

Ejemplo de Configuración de VLANs en Puntos de Acceso Aironet

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configurar](#)

[Configure el VLAN nativo en el AP](#)

[Configure los VLAN para los Usuarios invitados y los Usuarios administradores en el AP](#)

[Configure el switch de Catalyst](#)

[Configure el Router](#)

[Verificación](#)

[Troubleshooting](#)

[Procedimiento de Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona un ejemplo de configuración que muestra cómo configurar las VLAN en Puntos de acceso Cisco Aironet (AP) mediante la interfaz de línea de comandos (CLI).

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de la configuración básica del Aironet AP
- Conocimiento de la configuración del adaptador del cliente del Aironet 802.11a/b/g con utilidad Aironet Desktop
- Conocimiento básico de la configuración de los Switches y de los routers Cisco del Cisco Catalyst

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Serie AP del Aironet 1240AG que funciona con la versión 12.4(3g)JA1 del Cisco IOS ® Software
- Adaptador del cliente del Aironet 802.11a/b/g
- Utilidad Aironet Desktop esa versión de firmware 2.5 de los funcionamientos
- Catalyst 2950 Switch que funciona con el Cisco IOS Software Release 12.1(19)EA1
- Router de 2800 ISR que funciona con el Cisco IOS Software Release 12.4(11)T

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

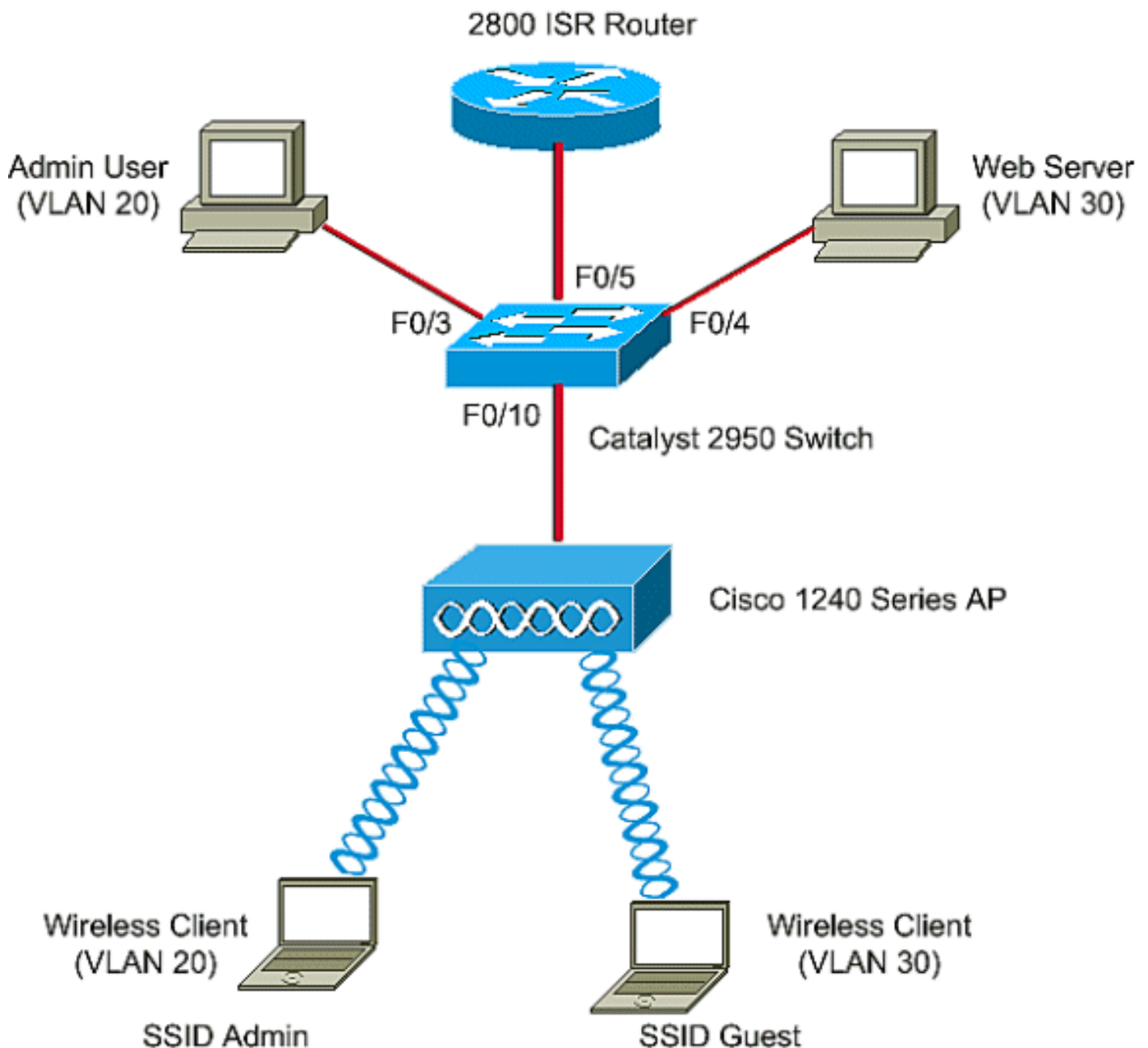
[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

