

Uso de las VLAN con el Equipo inalámbrico de Cisco Aironet

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Productos Relacionados](#)

[Convenciones](#)

[VLAN](#)

[Importancia de VLAN nativa](#)

[VLAN en puntos de acceso](#)

[Conceptos con puntos de acceso](#)

[Configuración del punto de acceso](#)

[VLAN en puentes](#)

[Conceptos sobre puentes](#)

[Configuración del puente](#)

[Utilice un Servidor RADIUS para Asignar Usuarios a VLAN](#)

[Utilizar un servidor RADIUS para la asignación de grupo de movilidad dinámica](#)

[Configuración de grupo de puentes en puntos de acceso y puentes](#)

[Routing y puente integrados \(IRB\)](#)

[Interacción con switches relacionados](#)

[Configuración del switch - Catalyst OS](#)

[Configuración del switch: switches Catalyst basados en IOS](#)

[Configuración de switch - Catalyst 2900XL/3500XL](#)

[Verificación](#)

[Verificar el equipo inalámbrico](#)

[Verificación del switch](#)

[Troubleshoot](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de ejemplo para utilizar las LAN virtuales (VLAN) con el equipo inalámbrico Cisco Aironet.

[Prerequisites](#)

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Familiaridad con el equipo inalámbrico de Cisco Aironet
- Familiaridad con los conceptos de switching LAN de VLAN y VLAN Trunking

Componentes Utilizados

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

- Puntos de acceso Aironet y Puentes inalámbricos de Cisco
- Cisco Catalyst Switches

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.

Productos Relacionados

Puede utilizar el lado del switch de esta configuración con cualquiera de estos hardware o software:

- Catalyst 6x00/5x00/4x00 que ejecuta CatOS o IOS
- Catalyst 35x0/37x0/29xx que ejecuta IOS
- Catalyst 2900XL/3500XL que ejecuta IOS

Convenciones

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

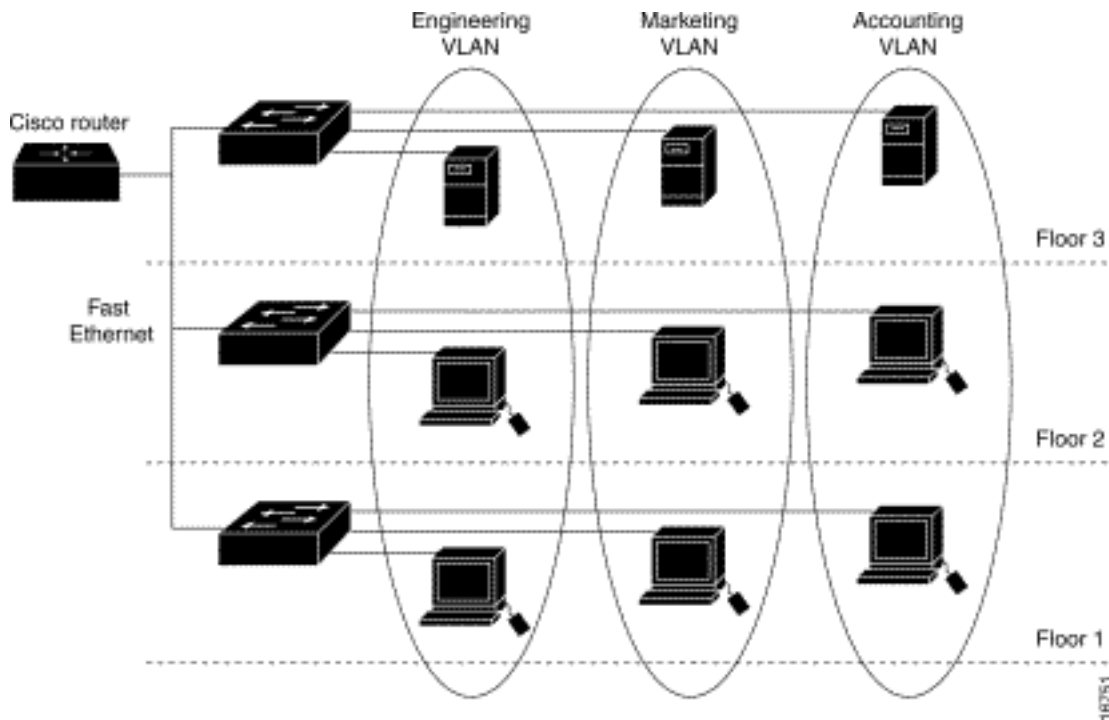
VLAN

Una VLAN es una red conmutada que está segmentada lógicamente por funciones, equipos de proyectos o aplicaciones en lugar de por una base física o geográfica. Por ejemplo, todas las estaciones de trabajo y los servidores utilizados por un equipo de grupo de trabajo determinado se pueden conectar a la misma VLAN, independientemente de sus conexiones físicas a la red o del hecho de que se puedan mezclar con otros equipos. Utilice las VLAN para reconfigurar la red a través del software en lugar de desconectar o mover físicamente los dispositivos o los cables.

Una VLAN se puede considerar como un dominio de broadcast que existe dentro de un conjunto definido de switches. Una VLAN consta de varios sistemas finales, ya sean hosts o equipos de red (como puentes y routers), conectados por un único dominio de conexión en puente. El dominio de conexión en puente se soporta en varios equipos de red, como switches LAN, que operan protocolos de conexión en puente entre ellos con un grupo separado para cada VLAN.

Cuando se conecta un dispositivo a un switch Cisco Catalyst, el puerto donde se conecta el dispositivo es miembro de VLAN 1. La dirección MAC de ese dispositivo es una parte de la VLAN

1. Puede definir múltiples VLAN en un solo switch y puede configurar un puerto de switch en la mayoría de los modelos Catalyst como miembro de múltiples VLAN.



Cuando el número de puertos en una red excede la capacidad del puerto del switch, debe conectar varios chasis de switch, lo que define un trunk. El tronco no es miembro de ninguna VLAN, sino un conducto por el cual pasa el tráfico para una o más VLAN.

En términos fundamentales, la clave en la configuración de un punto de acceso para conectarse a una VLAN específica es configurar su SSID para reconocer esa VLAN. Debido a que las VLAN se identifican mediante un ID o nombre de VLAN, se indica que, si el SSID en un punto de acceso se configura para reconocer un ID o nombre de VLAN específico, se establece una conexión con la VLAN. Cuando se realiza esta conexión, los dispositivos de cliente inalámbricos asociados que tienen el mismo SSID pueden acceder a la VLAN a través del punto de acceso. La VLAN procesa los datos hacia y desde los clientes de la misma manera que procesa los datos hacia y desde las conexiones cableadas. Puede configurar hasta 16 SSID en su punto de acceso, de modo que pueda admitir hasta 16 VLAN. Sólo puede asignar un SSID a una VLAN.

Las VLAN se extienden a una LAN inalámbrica cuando se agrega el reconocimiento de etiquetas IEEE 802.11Q al punto de acceso. Las tramas destinadas a diferentes VLAN son transmitidas por el punto de acceso de forma inalámbrica en diferentes SSID con diferentes claves WEP. Sólo los clientes asociados con esa VLAN reciben esos paquetes. Por el contrario, los paquetes que provienen de un cliente asociado a una VLAN determinada se etiquetan con 802.11Q antes de que se reenvíen a la red por cable.

Por ejemplo, los empleados y los invitados pueden tener acceso a la red inalámbrica de una empresa de forma simultánea y estar separados administrativamente. Una VLAN traza mapas para una SSID y el cliente inalámbrico se asocia al SSID adecuado. En las redes con puentes inalámbricos, puede pasar varias VLAN a través del link inalámbrico para proporcionar conectividad a una VLAN desde ubicaciones separadas.

