

Ejemplo de Configuración de VLANs en Puntos de Acceso Aironet

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configurar](#)

[Configure la VLAN nativa en el AP](#)

[Configure las VLAN para los usuarios temporales y administradores en el AP](#)

[Configure el switch Catalyst](#)

[Configure el router](#)

[Verificación](#)

[Troubleshoot](#)

[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).

[Prerequisites](#)

[Requirements](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de la configuración básica de los AP Aironet
- Conocimiento de la configuración del adaptador de clientes Aironet 802.11a/b/g con utilidad de escritorio Aironet
- Conocimiento básico de la configuración de los switches Cisco Catalyst y los routers Cisco

[Componentes Utilizados](#)

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

hardware.

- AP Aironet de la serie 1240AG que ejecuta el software Cisco IOS® versión 12.4(3g)JA1
- Adaptador de clientes Aironet 802.11a/b/g
- Utilidad de escritorio Aironet que ejecuta el firmware versión 2.5
- Switch Catalyst 2950 que ejecuta el software Cisco IOS versión 12.1(19)EA1
- Router ISR 2800 que ejecuta el software Cisco IOS versión 12.4(11)T

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

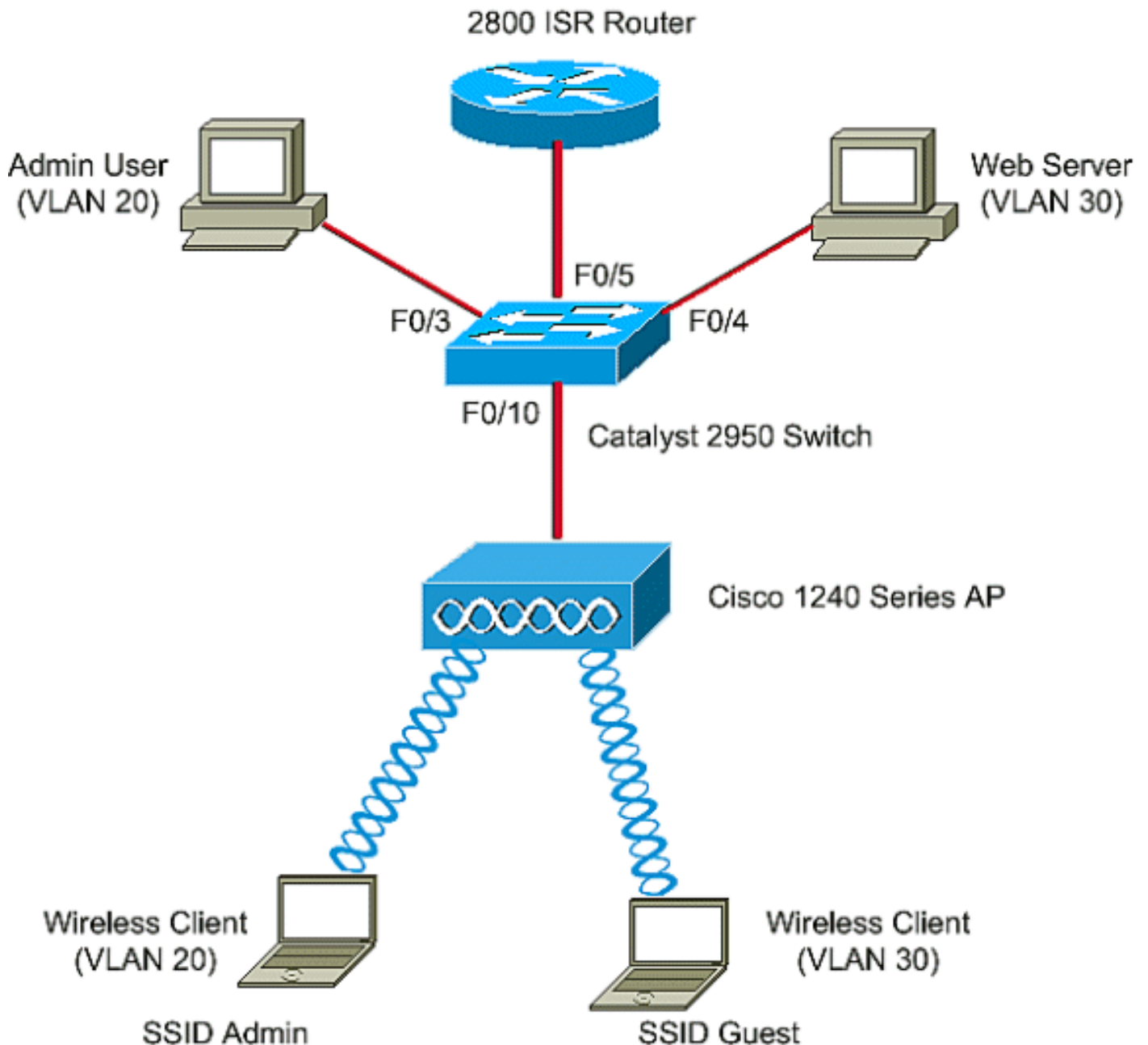
Convenciones

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:

