hierbei handelt es sich um Standardeinstellungen, die nur unter Anleitung geändert werden sollten. Wenn Sie diese Befehle entfernen, funktioniert das WLAN möglicherweise nicht wie erwartet.

Befehle zur Fehlerbehebung

Sie können diese Befehle auch verwenden, um eine Fehlerbehebung für Ihre Konfiguration auf dem Access Point durchzuführen:

Hinweis: 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**.

- VLANs anzeigen
- **show vlans dot1q**
- **dot11-Verbände anzeigen**

Auf dem Catalyst 2950-Switch können Sie die folgenden Befehle verwenden, um eine Fehlerbehebung für die Konfiguration durchzuführen:

- VLANs anzeigen
- **show interface fastethernet x/x switchport**
- **show interface fastethernet x/x trunk**

Führen Sie auf dem Router diese Befehle aus, um eine Fehlerbehebung für die Konfiguration durchzuführen.

- **debuggen ip dhcp server paket**
- **show ip interface brief**

Im Folgenden finden Sie eine Ausgabe der erfolgreichen Zuweisung von IP-Adressen an den Client in SSID Admin.

```
Router#debug ip dhcp server packet
*Nov 23 18:02:06.637: DHCPD: DHCPREQUEST received from client 0040.96ac.e657.
!--- Router receives the DHCP Request from the client *Nov 23 18:02:06.637: DHCPD: No default
domain to append - abort update *Nov 23 18:02:06.637: DHCPD: Sending DHCPACK to client
0040.96ac.e657 (172.16.2.50).
!--- Router acknowledges the client's request *Nov 23 18:02:06.637: DHCPD: creating ARP entry
(172.16.2.2, 0040.96ac.e657). *Nov 23 18:02:06.637: DHCPD: unicasting BOOTREPLY to client
0040.96ac.e657 (172.16.2.50).
!--- Router assigns ip address to the client from the VLAN 10 subnet
```

[Zugehörige Informationen](#)

- [Verwendung von VLANs mit Cisco Aironet Wireless Equipment](#)
- [EAP-Authentifizierung mit RADIUS-Server](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)