Si se configura 802.1q en la interfaz FastEthernet de un punto de acceso, el punto de acceso siempre envía señales de mantenimiento en VLAN1 aunque la VLAN1 no esté definida en el punto de acceso. Como resultado, el switch Ethernet se conecta al punto de acceso y genera un mensaje de advertencia. No hay pérdida de funciones ni en el punto de acceso ni en el switch,

pero el registro del switch contiene mensajes sin sentido que pueden hacer que los mensajes más importantes se ajusten y no se vean.

Este comportamiento crea un problema cuando todos los SSID de un punto de acceso están asociados a las redes de movilidad. Si todos los SSID están asociados a las redes de movilidad, el puerto del switch Ethernet al que está conectado el punto de acceso se puede configurar como puerto de acceso. El puerto de acceso se asigna normalmente a la VLAN nativa del punto de acceso, que no necesariamente es VLAN1. Esto hace que el switch Ethernet genere mensajes de advertencia y observe que el tráfico con una etiqueta 802.1q se envía desde el punto de acceso.

Puede eliminar los mensajes excesivos en el switch si inhabilita la función keepalive.

Si ignora puntos menores en estos conceptos cuando implementa VLAN con equipos inalámbricos Cisco Aironet, puede experimentar un rendimiento inesperado, por ejemplo:

- La ausencia de límites permitió las VLAN en el enlace troncal en vez de aquella definida en el dispositivo inalámbrico. Si las VLAN 1, 10, 20, 30 y 40 se definen en el switch pero sólo las VLAN 1, 10 y 30 se definen en el equipo inalámbrico, debe eliminar las otras del puerto del switch troncal.
- Uso indebido de la designación de infraestructura SSID Cuando instale puntos de acceso, asigne solamente el SSID de infraestructura cuando utilice un SSID en: Workgroup Bridge Devices puntos de acceso del repetidor Bridge no raíz Se trata de un error de configuración al designar el SSID de infraestructura para un SSID con sólo ordenadores portátiles inalámbricos para los clientes, y provoca resultados impredecibles. En las instalaciones de puente, sólo puede tener un SSID de infraestructura. El SSID de infraestructura debe ser el SSID que se correlaciona con la VLAN nativa.
- Uso incorrecto o diseño incorrecto de la designación SSID de modo invitado Al definir múltiples SSID/VLAN en el equipo inalámbrico de Cisco Aironet, se puede asignar un (1) SSID como SSID de modo invitado con la transmisión de SSID en radiobalanza 802.11. Los otros SSID no se transmiten. Los dispositivos cliente deben indicar que SSID se debe conectar.
- Falla al reconocer que las VLAN y SSID múltiples indican subredes múltiples de capa 3 del modelo OSI Las versiones obsoletas del software Cisco Aironet permiten vincular varios SSID a una VLAN. Las versiones actuales no lo hacen.
- Fallos de ruteo de Capa 3 del Modelo OSI o diseños incorrectos Cada SSID y su VLAN vinculada deben tener un dispositivo de ruteo y algún origen para dirigir a los clientes, por ejemplo un servidor DHCP o el alcance en un servidor DHCP.
- Error de comprensión o configuración incorrecta de VLAN nativa Los routers y switches que forman la infraestructura física de la red se administran con un método diferente que las PC cliente que se conectan a esa infraestructura física. La VLAN a la que pertenecen estas interfaces de router y de switch se denomina VLAN Nativa (De manera predeterminada, VLAN 1). Los PC cliente son miembros de una VLAN diferente, al igual que los teléfonos IP son miembros de otra VLAN. Las interfaces administrativas del punto de acceso o del puente (interfaz BVI1) se consideran y se enumeran como parte de la VLAN nativa sin importar qué VLAN o SSID pasan a través de ese dispositivo inalámbrico.

[Importancia de VLAN nativa](#)

Cuando utiliza un puerto troncal IEEE 802.1Q, todas las tramas se etiquetan excepto las de la

VLAN configurada como la "VLAN nativa" para el puerto. Las tramas en la VLAN nativa siempre se transmiten sin etiquetar y normalmente se reciben sin etiquetar. Por lo tanto, cuando un AP se conecta al switchport, la VLAN nativa configurada en el AP debe coincidir con la VLAN nativa configurada en el switchport.

Nota: Si hay una discordancia en las VLAN nativas, las tramas se descartan.

Este escenario se explica mejor con un ejemplo. Si la VLAN nativa en el switchport se configura como VLAN 12 y en el AP, la VLAN nativa se configura como VLAN 1, entonces cuando el AP envía una trama en su VLAN nativa al switch, el switch considera que la trama pertenece a VLAN 12 dado que las tramas de la VLAN nativa del AP no se etiquetan. Esto causa confusión en la red y da lugar a problemas de conectividad. Lo mismo sucede cuando el switchport reenvía una trama de su VLAN nativa al AP.

La configuración de VLAN nativa se vuelve aún más importante cuando tiene una configuración de AP repetidor en su red inalámbrica. No puede configurar varias VLAN en los AP repetidores. Los AP repetidores soportan solamente la VLAN nativa. Por lo tanto, la configuración de VLAN nativa en el AP raíz, el puerto del switch al que se conecta el AP y el AP del repetidor deben ser iguales. De lo contrario, el tráfico a través del switch no pasa hacia y desde el punto de acceso del repetidor.

Un ejemplo para el escenario donde la discordancia en la configuración de VLAN nativa del punto de acceso del repetidor puede crear problemas es cuando hay un servidor DHCP detrás del switch al que se conecta el AP raíz. En este caso, los clientes asociados con el AP repetidor no reciben una dirección IP del servidor DHCP porque las tramas (solicitudes DHCP en nuestro caso) de la VLAN nativa del AP repetidor (que no es la misma que el AP raíz y el switch) se descartan.

Además, cuando configure el puerto del switch, asegúrese de que todas las VLAN configuradas en los AP estén permitidas en el puerto del switch. Por ejemplo, si existen VLAN 6, 7 y 8 en el AP (red inalámbrica), las VLAN deben estar permitidas en el puerto de switch. Esto se puede hacer usando este comando en el switch:

```
switchport trunk allowed vlan add 6,7,8
```

De forma predeterminada, un switchport configurado como trunk permite que todas las VLAN pasen a través del puerto trunk. Refiérase a [Interacción con Switches Relacionados](#) para obtener más información sobre cómo configurar el switchport.

Nota: Permitir todas las VLAN en el AP también puede convertirse en un problema en algunos casos, específicamente si es una red grande. Esto puede resultar en una alta utilización de la CPU en los AP. Quite las VLAN en el switch de modo que sólo el tráfico VLAN en el que el AP está interesado pase a través del AP para evitar una CPU alta.

[VLAN en puntos de acceso](#)

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

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice

la [Command Lookup Tool](#) (sólo clientes registrados) .

Conceptos con puntos de acceso

Esta sección trata los conceptos sobre cómo implementar VLAN en los puntos de acceso y hace referencia a este diagrama de red.

En esta red de ejemplo, la VLAN 1 es la VLAN nativa, y las VLAN 10, 20, 30 y 40 existen, y están enlazadas a otro chasis de switch. Sólo las VLAN 10 y 30 se extienden al dominio inalámbrico. La VLAN nativa es necesaria para proporcionar capacidad de administración y autenticación de cliente.