[Diagrama de la red](#)

Este documento utiliza esta configuración de red:

Las 1200 Series AP del Aironet tienen tres VLAN — VLAN2, VLAN20, y VLAN 30. La configuración en este documento utiliza el VLAN2 como el VLAN nativo, el VLAN20 para el departamento administrativo (admin), y el VLAN 30 para los Usuarios invitados. Los usuarios de red inalámbrica que pertenecen al departamento de administración deben conectar con el AP y deben poder conectar con los usuarios del departamento administrativos en la red alámbrica (en el VLAN20). Los Usuarios invitados inalámbricos deben poder conectar con un servidor Web que esté en el segmento cableado en el VLAN 30. Un Catalyst 2950 Switch conecta el AP con la red alámbrica. Un router de 2800 ISR conecta con el mismo Switch y actúa como servidor DHCP para los clientes de red inalámbrica que pertenecen al VLAN20 y al VLAN 30. El router necesita asignar los IP Addresses a los clientes de su subred correspondiente. Usted debe configurar el AP, el switch de Catalyst, y al router para una implementación de esta configuración.



Abajo está la lista de IP Addresses usada para los dispositivos en el documento. Toda la máscara de subred de /24 del uso de los IP Addresses

- Dirección IP del (BVI) del Interfaz Virtual de Bridge-Group AP (VLAN 2) — 172.16.1.20
- El cliente de red inalámbrica (SSID Admin) que conecta con el VLAN20 consigue una dirección IP del servidor DHCP del router de la subred 172.16.2.0
- El cliente de red inalámbrica (invitado SSID) que conecta con el VLAN 30 consigue una dirección IP del servidor DHCP del router de la subred 172.16.3.0
- Usuario administrador en la red alámbrica en el VLAN20 — 172.16.2.60 (IP estático)
- Servidor Web en el VLAN 30 — 172.16.3.60 (IP estático)
- Sub-interfaz del router en el VLAN2 — 172.16.1.1
- Sub-interfaz del router en el VLAN20 — 172.16.2.1
- Sub-interfaz del router en el VLAN 30 — 172.16.3.1

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la herramienta [Command Lookup Tool \(clientes registrados solamente\)](#) para encontrar más información sobre los comandos usados en este documento.

