Usando los VLA N con el equipo del Aironet de red inalámbrica de Cisco

Contenido

Introducción

Este documento proporciona a una configuración de muestra para utilizar los LAN virtuales (VLA N) con el equipo del Aironet de red inalámbrica de Cisco.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Familiaridad con el equipo del Aironet de red inalámbrica de Cisco
- Familiaridad con los conceptos del Switching de LAN de VLA N y de enlace del VLA N

Componentes Utilizados

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

- Puntas de acceso Aironet de Cisco y puentes inalámbricos
- Switches del Cisco Catalyst

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.

Productos relacionados

Usted puede utilizar el lado del conmutador de esta configuración con ninguno de estos soporte físico o software:

- Catalizador 6x00/5x00/4x00 que funciona con CatOS o el IOS
- Catalizador 35x0/37x0/29xx que funciona con el IOS
- Catalizador 2900XL/3500XL que funciona con el IOS

Convenciones

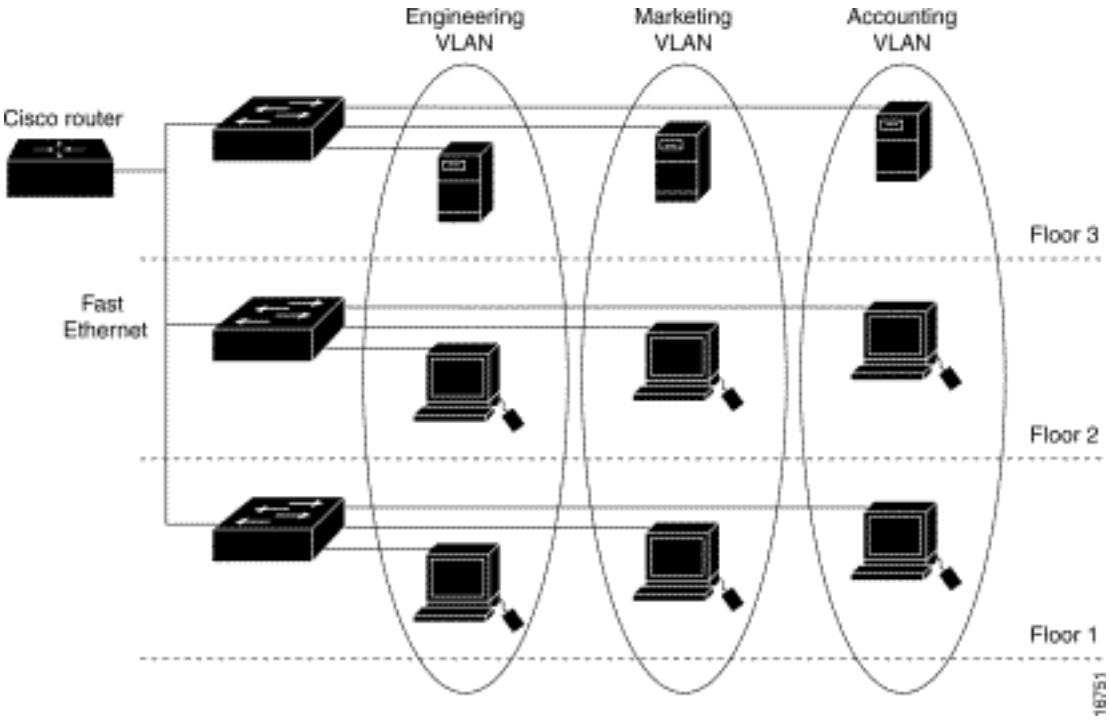
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

VLA N

UN VLA N es una red de switch que es dividida en segmentos lógicamente por las funciones, los equipos de proyecto, o las aplicaciones bastante que en una comprobación o un de modo geográfico. Por ejemplo, todos los puestos de trabajo y servidores usados por un equipo determinado del grupo de trabajo se pueden conectar con el mismo VLA N, sin importar sus conexiones físicas a la red o al hecho de que pueden ser mezclados con otros equipos. Los VLA N del uso para configurar de nuevo la red a través del software bastante que desenchufan o mueven físicamente los dispositivos o los alambres.