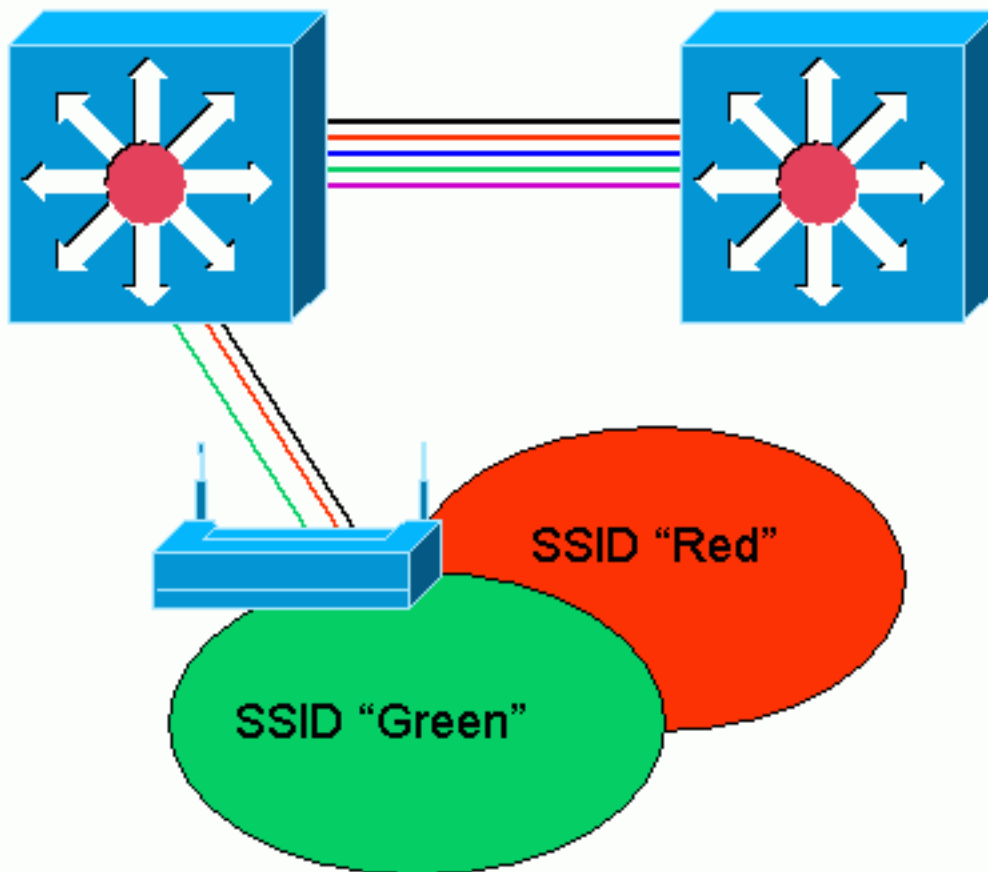
VLAN 1 (Native)

VLAN 10

VLAN 20

VLAN 30

VLAN 40

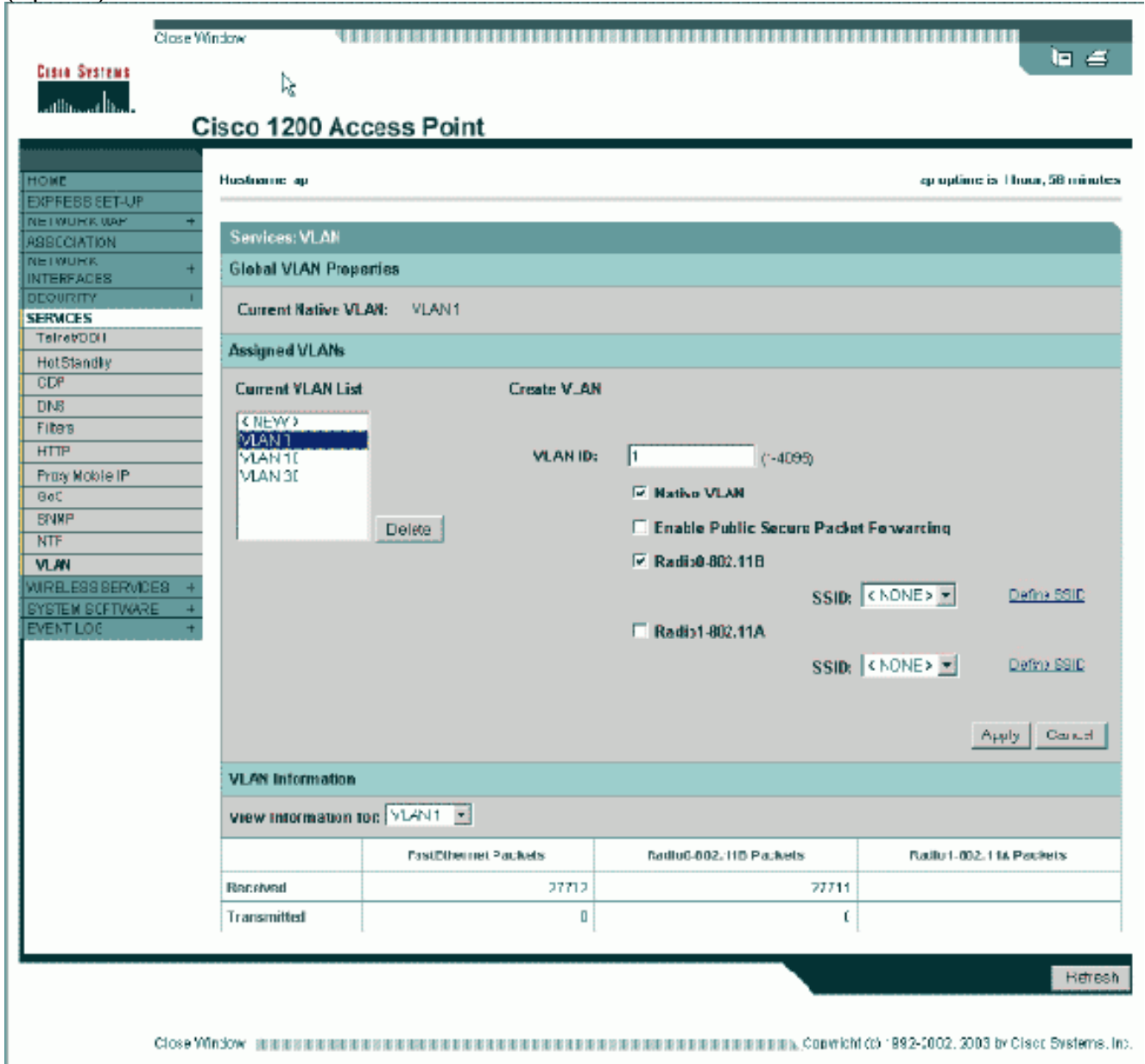


[Configuración del punto de acceso](#)

Para configurar el punto de acceso para las VLAN, complete estos pasos:

1. Desde la GUI de AP, haga clic en Services > VLAN para navegar a los **Servicios: página VLAN** .El primer paso es configurar la VLAN nativa. En Current VLAN List (Lista de VLAN actuales), seleccione **New**.Ingrese el número de VLAN de la VLAN nativa en la casilla de identificación de VLAN. El número de VLAN debe coincidir con la VLAN nativa configurada

en el switch. Debido a que la interfaz BVI 1 está asociada a la subinterfaz de la VLAN nativa, la dirección IP asignada a la interfaz BVI 1 debe estar en la **misma subred IP** que otros dispositivos de infraestructura en la red (es decir, la interfaz SC0 en un switch Catalyst que ejecuta CatOS.) Marque la casilla de verificación correspondiente a la VLAN nativa. Active las casillas de verificación para la interfaz de radio o las interfaces donde se aplica esta VLAN. Haga clic en Apply (Aplicar).