Un AP Aironet de la serie 1200 tiene tres VLAN: VLAN 2, VLAN 20 y VLAN 30. En la configuración de este documento se usa la VLAN 2 como VLAN nativa, la VLAN 20 para el departamento administrativo (admin) y la VLAN 30 para los usuarios temporales. Los usuarios inalámbricos que pertenecen al departamento administrativo deben conectarse al AP y a los usuarios del departamento administrativo en la red cableada (VLAN 20). Los usuarios inalámbricos temporales deben conectarse a un servidor web en el segmento cableado de la VLAN 30. Un switch Catalyst 2950 conecta el AP a la red cableada. Un router ISR 2800 se conecta al mismo switch y actúa como servidor DHCP para los clientes inalámbricos que pertenecen a la VLAN 20 y la VLAN 30. El router debe asignar direcciones IP a los clientes desde la subred respectiva. Debe configurar el AP, el switch Catalyst y el router para implementar esta configuración.



A continuación se muestra la lista de direcciones IP que usan los dispositivos en el documento. Todas las direcciones IP usan la máscara de subred /24.

- Dirección IP de la interfaz virtual del grupo de puentes (BVI) del AP (VLAN 2): 172.16.1.20
- Cliente inalámbrico (administrador de SSID) que se conecta a la VLAN 20 y obtiene una dirección IP del servidor DHCP del router de la subred 172.16.2.0
- Cliente inalámbrico (usuario temporal de SSID) que se conecta a la VLAN 30 y obtiene una dirección IP del servidor DHCP del router de la subred 172.16.3.0
- Usuario administrador en la red cableada de la VLAN 20: 172.16.2.60 (IP estático)
- Servidor web en la VLAN 30: 172.16.3.60 (IP estático)
- Subinterfaz del router en la VLAN 2: 172.16.1.1
- Subinterfaz del router en la VLAN 20: 172.16.2.1
- Subinterfaz del router en la VLAN 30: 172.16.3.1

Configurar

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

Nota: Use la [Command Lookup Tool](#) (sólo [clientes registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

A fin de configurar el AP para que se conecte a una VLAN específica, debe establecer el identificador de conjunto de servicios (SSID) para que reconozca la VLAN. Puede ser un ID de VLAN o un nombre que identifique la VLAN. Por lo tanto, si configura el SSID en un AP para que reconozca un ID o un nombre de VLAN específicos, podrá establecer una conexión a la VLAN. Después de establecer la conexión, los clientes inalámbricos que se conectan al AP con el SSID específico se asignan a dicha VLAN. Dado que puede configurar hasta 16 SSID en un AP, puede crear 16 VLAN en un AP. Para configurar las VLAN en los AP y establecer la conectividad, debe completar los siguientes pasos:

1. [Configure la VLAN nativa en el AP.](#)
2. [Configure las VLAN para los usuarios temporales y los usuarios administradores en el AP.](#)
3. [Configure el switch Catalyst.](#)
4. [Configure el router](#)

[Configure la VLAN nativa en el AP](#)

La VLAN, a la que el punto de acceso y otros dispositivos de infraestructura, como el switch, se conectan, se denomina "VLAN nativa". Por lo general, la VLAN nativa del punto de acceso es diferente de otras VLAN configuradas en el punto de acceso. Se trata de la **interfaz virtual del grupo de puentes (BVI)**, que se utiliza para administrar el punto de acceso que tiene asignada una dirección IP en la subred de la VLAN nativa. El tráfico, por ejemplo, el tráfico de administración, enviado hacia y por el punto de acceso asume la VLAN nativa y no está etiquetado. Todo el tráfico sin etiquetar recibido en un puerto de enlace troncal IEEE 802.1Q (dot1q) se reenvía a la VLAN nativa configurada para el puerto. Si un paquete tiene un ID de VLAN similar al ID de VLAN nativa del puerto de envío, el switch envía el paquete sin ninguna etiqueta. De lo contrario, el switch envía el paquete con una etiqueta.

Para configurar una VLAN nativa en un AP, emita 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 las VLAN para los usuarios temporales y administradores en el AP](#)

Aquí debe configurar dos VLAN, una para los usuarios temporales y otra para los usuarios del departamento administrativo. También debe asociar el SSID a las VLAN específicas. En este ejemplo se configura lo siguiente:

- La VLAN 20 para el departamento administrativo que usa el **administrador de SSID**.