UN VLA N se puede pensar en como dominio de broadcast que exista dentro de un conjunto definido de Switches. UN VLA N consiste en varios sistemas de extremo, los host o equipo de red (tal como puentes y Routers), conectado por un solo dominio que puentea. El dominio que puentea se utiliza en los diversos pedazos de equipo de red, tales como Switches LAN, que actúa puentear los protocolos entre ellos con un grupo separado para cada VLA N.

Cuando usted conecta un dispositivo con un conmutador del Cisco Catalyst, el puerto donde el dispositivo está conectado es un miembro de VLAN 1. La dirección MAC de ese dispositivo es un VLA N 1. de la parte de. 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 conmutador, usted debe cruz-conectar el chasis de switch múltiple, que define un tronco. El tronco no es un miembro de ningún VLA N, solamente un conducto sobre quien trafica los pasos para uno o más VLA N.

En los términos fundamentales, la clave en la configuración de un Punto de acceso a conectar con un VLA N específico es configurar su SSID para reconocer ese VLA N. Porque los VLA N son identificados por una identificación del VLA N o un nombre, sigue que, si el SSID en un Punto de acceso se configura para reconocer una identificación del VLA N o un nombre específica, una conexión al VLA N está establecida. Cuando se hace esta conexión, los dispositivos de red inalámbrica de cliente asociados que tienen el mismo SSID pueden tener acceso al VLA N a través del Punto de acceso. El VLA N procesa los datos a y desde los clientes la misma manera que procesa los datos a y desde las conexiones alámbricas. Usted puede configurar hasta 16 SSID en su Punto de acceso, así que usted puede utilizar hasta 16 VLA N. Usted puede asignar solamente un SSID a un VLA N.

Usted amplía los VLA N en un LAN de la Tecnología inalámbrica cuando usted agrega la conciencia de la etiqueta de IEEE 802.11Q al Punto de acceso. Los capítulos destinados para diversos VLA N son transmitidos por el Punto de acceso sin hilos en diversos SSID con diversas claves WEP. Solamente los clientes asociados a ese VLA N reciben esos paquetes. Inversamente, los paquetes que vienen de un cliente asociado a cierto VLA N son 802.11Q marcados con etiqueta antes de que se remitan sobre la red alámbrica.

Por ejemplo, los empleados y los invitados pueden tener acceso a la red inalámbrica de una compañía al mismo tiempo y ser administrativo separados. UN VLA N asocia a un SSID, y a los attaches del cliente de red inalámbrica al SSID apropiado. En las redes con los puentes inalámbricos, usted puede pasar los VLAN múltiples a través del link de red inalámbrica para proporcionar a la Conectividad a un VLA N de las ubicaciones separadas.

Si 802.1q se configura en la interfaz FastEthernet de un Punto de acceso, el Punto de acceso

envía siempre el Keepalives en VLAN1 incluso si el VLA N 1 no se define en el Punto de acceso. Como consecuencia, el conmutador de los Ethernetes conecta con el Punto de acceso y genera un mensaje de advertencia. No hay pérdida de función en el Punto de acceso o el conmutador, pero el registro del switch seleccionar contiene los mensajes sin setido que pueden hacer mensajes más importantes ser envuelto y no ser considerado.

Este comportamiento crea un problema cuando todos los SSID en un Punto de acceso se asocian a las redes de la movilidad. Si todos los SSID se asocian a las redes de la movilidad, el puerto de un switch de Ethernet con el cual el Punto de acceso está conectado se pueden configurar como puerto de acceso. El puerto de acceso se asigna normalmente al VLA N nativo del Punto de acceso, que no es necesariamente VLAN1. Esto hace el conmutador de los Ethernetes generar los mensajes de advertencia que observan que el tráfico con una etiqueta 802.1q está enviado del Punto de acceso.