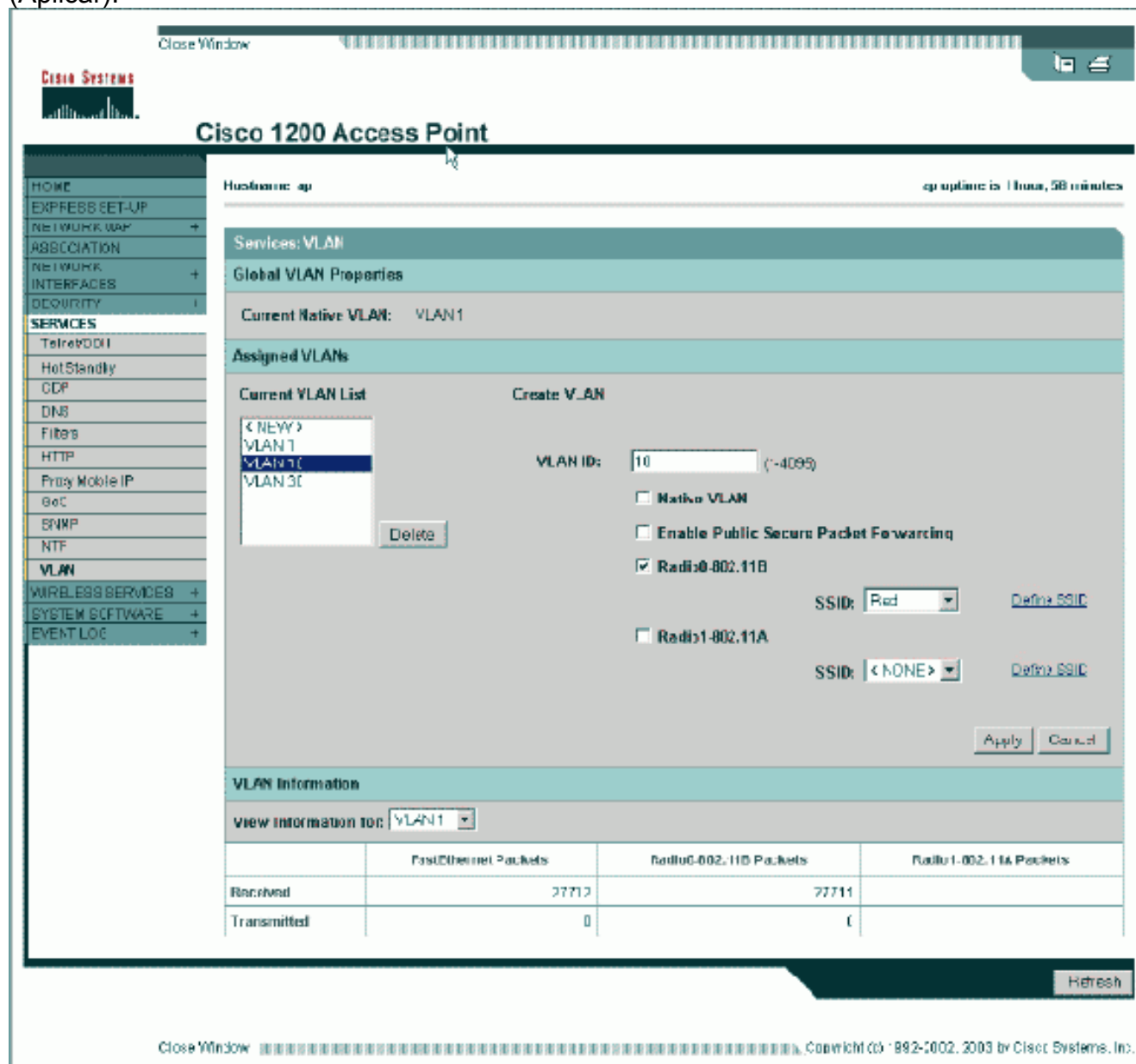


O, desde el CLI, ejecute estos comandos:

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0.1
AP(config-subif)# encapsulation dot1q 1 native
AP(config-subif)# interface FastEthernet0.1
AP(config-subif)# encapsulation dot1q 1 native
AP(config-subif)# end
AP# write memory
```

- Para configurar otras VLAN, siga estos pasos: En Current VLAN List (Lista de VLAN actuales), seleccione **New**. Introduzca el número VLAN de la VLAN deseada en la casilla ID de VLAN. El número de VLAN debe coincidir con una VLAN configurada en el switch. Active

las casillas de verificación para la interfaz de radio o las interfaces donde se aplica esta VLAN. Haga clic en Apply (Aplicar).



O, desde el CLI, ejecute estos comandos:

```
AP# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)# interface Dot11Radio0.10
```

```
AP(config-subif)# encapsulation dot1Q 10
```

```
AP(config-subif)# interface FastEthernet0.10
```

```
AP(config-subif)# encapsulation dot1Q 10
```

```
AP(config-subif)# end
```

```
AP# write memory
```

Repita los pasos 2a a 2d para cada VLAN deseada o ingrese estos comandos desde la CLI con los cambios adecuados en la subinterfaz y los números de VLAN:

```
AP# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)# interface Dot11Radio0.30
```

```
AP(config-subif)# encapsulation dot1Q 30
```

```
AP(config-subif)# interface FastEthernet0.30
```

```
AP(config-subif)# encapsulation dot1Q 30
```

```
AP(config-subif)# end
```


AP# write memory

3. El siguiente paso es asociar las VLAN configuradas a los SSID. Para hacer esto, haga clic en **Security > SSID Manager**.**Nota:** No es necesario asociar cada VLAN definida en el punto de acceso con un SSID. Por ejemplo, por razones de seguridad, la mayoría de las instalaciones de puntos de acceso no asocian un SSID con la VLAN nativa. Para crear un nuevo SSID, elija **New**. Introduzca el SSID deseado (que distingue entre mayúsculas y minúsculas) en el cuadro SSID. Seleccione el número deseado de VLAN para asociar este SSID con la lista desplegable.**Nota:** Para mantener este documento dentro del alcance previsto, no se aborda la seguridad para un SSID. Haga clic en Apply-RadioX para crear el SSID en la radio seleccionada o Apply-all para crearlo en todas las radios.

Close Window

Cisco Systems

Cisco 1200 Access Point

RADIO0-802.11B RADIO1-802.11A

Hostname: ap ap uptime is 1 hour, 59 minutes

Security: SSID Manager - Radio0 802.11B

SSID Properties

Current SSID List

- < NEW >
- Green
- Red**

SSID: Red VLAN: 10 [Define VLANs](#)

Authentication Methods Accepted:

- Open Authentication: < NO ADDITION >
- Shared Authentication: < NO ADDITION >
- Network EAP: < NO ADDITION >

Authenticated Key Management:

- None
- CKM: Mandatory
- WPA: Optional

WPA Pre-shared Key: ASCII Hexadecimal

EAP Client (optional):

Username: Password:

Association Limit (optional): 11-255

- Enable Proxy Mobile IP
- Enable Accounting

Apply-Radius0 Apply-All Cancel

Global Radio0-802.11B SSID Properties

Set Guest Mode SSID: < NONE >

Set Infrastructure SSID: < NONE > Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Close Window

Copyright (c) 1992-2002, 2003 by Cisco Systems, Inc.

O desde la CLI, ejecute estos comandos:

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Red
AP(config-if-ssid)# vlan 10
AP(config-if-ssid)# end
AP# write memory
```

4. Repita los pasos 3a a 3d para cada SSID deseado o ingrese estos comandos desde la CLI con los cambios adecuados al SSID.

```
AP# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.  
AP(config)# interface Dot11Radio0  
AP(config-if)# ssid Green  
AP(config-if-ssid)# vlan 30  
AP(config-if-ssid)# end  
AP# write memory
```