Para configurar el AP para conectar con un VLA N específico, usted debe configurar el Service Set Identifier (SSID) para reconocer el VLA N. Un VLAN ID o un nombre identifica un VLA N. Por lo tanto, si usted configura el SSID en un AP para reconocer un VLAN ID o un nombre específico, usted puede establecer una conexión al VLA N. Después del establecimiento de la conexión, asignan los clientes de red inalámbrica que conectan con el AP con el uso del SSID específico a ese VLA N. Porque usted puede configurar hasta 16 SSID en un AP, usted puede crear 16 VLA N en un AP. Para configurar los VLA N en los AP y establecer la Conectividad, usted debe completar estos pasos:

1. [Configure el VLAN nativo en el AP.](#)
2. [Configure los VLA N para los Usuarios invitados y los Usuarios administradores en el AP.](#)
3. [Configure el switch de Catalyst.](#)
4. [Configure al router](#)

[Configure el VLAN nativo en el AP](#)

El VLA N, al cual el Punto de acceso sí mismo y otros dispositivos de infraestructura tales como el Switch, con que el Punto de acceso conecta, se llama VLAN nativo. El VLAN nativo del Punto de acceso es generalmente diferente de otros VLA N configurados en el Punto de acceso. Es la **interfaz BVI**, que se utiliza para la Administración del Punto de acceso que se asigna una dirección IP en la subred del VLAN nativo. El tráfico, por ejemplo, tráfico de administración, envió a y por el Punto de acceso sí mismo asume el VLAN nativo, y es untagged. Todo el tráfico sin Tags que se recibe en un puerto troncal del IEEE 802.1Q (dot1q) se remite con el VLAN nativo que se configura para el puerto. Si un paquete tiene un VLAN ID que sea lo mismo que el VLAN nativo ID del puerto de envío, el Switch envía el paquete sin una etiqueta. Si no, el Switch envía el paquete con una etiqueta.

Para configurar un VLAN nativo en un AP, publique estos comandos en el modo de configuración global en el AP:

```
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
```

[Configure los VLA N para los Usuarios invitados y los Usuarios administradores en el AP](#)

Aquí, usted necesita configurar dos VLA N, uno para los Usuarios invitados y el otro para los usuarios del departamento administrativos. Usted también necesita asociar el SSID a los VLA N específicos. Este ejemplo configura:

- El VLAN20 para el departamento de administración y utiliza el SSID Admin
- El VLAN 30 para los Usuarios invitados y utiliza al invitado SSID

Para configurar estos VLAN, ingrese estos comandos en el modo de configuración global:

```

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

```

Relance el mismo procedimiento para configurar el VLAN 30 para los Usuarios administradores:

```

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

```

Nota: Este documento utiliza la autenticación abierta para SSID Admin y el invitado. Atan a los tipos de autenticación a los SSID que usted configura para el AP. Para la información sobre cómo configurar diversos tipos de autenticación en el AP, refiera a [configurar los tipos de autenticación](#).

[Configure el switch de Catalyst](#)

El siguiente paso es configurar los puertos del switch que conectarán los AP y al router con la red alámbrica. Usted debe configurar el puerto del switch que conecta con el AP y el router como puerto troncal porque este puerto lleva el tráfico de todos los VLAN en la red inalámbrica. En este ejemplo, los VLAN son VLAN20, VLAN 30, y el VLAN nativo 2. Cuando usted configura el puerto

del switch, que conecta con el AP y el router, asegúrese de que los VLAN nativos que usted configura la coincidencia el VLAN nativo en el AP y el router. Si no, se caen las tramas. Para configurar el puerto troncal en el Switch, publique estos comandos del CLI en el Switch:

Nota: Este documento utiliza el Catalyst 2950 Switch. Las configuraciones en el puerto del switch pueden variar, que depende del modelo de switches que usted utiliza. Tal y como se muestra en del diagrama, el FastEthernet 0/5 de la interfaz conecta con el **router**, y el FastEthernet 0/10 de la interfaz conecta con el **Punto de acceso**.

```
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
```

Nota: El equipo basado en software del Aironet de red inalámbrica del Cisco IOS no soporta el Dynamic Trunking Protocol (DTP). Por lo tanto, el Switch no debe intentar negociar el DTP.