Usted puede eliminar los mensajes excesivos en el conmutador si usted inhabilita la función de keepalive.

Si usted ignora los puntos casi insignificantes en estos conceptos cuando usted despliega los VLA N con el equipo del Aironet de red inalámbrica de Cisco, usted puede experimentar el funcionamiento inesperado, por ejemplo:

- El error limitar permitió los VLA N en el tronco a ésos definidos en el dispositivo de red inalámbricaSi los VLA N 1, 10, 20, 30 y 40 se definen en el conmutador, pero solamente los VLA N 1, 10 y 30 se definen en el equipo de red inalámbrica, usted deben quitar los otros del switch de puerto troncal.
- Uso erróneo de la designación de la infraestructura SSIDCuando usted instala los Puntos de acceso, sólo asigne la infraestructura SSID cuando usted utiliza un SSID encendido:dispositivos del puente del grupo de trabajoPuntos de acceso del repetidorpuentes de la no-raízEs un misconfiguration para señalar la infraestructura SSID para un SSID con solamente las laptopes inalámbricas para los clientes, y causa los resultados no predecibles.En las instalaciones del puente, usted puede solamente tener una infraestructura SSID. La infraestructura SSID debe ser el SSID que correlaciona al VLA N nativo.
- Uso erróneo o diseño incorrecto de designación SSID del modo de invitadoCuando usted define los SSID/los VLA N múltiples en el equipo del Aironet de red inalámbrica de Cisco, un (1) SSID se puede asignar como modo de invitado SSID con la difusión SSID en las radiobalizas del 802.11. Los otros SSID no son difusión. Los dispositivos cliente deben indicar qué SSID a conectar.
- Error reconocer que los VLAN múltiples y los SSID indican las subredes múltiples de la capa 3 del modelo de OSILas versiones desaprobadas del software de Cisco Aironet permiten atar los SSID múltiples a un VLA N. Las versiones actuales no hacen.
- Errores de encaminamiento de la capa 3 del modelo de OSI o diseños incorrectosCada SSID y su VLA N conectado deben tener un dispositivo de la encaminamiento y cierta fuente para dirigirse a los clientes, por ejemplo un servidor del DHCP o el alcance en un servidor del DHCP.
- Entienda mal o configure incorrectamente el VLA N nativoManejan al Routers y el Switches que componen la Infraestructura física de una red en un método distinto que las PC del cliente que asocian a esa Infraestructura física. El VLA N este router y las interfaces del switch es miembros de se llama el VLA N nativo (por abandono, el VLA N 1). Las PC del cliente son miembros de un diverso VLA N, apenas pues los teléfonos IP son miembros de otro VLA N. El interfaz administrativo del Punto de acceso o el puente (interfaz BVI1) se

considera y numeró a una parte del VLA N nativo sin importar qué VLA N o SSID pasan a través de ese dispositivo de red inalámbrica.

Significación del VLA N nativo

Cuando usted utiliza un puerto de tronco 802.1q de IEEE, todos los marcos se marcan con etiqueta a menos que ésos en el VLA N configurado como el “VLA N nativo” para el puerto. Los capítulos en el VLA N nativo son siempre untagged transmitido y normalmente se reciben untagged. Por lo tanto, cuando un AP está conectado con el switchport, el VLA N nativo configurado en el AP debe hacer juego el VLA N nativo configurado en el switchport.

Nota: Si hay una discordancía en los VLA N nativos, se caen los marcos.

Este decorado se explica mejor con un ejemplo. Si el VLA N nativo en el switchport se configura como VLA N 12 y en el AP, el VLA N nativo se configura como VLA N 1, después cuando el AP envía un marco en su VLA N nativo al conmutador, el conmutador considera el marco como perteneciendo al VLA N 12 puesto que los marcos del VLA N nativo del AP son untagged. Esto causa la confusión en la red y los resultados en los problemas de conectividad. Lo mismo sucede cuando el switchport adelante un marco de su VLA N nativo al AP.