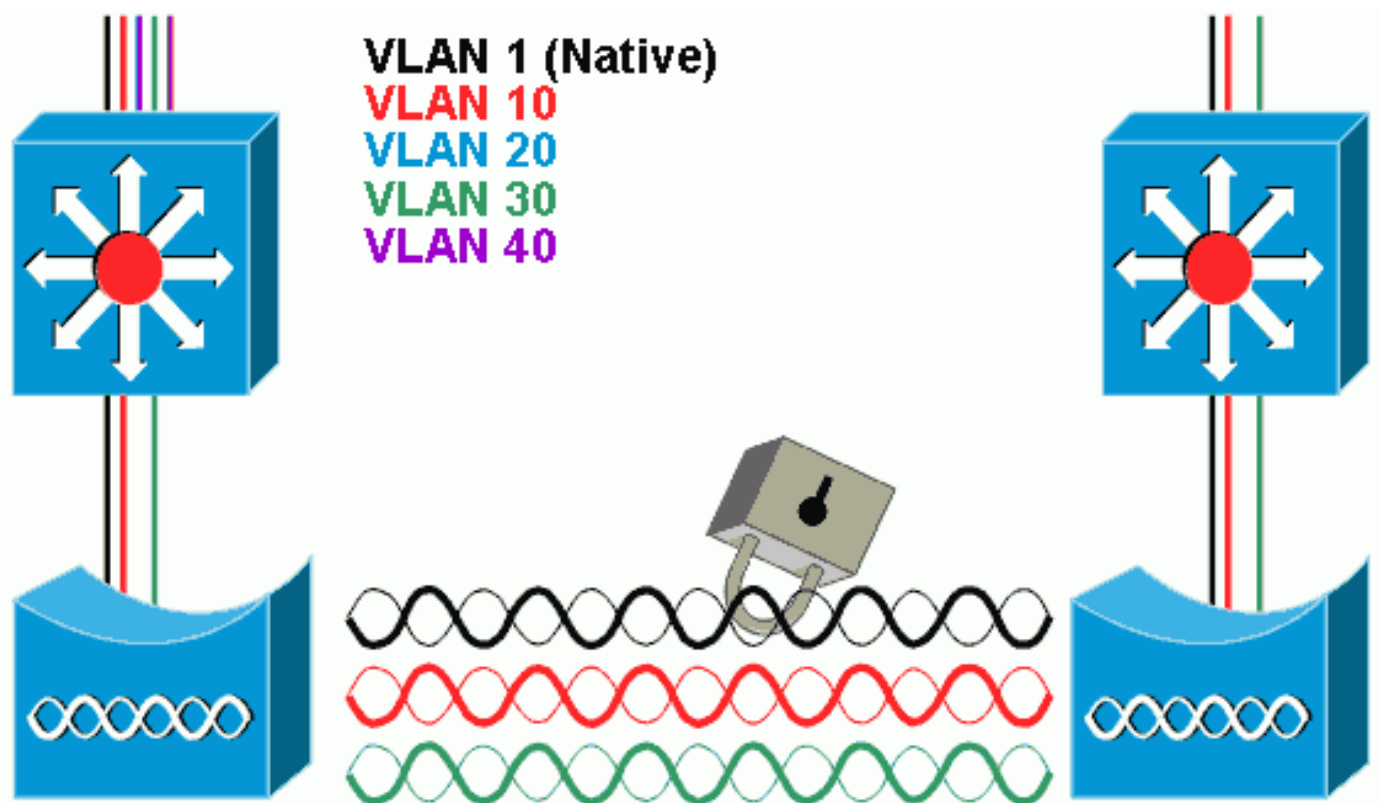
Nota: Estos ejemplos no incluyen autenticación. Se requiere algún tipo de autenticación (Open, Network-EAP) para que los clientes se asocien.

VLAN en puentes

Conceptos sobre puentes

Esta sección trata los conceptos relacionados con cómo implementar las VLAN en los bridges y hace referencia a este diagrama de red.

En esta red de ejemplo, la VLAN 1 es la VLAN nativa, y las VLAN 10, 20, 30 y 40 existen. Sólo las VLAN 10 y 30 se extienden al otro lado del link. El enlace inalámbrico está cifrado.



Para cifrar los datos que pasan por el link de radio, aplique el cifrado sólo al SSID de la VLAN nativa. Ese cifrado se aplica a todas las demás VLAN. Cuando se establece un puente, no hay necesidad de asociar un SSID separado a cada VLAN. Las configuraciones de VLAN son las mismas en los bridges raíz y no raíz.

Configuración del puente

Para configurar el puente para las VLAN, como el diagrama de red de ejemplo, complete estos pasos:

- Desde la GUI de AP, haga clic en **Services > VLAN** para navegar a los **Servicios**: página **VLAN**. El primer paso es configurar la VLAN nativa. Para hacer esto, elija **<New>** de la Lista de VLAN Actuales. Ingrese el número de VLAN de la VLAN nativa en la casilla de identificación de VLAN. Esto debe coincidir con la VLAN nativa configurada en el switch. Debido a que la interfaz BVI 1 está asociada a la subinterfaz de la VLAN nativa, la dirección IP asignada a la interfaz BVI 1 debe estar en la **misma subred IP** que otros dispositivos de infraestructura en la red (es decir, la interfaz SC0 en un switch Catalyst que ejecute CatOS.) Marque la casilla de verificación correspondiente a la VLAN nativa. Haga clic en **Apply** (Aplicar).

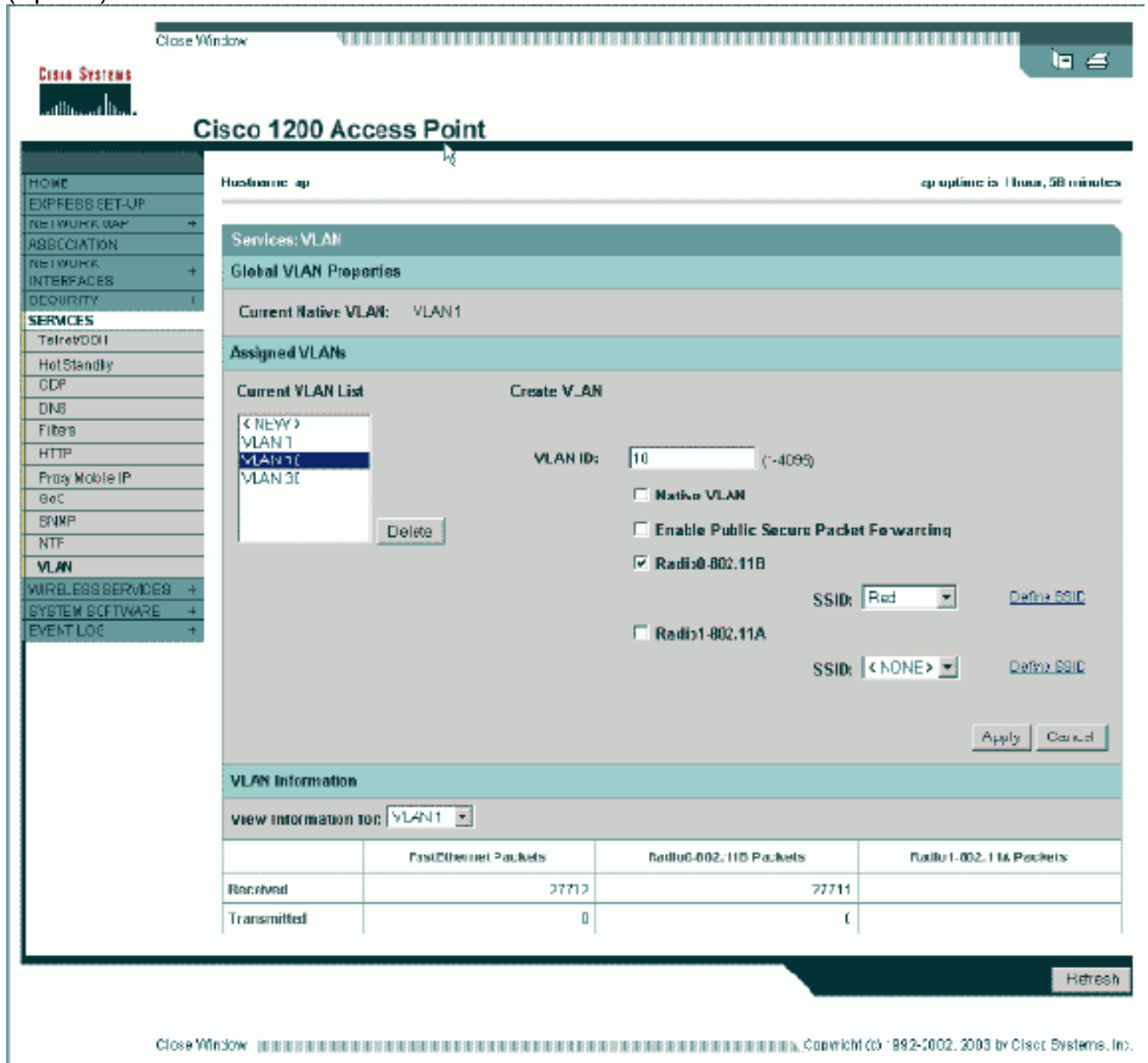
The screenshot shows the Cisco 1200 Access Point GUI. The left sidebar contains a navigation menu with options like HOME, EXPRESS SET-UP, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, and WIRELESS SERVICES. The main content area is titled 'Services: VLAN' and includes sections for 'Global VLAN Properties' (Current Native VLAN: VLAN1) and 'Assigned VLANs'. Under 'Assigned VLANs', there is a 'Current VLAN List' showing '<NEW>', 'VLAN1', 'VLAN10', and 'VLAN30'. The 'Create VLAN' section has 'VLAN ID: 1' and 'Native VLAN' checked. There are also radio options for 802.11B and 802.11A with SSID dropdowns. Buttons for 'Apply' and 'Cancel' are visible. At the bottom, there is a 'VLAN Information' table showing statistics for FastEthernet, Radio 802.11B, and Radio 802.11A.