- La VLAN 30 para los usuarios temporales que usa el usuario temporal de SSID.

Para configurar estas VLAN, introduzca 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
```

Repita el mismo procedimiento para configurar la 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 los SSID Admin y Guest. Los tipos de autenticación están vinculados a los SSID configurados en el AP. Para obtener información sobre cómo configurar diferentes tipos de autenticación en el AP, consulte [Configuración de los tipos de autenticación](#).

[Configure el switch Catalyst](#)

El siguiente paso es configurar los puertos de switch que conectarán los AP y el router a la red cableada. Debe configurar el puerto de switch que se conecta al AP y el router como puerto de enlace troncal, dado que este puerto transporta el tráfico de todas las VLAN en la red inalámbrica. En este ejemplo, las VLAN son la VLAN 20, la VLAN 30 y la VLAN 2 nativa. Cuando configure el

puerto de switch, que se conecta al AP y el router, asegúrese de que las VLAN nativas configuradas coincidan con la VLAN nativa del AP y el router. De lo contrario, se descartan las tramas. Para configurar el puerto de enlace troncal en el switch, emita estos comandos desde la CLI en el switch:

Nota: Este documento utiliza el switch Catalyst 2950. Las configuraciones en el puerto de switch pueden variar, lo que depende del modelo de switch que use. Como se muestra en el diagrama, la interfaz FastEthernet 0/5 se conecta al router y la interfaz FastEthernet 0/10 se conecta al 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 inalámbrico Aironet basado en el software Cisco IOS no admite el protocolo de enlace troncal dinámico (DTP). Por lo tanto, el switch no debe intentar negociar el DTP.

Configure el router

El router está configurado como servidor DHCP para los clientes inalámbricos en la VLAN 20 y la VLAN 30. El router tiene tres subinterfaces, una para cada VLAN 2, 20 y 30, a fin de asignar direcciones IP a los clientes en la subred de la VLAN respectiva 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 .

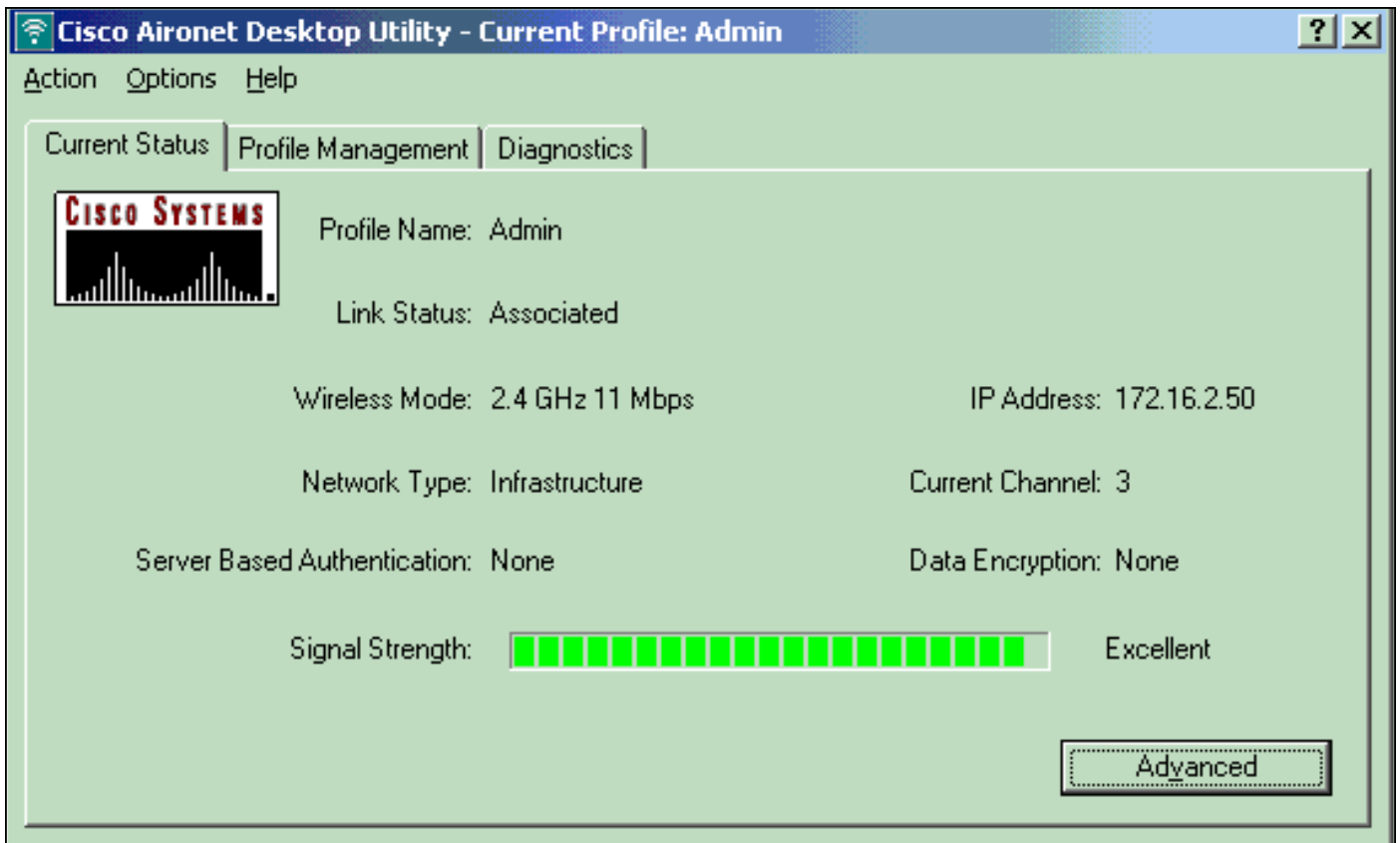
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Puede comprobar si la configuración funciona según lo esperado. El cliente inalámbrico (usuario administrador) configurado con el **administrador de SSID debe conectarse a la VLAN 20**. El mismo usuario debe conectarse al usuario administrador en la red cableada, que también está en la misma VLAN. Para verificarlo, active el perfil de cliente inalámbrico para el usuario administrador.

Nota: Este documento no explica cómo configurar el cliente inalámbrico para configurar perfiles. Para obtener información sobre cómo configurar el adaptador de cliente inalámbrico, consulte [Configuración del adaptador de clientes](#).

En esta ventana de ejemplo se muestra que el cliente inalámbrico está asociado al AP:



El comando **show dot11 associations** en el AP también verifica que el cliente se conecte a la VLAN 10:

Nota: La [Herramienta Output Interpreter](#) (sólo clientes registrados) (OIT) admite determinados 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

Puede ejecutar el comando **show vlans** en el AP para mostrar las VLAN configuradas 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
```