La configuración del VLA N nativo llega a ser aún más importante cuando usted hace un AP de repetidor poner en su red inalámbrica. Usted no puede configurar los VLAN múltiples en el repetidor APs. El repetidor APs utiliza solamente el VLA N nativo. Por lo tanto, la configuración de VLAN nativa en el AP raíz, el puerto del switch con el cual el AP está conectado, y el AP de repetidor, debe ser lo mismo. Si no el tráfico a través del conmutador no pasa a y desde el AP de repetidor.

Un ejemplo para el decorado donde la discordancía en la configuración de VLAN nativa AP del repetidor puede crear los problemas está cuando hay un servidor del DHCP detrás del conmutador con el cual el AP raíz está conectado. En este caso los clientes asociados al AP de repetidor no reciben una dirección IP del servidor del DHCP porque los marcos (solicitudes del DHCP en nuestro caso) del VLA N nativo AP del repetidor (que no es lo mismo que el AP raíz y el conmutador) se caen.

También, cuando usted configura el puerto del switch, *asegúrese de que todos los VLA N que se configuran en los APs estén permitidos en el switchport.* Por ejemplo, si los VLA N 6, 7, y 8 existen en el AP (red inalámbrica) los VLA N tienen que ser permitidos en el switchport. Esto se puede hacer usando este comando en el conmutador:

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

Por abandono, un switchport configurado como tronco permite que todos los VLA N pasen a través del puerto troncal. Refiera a la interacción con el Switches relacionado para más información sobre cómo configurar el switchport.

Nota: Permitir todos los VLA N en el AP puede también convertirse en un problema en algunos casos, específicamente si es una Red grande. Esto puede dar lugar CPU elevada a la utilización en los APs. Pode los VLA N en el conmutador de modo que solamente el tráfico del VLA N que el AP está interesado en los pasos con el AP evitar CPU elevada.