	FastEthernet Packets	Radio 802.11B Packets	Radio 802.11A Packets
Received	27712	27711	
Transmitted	0	0	

O, desde el CLI, ejecute estos comandos:

```
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# interface Dot11Radio0.1
bridge(config-subif)# encapsulation dot1Q 1 native
bridge(config-subif)# interface FastEthernet0.1
bridge(config-subif)# encapsulation dot1Q 1 native
bridge(config-subif)# end
bridge# write memory
```

2. Para configurar otras VLAN, siga estos pasos: En Current VLAN List (Lista de VLAN actuales), seleccione **New**. Introduzca el número VLAN de la VLAN deseada en la casilla ID de VLAN. El número de VLAN debe coincidir con una VLAN configurada en el switch. Haga clic en Apply (Aplicar).



O, desde el CLI, ejecute estos comandos:

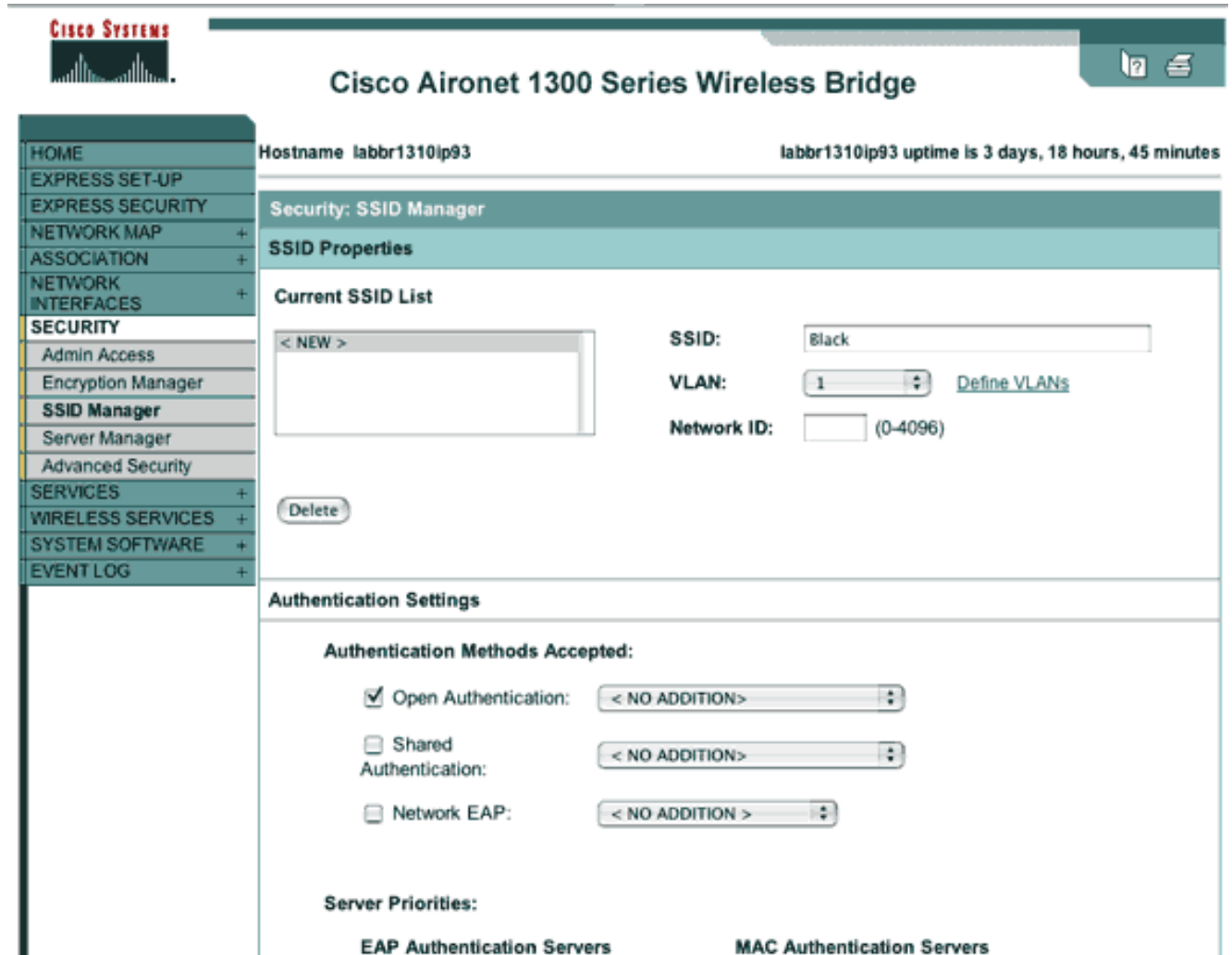
```
bridge# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# interface Dot11Radio0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# interface FastEthernet0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# end
bridge# write memory
```

Repita los pasos 2a a 2c para cada VLAN deseada o ingrese los comandos desde la CLI con los cambios adecuados en la subinterfaz y los números de VLAN.