Ahora puede verificar si el usuario administrador inalámbrico es capaz de conectarse al usuario administrador en el lado cableado, que está configurado para la misma VLAN. Emita el comando **ping en el cliente inalámbrico**. 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
```

De manera similar, puede comprobar si los usuarios temporales se conectan a la VLAN 30. Puede ejecutar el comando **ping en el cliente inalámbrico temporal para probar la conectividad al**

servidor web en el lado cableado. 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
```

Troubleshoot

Use esta sección para resolver problemas de configuración.

Procedimiento de Troubleshooting

Siga estas instrucciones para resolver problemas de configuración:

1. Verifique si la VLAN nativa que está configurada en el puerto de switch y conectada al AP coincide con la VLAN nativa del AP. Si hay una incompatibilidad en la VLAN nativa, no sucede la conectividad a través del switch.
2. Asegúrese de que todas las VLAN configuradas en el lado inalámbrico estén permitidas en el puerto de switch configurado como enlace troncal. De manera predeterminada, todas las VLAN se permiten en un enlace troncal.
3. Verifique que el comando **bridge-group** esté configurado en todas las VLAN, excepto la **VLAN nativa**. No es necesario configurar un grupo de puentes en la subinterfaz establecida como VLAN nativa. Este grupo de puentes se traslada automáticamente a la subinterfaz nativa para mantener el enlace a BVI 1, que representa las interfaces de radio y Ethernet. **Precaución:** Cuando configura el comando **bridge-group**, estos comandos se habilitan automáticamente:

```
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
```

Estas son las configuraciones predeterminadas estándar; no debe cambiarlas a menos que se le indique. Si elimina estos comandos, la WLAN no funcionará como se espera.

Comandos para resolución de problemas

También puede usar estos comandos para solucionar problemas en la configuración en el AP:

Nota: La [Herramienta Output Interpreter](#) (sólo clientes registrados) (OIT) admite determinados comandos [show](#). Utilice la OIT para ver un análisis del resultado del comando show.

- **show vlans**
- **show vlans dot1q**
- **show dot11 associations**

En el switch Catalyst 2950, puede usar estos comandos para resolver problemas de configuración:

- **show vlans**
- **show interface fastethernet x/x switchport**
- **show interface fastethernet x/x trunk**

En el router, emita estos comandos para resolver problemas de configuración:

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

Aquí se muestra el resultado de la asignación correcta de direcciones IP al cliente en el administrador de SSID.

```
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 del EAP con servidor RADIUS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).