VLA N en los Puntos de acceso

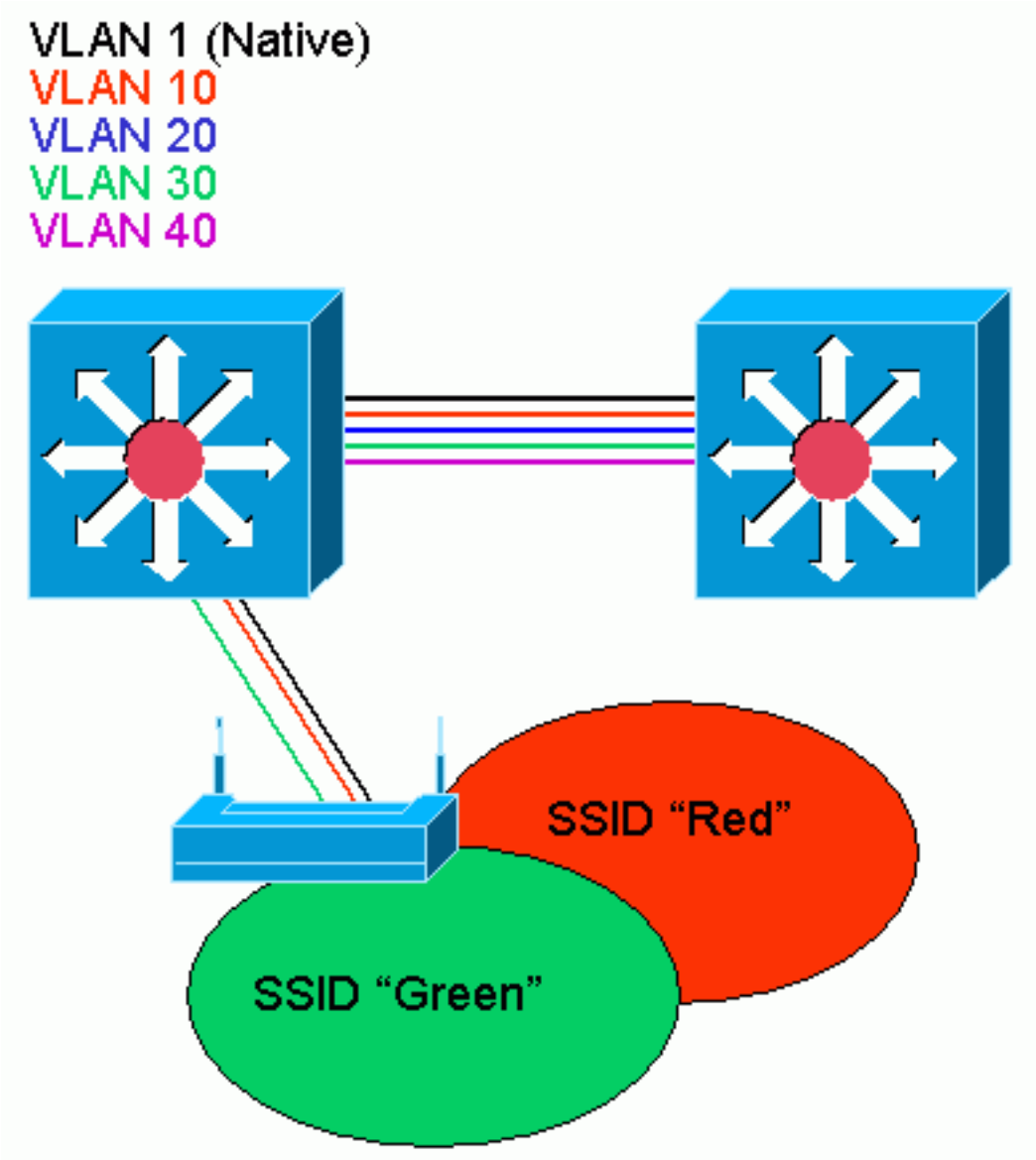
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para encontrar la información adicional en los comandos usados en este documento, use la Command Lookup Tool (clientes registrados solamente).

Conceptos con los Puntos de acceso

Esta sección discute los conceptos sobre cómo desplegar los VLA N en los Puntos de acceso y refiere a este diagrama de la red.