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
bridge(config)# interface Dot11Radio0.30
bridge(config-subif)# encapsulation dot1Q 30
bridge(config-subif)# interface FastEthernet0.30
```

```
bridge(config-subif)# encapsulation dot1Q 30
bridge(config-subif)# end
bridge# write memory
```

3. Desde el Administrador SSID (en el elemento de menú **Security > SSID Manager**), asocie la VLAN nativa con un SSID. **Nota:** Cuando se establece un puente, el único SSID que debe asociar a una VLAN es el que se correlaciona con la VLAN nativa. Debe designar este SSID como el SSID de infraestructura. En la Lista actual de SSID, seleccione **Nuevo**. Introduzca el SSID deseado (que distingue entre mayúsculas y minúsculas) en el cuadro SSID. Seleccione el número de VLAN que se correlaciona con la VLAN nativa de la lista desplegable. **Nota:** Para mantener este documento dentro del alcance previsto, no se aborda la seguridad para un SSID. Haga clic en **Aplicar** para crear el SSID en la radio y asociarlo a la VLAN nativa.



The screenshot displays the Cisco Aironet 1300 Series Wireless Bridge configuration interface. The top navigation bar includes the Cisco Systems logo and the device name 'Cisco Aironet 1300 Series Wireless Bridge'. The left sidebar shows a menu with categories like HOME, EXPRESS SET-UP, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled 'Security: SSID Manager' and shows the 'SSID Properties' section. Under 'Current SSID List', there is a 'NEW' button and a 'Delete' button. The 'SSID Properties' section includes fields for 'SSID' (Black), 'VLAN' (1), and 'Network ID' (0-4096). Below this is the 'Authentication Settings' section, which includes 'Authentication Methods Accepted' with checkboxes for 'Open Authentication', 'Shared Authentication', and 'Network EAP', each with a dropdown menu set to '< NO ADDITION >'. The 'Server Priorities' section is partially visible at the bottom.

Desplácese hacia atrás hasta la parte inferior de la página, y bajo **Propiedades globales de SSID de Radio0-802.11G** seleccione el **SSID** de la lista desplegable **Establecer SSID de infraestructura**. Haga clic en **Apply** (Aplicar).

Username: Password:

Apply Cancel

Global Radio0-802.11G SSID Properties

Set Guest Mode SSID:

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

Apply Cancel

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

O desde la CLI, ejecute estos comandos:

```
AP# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
AP(config)# interface Dot11Radio0
AP(config-if)# ssid Black
AP(config-if-ssid)# vlan 1
AP(config-if-ssid)# infrastructure-ssid
AP(config-if-ssid)# end
AP# write memory
```

Nota: Cuando las VLAN están en uso, los SSID se configuran bajo la interfaz física Dot11Radio, no bajo ninguna subinterfaz lógica. **Nota:** Este ejemplo no incluye autenticación. Los puentes raíz y no raíz requieren alguna forma de autenticación (Open, Network-EAP, etc.) para asociarse.

[Utilice un Servidor RADIUS para Asignar Usuarios a VLAN](#)

Puede configurar su servidor de autenticación RADIUS para asignar usuarios o grupos de usuarios a una VLAN específica cuando se autentican en la red. Para obtener información sobre esta función, consulte la sección [Uso de un Servidor RADIUS para Asignar Usuarios a VLAN](#) del documento *Guía de Configuración de Cisco IOS Software para Puntos de Acceso Cisco Aironet, 12.4(3g)JA y 12.3(8)JEB*.

[Utilizar un servidor RADIUS para la asignación de grupo de movilidad dinámica](#)

También puede configurar un servidor RADIUS para asignar dinámicamente grupos de movilidad a usuarios o grupos de usuarios. Esto elimina la necesidad de configurar varios SSID en el punto de acceso. En su lugar, debe configurar sólo un SSID por punto de acceso. Para obtener información sobre esta función, refiérase a la sección [Uso de un Servidor RADIUS para la Asignación de Grupo de Movilidad Dinámica](#) del documento *Guía de Configuración de Cisco IOS Software para Puntos de Acceso Cisco Aironet, 12.4(3g)JA y 12.3(8)JEB*.

[Configuración de grupo de puentes en puntos de acceso y puentes](#)

En general, los grupos de bridges crean dominios de conmutación segmentados. El tráfico se

limita a los hosts dentro de cada grupo de puentes, pero no entre los grupos de puentes. El switch reenvía el tráfico solamente entre los hosts que forman el grupo de puentes, lo que restringe el tráfico de difusión y multidifusión (inundación) sólo a esos hosts. Los grupos de puentes alivian la congestión de la red y proporcionan seguridad de red adicional cuando segmentan el tráfico a determinadas áreas de la red.

Refiérase a [Descripción General del Bridging](#) para obtener información detallada.

En una red inalámbrica, los grupos de puentes se configuran en los puntos de acceso y puentes inalámbricos para que el tráfico de datos de una VLAN se transmita desde los medios inalámbricos al lado cableado y viceversa.

Realice este paso desde la CLI del AP para habilitar grupos de bridges globalmente en el punto de acceso/puente.

En este ejemplo, se utiliza el bridge-group número 1.

```
Ap(configure)#bridge 1
```

Nota: Puede numerar sus grupos de puentes de 1 a 255.

Configure la interfaz de radio y la interfaz Fast Ethernet del dispositivo inalámbrico para que estén en el mismo grupo de puentes. Esto crea un trayecto entre estas dos interfaces diferentes, y se encuentran en la misma VLAN con fines de etiquetado. Como resultado, los datos transmitidos desde el lado inalámbrico a través de la interfaz de radio se transmiten a la interfaz Ethernet a la que está conectada la red por cable y viceversa. En otras palabras, las interfaces de radio y Ethernet que pertenecen al mismo grupo de bridges realmente conectan los datos entre ellos.

En un punto de acceso/puente, necesita tener un grupo de puente por VLAN para que el tráfico pueda pasar del cable a la red inalámbrica y viceversa. Cuanta más VLAN tenga que pasar el tráfico a través de la red inalámbrica, más grupos de puentes se necesitarán.

Por ejemplo, si sólo tiene una VLAN para pasar el tráfico a través del lado inalámbrico al lado cableado de su red, configure solamente un grupo de puente desde la CLI del AP/bridge. Si tiene varias VLAN para pasar tráfico del lado inalámbrico al lado cableado y viceversa, configure grupos de puentes para cada VLAN en la subinterfaz de radio, así como la subinterfaz Fast Ethernet.

1. Configure el grupo de bridges en la interfaz inalámbrica con el comando **bridge group dot11radio interface**. Esto es un ejemplo.

```
AP# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
AP(config)# interface Dot11Radio0.1  
Ap(config-subif)# encapsulation dot1q 1 native  
Ap(config-subif)# bridge group 1 !--- Here "1" represents the bridge group number.  
ap(config-subif)# exit
```

2. Configure el grupo de puentes con el mismo número de grupo de puentes ("1" en este ejemplo) en la interfaz Fast Ethernet de modo que el tráfico VLAN 1 se pase a través de la interfaz inalámbrica a este lado cableado y viceversa.

```
Ap(config)# interface fastEthernet0.1  
Ap(config-subif)# encapsulation dot1q 1 native  
Ap(config-subif)# bridge group 1 !--- Here "1" represents the bridge group number.  
Ap(config-subif)# exit
```


Nota: Cuando configura un grupo de bridges en la interfaz de radio, estos comandos se configuran automáticamente.
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
Nota: Cuando configura un grupo de bridges en la interfaz Fast Ethernet, estos comandos se configuran automáticamente.
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled

Routing y puente integrados (IRB)

La integración entre ruteo y bridging permiten rutear un protocolo específico entre las interfaces ruteadas y los grupos de bridges, o rutear un protocolo específico entre grupos de bridges. El tráfico local o no enrutable se puede puentear entre las interfaces puenteadas del mismo grupo de bridges, mientras que el tráfico enrutable se puede rutear a otras interfaces ruteadas o grupos de bridges

Con el ruteo y el bridging integrados, puede hacer lo siguiente:

- Conmutar paquetes de una interfaz puenteadada a una interfaz ruteada
- Conmutar paquetes de una interfaz ruteada a una interfaz puenteadada
- Conmutación de paquetes dentro del mismo grupo de bridges

Habilite IRB en los puntos de acceso y puentes inalámbricos para rutear el tráfico entre grupos de puentes o entre interfaces ruteadas y grupos de puentes. Necesita un router externo o un switch de Capa 3 para rutear entre grupos de bridges o entre grupos de bridges e interfaces ruteadas.

Ejecute este comando para habilitar IRB en el AP/bridge.

AP(configure)#bridge irb

El routing y el puente integrados utilizan el concepto de interfaz virtual de grupo de puente (BVI) para enrutar el tráfico entre las interfaces enrutadas y los grupos de puente o entre los grupos de puente.

Una BVI es una interfaz virtual dentro del router de switch de Capa 3 que actúa como una interfaz ruteada normal. Una BVI no soporta el bridging pero en realidad representa el grupo de bridge correspondiente a las interfaces ruteadas dentro del router de switch de Capa 3. Tiene todos los atributos de capa de red (como una dirección de capa de red y filtros) que se aplican al grupo de puente correspondiente. El número de interfaz asignado a esta interfaz virtual corresponde al grupo de bridges que representa esta interfaz virtual. Este número es el link entre la interfaz virtual y el grupo de bridges.

Realice estos pasos para configurar el BVI en los puntos de acceso y puentes.

1. Configure el BVI y asigne el número correspondiente del grupo de puentes al BVI. En este ejemplo, se asigna el bridge group número 1 a la BVI.