[Configure el Router](#)

Configuran al router como el servidor DHCP para los clientes de red inalámbrica en el VLAN20 y el VLAN 30. El router tiene tres subinterfaces, uno para cada VLAN2, 20, y 30 de modo que pueda asignar los IP Addresses a los clientes en la subred de su VLAN respectivo y realizar el Routing entre VLAN.

```
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 .

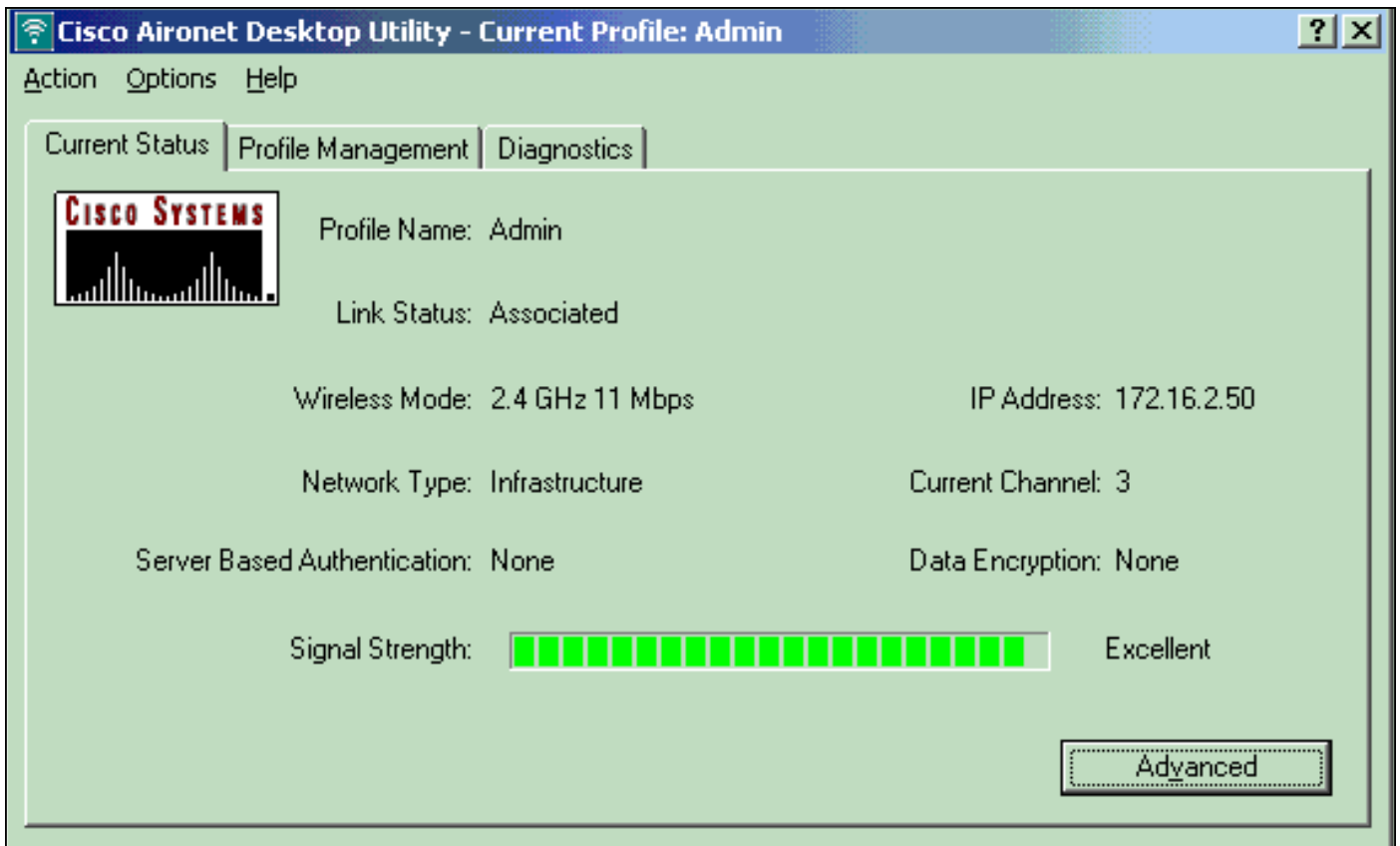
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Usted puede marcar si la configuración trabaja como se esperaba. El cliente de red inalámbrica (Usuario administrador) que se configura con SSID **Admin** debe conseguir conectado con el VLAN20. El mismo usuario debe poder conectar con el Usuario administrador en la red alámbrica, que está también en el mismo VLA N. Para verificar, active el perfil del cliente de red inalámbrica para el Usuario administrador.

Nota: Este documento no explica cómo configurar al cliente de red inalámbrica para configurar los perfiles. Para la información sobre cómo configurar el adaptador de red inalámbrica de cliente, refiera a [configurar el adaptador del cliente](#).

Esta ventana de muestra muestra que asocian al cliente de red inalámbrica al AP:



El comando **show dot11 associations** en el AP también verifica que el cliente consiga conectado con el VLAN10:

Nota: [La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