```
Ap(configure)#interface BVI 1
AP(config-if)#ip address 10.1.1.1 255.255.0.0 !--- Assign an IP address to the BVI.
Ap(config-if)#no shut
```

2. Habilite una BVI para aceptar y rutear los paquetes ruteables que recibe de su bridge group correspondiente.

```
Ap(config)# bridge 1 route ip!---
```

```
!--- This example enables the BVI to accept and route the IP packet.
```

Es importante comprender que sólo necesita una BVI para la administración/VLAN nativa en la que se encuentra el AP (en este ejemplo, VLAN 1). No necesita una BVI para ninguna otra subinterfaz, independientemente de cuántas VLAN y grupos de puente configure en su AP/bridge. Esto se debe a que etiqueta el tráfico en todas las demás VLAN (excepto la VLAN nativa) y lo envía al switch a través de una interfaz troncal dot1q en el lado cableado. Por ejemplo, si tiene 2 VLAN en su red, necesita dos grupos de puente, pero sólo un correspondiente BVI de la VLAN de administración es suficiente en su red inalámbrica. Cuando habilita el ruteo para un protocolo dado en la interfaz virtual del grupo de bridges, los paquetes que vienen de una interfaz ruteada pero están destinados a un host en un dominio puenteado, se rutean a la interfaz virtual del grupo de bridges y se reenvían a la interfaz puenteada correspondiente. Todo el tráfico que se rutea a la interfaz virtual del grupo de bridges se reenvía al grupo de bridges correspondiente como tráfico puenteado. Todo el tráfico enrutable recibido en una interfaz puenteada se rutea a otras interfaces ruteadas como si viniera directamente de la interfaz virtual del grupo de bridges. Refiérase a [Configurar Bridging](#) para obtener información más detallada sobre bridging e IRB.

[Interacción con switches relacionados](#)

En esta sección, se le presenta la información para configurar o verificar la configuración de los switches Cisco que se conectan al equipo inalámbrico Cisco Aironet.

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la [Command Lookup Tool](#) ([sólo](#) clientes registrados) .

[Configuración del switch - Catalyst OS](#)

Para configurar un switch que ejecuta Catalyst OS en VLAN troncales a un punto de acceso, la sintaxis del comando se establece `trunk <module #/port #> en dot1q` y `set trunk <module #/port #> <vlan list>`.

Un ejemplo de al diagrama de red de ejemplo es:

```
set trunk 2/1 on dot1q
set trunk 2/1 1,10,30
```

[Configuración del switch: switches Catalyst basados en IOS](#)

Desde el modo de configuración de la interfaz, ingrese estos comandos, si desea:

- Configure el switchport a las VLAN troncales a un punto de acceso
- En un switch Catalyst que ejecuta IOS
- El CatIOS incluye pero no se limita a: 6 x 004x0035x0295 veces

```
switchport mode trunk
```

```
switchport trunk encapsulation dot1q
switchport nonegotiate
switchport trunk native vlan 1
switchport trunk allowed vlan add 1,10,30
```

Nota: El equipo inalámbrico Cisco Aironet basado en IOS no admite el protocolo de enlace troncal dinámico (DTP), por lo que el switch no debe intentar negociarlo.

Configuración de switch - Catalyst 2900XL/3500XL

Desde el modo de configuración de la interfaz, ingrese estos comandos, si desea configurar el switchport a las VLAN troncales a un punto de acceso en un switch Catalyst 2900XL o 3500XL que ejecute IOS:

```
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,10,30
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Verificar el equipo inalámbrico

- **show vlan:** muestra todas las VLAN configuradas actualmente en el punto de acceso y su estado

```
ap#show vlan
```

```
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)
```

```
vLAN Trunk Interfaces: FastEthernet0.1
Dot11Radio0.1
Virtual-Dot11Radio0.1
```

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

```
FastEthernet0
Dot11Radio0
Virtual-Dot11Radio0
```

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 1	36954	0
Bridging	Bridge Group 1	36954	0

```
Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)
```

```
vLAN Trunk Interfaces: FastEthernet0.10
Dot11Radio0.10
Virtual-Dot11Radio0.10
```

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 10	5297	0
Bridging	Bridge Group 10	5297	0
Bridging	Bridge Group 10	5297	0

Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation)

vLAN Trunk Interfaces: FastEthernet0.30
Dot11Radio0.30
Virtual-Dot11Radio0.30

Protocols Configured:	Address:	Received:	Transmitted:
Bridging	Bridge Group 30	5290	0
Bridging	Bridge Group 30	5290	0
Bridging	Bridge Group 30	5290	0

ap#

- **show dot11 associations**—Muestra información acerca de los clientes relacionados por SSID/VLAN

ap#**show dot11 associations**

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others: (not related to any ssid)

ap#

Verificación del switch

- En un switch basado en Catalyst OS, **show trunk <module #/port #>** —muestra el estado de un trunk en un puerto dado

Console> (enable) show trunk 2/1

* - indicates vtp domain mismatch

Port	Mode	Encapsulation	Status	Native vlan
2/1	on	dot1q	trunking	1

Port Vlans allowed on trunk

2/1 1,10,30

Port Vlans allowed and active in management domain

2/1 1,10,30

Port Vlans in spanning tree forwarding state and not pruned

2/1 1,10,30

Console> (enable)

- En un switch basado en IOS, **show interface fastethernet <module #/port #> trunk**—muestra el estado de un trunk en una interfaz dada

2950g#show interface fastEthernet 0/22 trunk

Port	Mode	Encapsulation	Status	Native vlan
Fa0/22	on	802.1q	trunking	1

Port Vlans allowed on trunk

Fa0/22 1,10,30

Port Vlans allowed and active in management domain

Fa0/22 1,10,30

```
Port          Vlans in spanning tree forwarding state and not pruned
Fa0/22        1,10,30
2950gA#
```

- En un switch Catalyst 2900XL/3500XL, **show interface fastethernet <module #/port #> switchport**—muestra el estado de un trunk en una interfaz dada

```
cat3524xl#show interface fastEthernet 0/22 switchport
Name: Fa0/22
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1,10,30,1002-1005
Trunking VLANs Active: 1,10,30
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
Appliance trust: none
Self Loopback: No
wlan-cat3524xl-a#
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Configuración de las VLAN \(Pautas de configuración del punto de acceso\)](#)
- [Configuración de VLAN \(Guía de Configuración de Bridge\)](#)
- [Soporte técnico de conexión troncal](#)
- [Interacción con switches relacionados](#)
- [Requisitos del Sistema para Implementar el Trunking](#)
- [Descripción General del Bridging](#)
- [Ejemplo de Configuración de Tipos de Autenticación Inalámbrica en un ISR Fijo](#)
- [Ejemplo de Configuración de Tipos de Autenticación Inalámbrica en ISR Fijo a través de SDM](#)
- [Ejemplo de configuración de conectividad de LAN inalámbrica mediante un ISR con encriptación WEP y autenticación LEAP](#)
- [Ejemplo de Configuración de Conexión LAN de Elementos Básicos de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)