```
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

Usted puede publicar el **comando show vlans** en el AP para visualizar los VLAN que se configuran en el AP. Aquí tiene un ejemplo:

```
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                     19

```

```

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

```

```

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

```

```

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

```

Usted puede ahora marcar si el Usuario administrador inalámbrico puede conectar con el Usuario administrador en la cara tela, que se configura para el mismo VLA N. Publique el **comando ping** en el cliente de red inalámbrica. Aquí tiene un ejemplo:

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

```

Semejantemente, usted puede marcar si los Usuarios invitados consiguen conectados con el VLAN 30. Usted puede publicar el **comando ping** en el cliente de red inalámbrica del invitado para

probar la Conectividad al servidor Web en la cara tela. Aquí tiene un ejemplo:

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

Troubleshooting

Use esta sección para resolver problemas de configuración.

Procedimiento de Troubleshooting

Siga estas instrucciones para resolver problemas su configuración:

1. Marque si el VLAN nativo que se configura en el puerto del switch y está conectado con el AP hace juego el VLAN nativo del AP. Si hay una discordancia en el VLAN nativo, la Conectividad a través del Switch no sucede.
2. Asegúrese de que todos los VLAN que se configuran en el lado de la Tecnología inalámbrica estén permitidos en el puerto del switch que se configura como el trunk. Por abandono, todos los VLAN se permiten a través del puerto troncal.
3. Marque si configuran al **comando bridge-group** en todos los VLAN excepto el VLAN nativo. Usted no necesita configurar a un Grupo de Bridge en la subinterfaz esa usted configura como el VLAN nativo. Este Grupo de Bridge se mueve automáticamente a la subinterfaz nativa para mantener el link al BVI 1, que representa la radio y las interfaces de Ethernet. **Precaución:** Cuando usted configura el **comando bridge-group**, estos comandos consiguen automáticamente habilitados:

```
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
```

Éstas son configuraciones predeterminadas estándar, y usted no debe cambiarlos a menos que le dirijan. Si usted quita estos comandos, la red inalámbrica (WLAN) puede no poder funcionar como se esperaba.

Comandos para resolución de problemas

Usted puede también utilizar estos comandos para resolver problemas su configuración en el AP:

Nota: [La herramienta Output Interpreter Tool](#) ([clientes registrados solamente](#)) (OIT) soporta

ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- muestre el vlans
- muestre el dot1q del vlans
- muestre las asociaciones del dot11

En el Catalyst 2950 Switch, usted puede utilizar estos comandos para resolver problemas la configuración:

- muestre el vlans
- muestre el switchport del FastEthernet *x/x de la interfaz*
- muestre el trunk del FastEthernet *x/x de la interfaz*

En el router, publique estos comandos para resolver problemas la configuración.

- debug ip dhcp server packet
- *show ip interface brief*

Aquí está una salida de la asignación acertada del IP address al cliente en 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
```

Información Relacionada

- [Uso de las VLAN con el Equipo inalámbrico de Cisco Aironet](#)
- [Autenticación EAP con el servidor de RADIUS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)