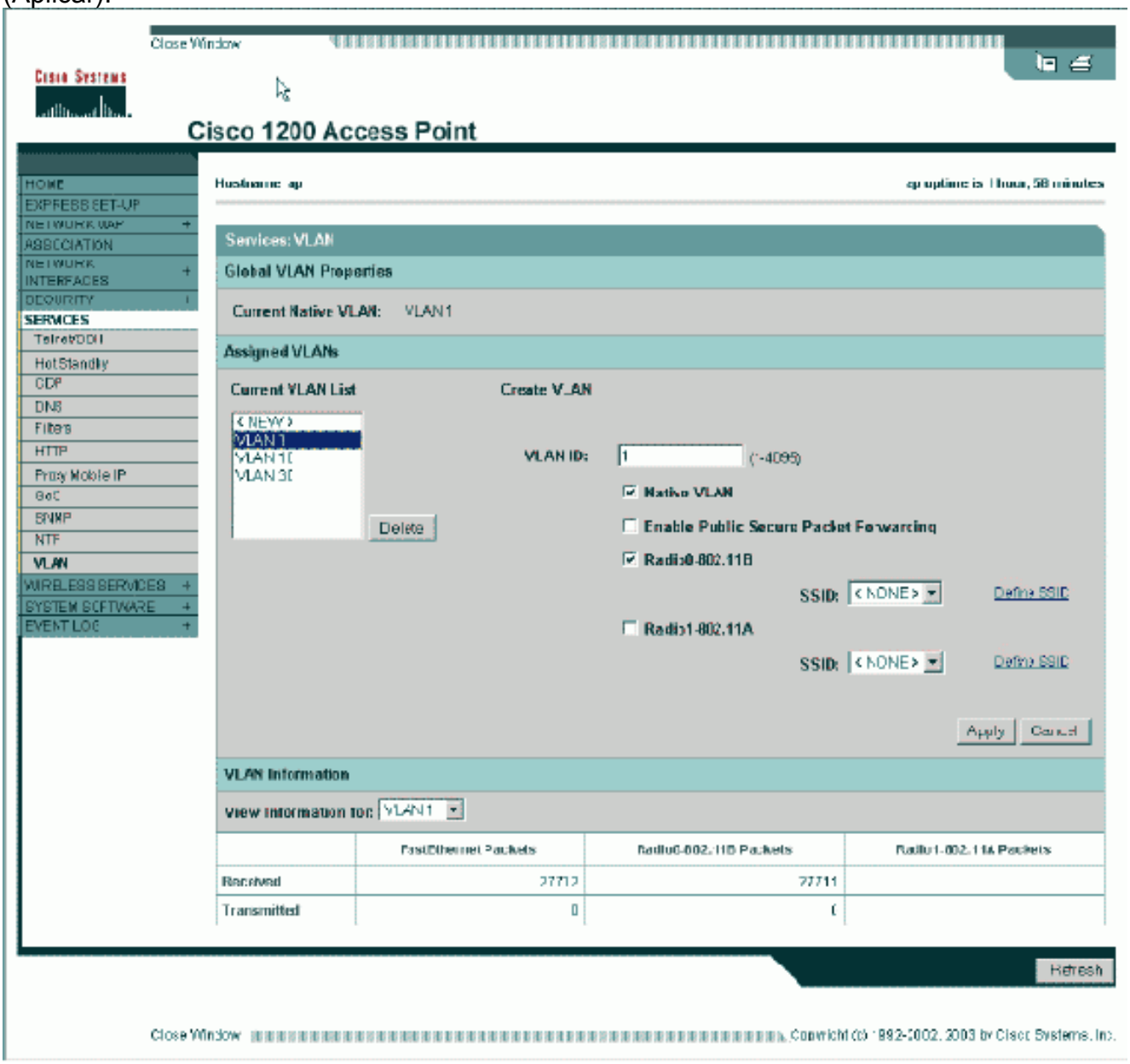
En esta red de muestra, el VLA N 1 es el VLA N nativo, y los VLA N 10, 20, 30 y 40 existen, y son trunked a otro chasis del switch. Solamente los VLA N 10 y 30 son extendidos en el dominio de red inalámbrica. El VLA N nativo se requiere para proporcionar a las autenticaciones de la capacidad de administración y de cliente.



Configuración de punto de acceso

Para configurar el Punto de acceso para los VLA N, complete estos pasos:

1. Del GUI AP, haga clic los servicios > el VLA N a navegar a los **servicios:** Página del **VLA N**.El primer paso es configurar el VLA N nativo. De la lista actual del VLA N, seleccione **nuevo**.Ingrese el número del VLA N del VLA N nativo en el rectángulo identificación del VLA N. El número del VLA N debe hacer juego el VLA N nativo configurado en el conmutador.Porque el interfaz BVI 1 se asocia al subinterface del VLA N nativo, la dirección IP asignada para interconectar BVI 1 debe estar en la **misma subred IP** que otros dispositivos de infraestructura en la red (es decir, el interfaz SC0 en un conmutador del catalizador que ejecuta CatOS.)Marque la casilla de verificación correspondiente a la VLAN nativa.Seleccione las casillas de verificación para la interfaz radio o los interfaces donde este VLA N se aplica.Haga clic en Apply
(Aplicar).

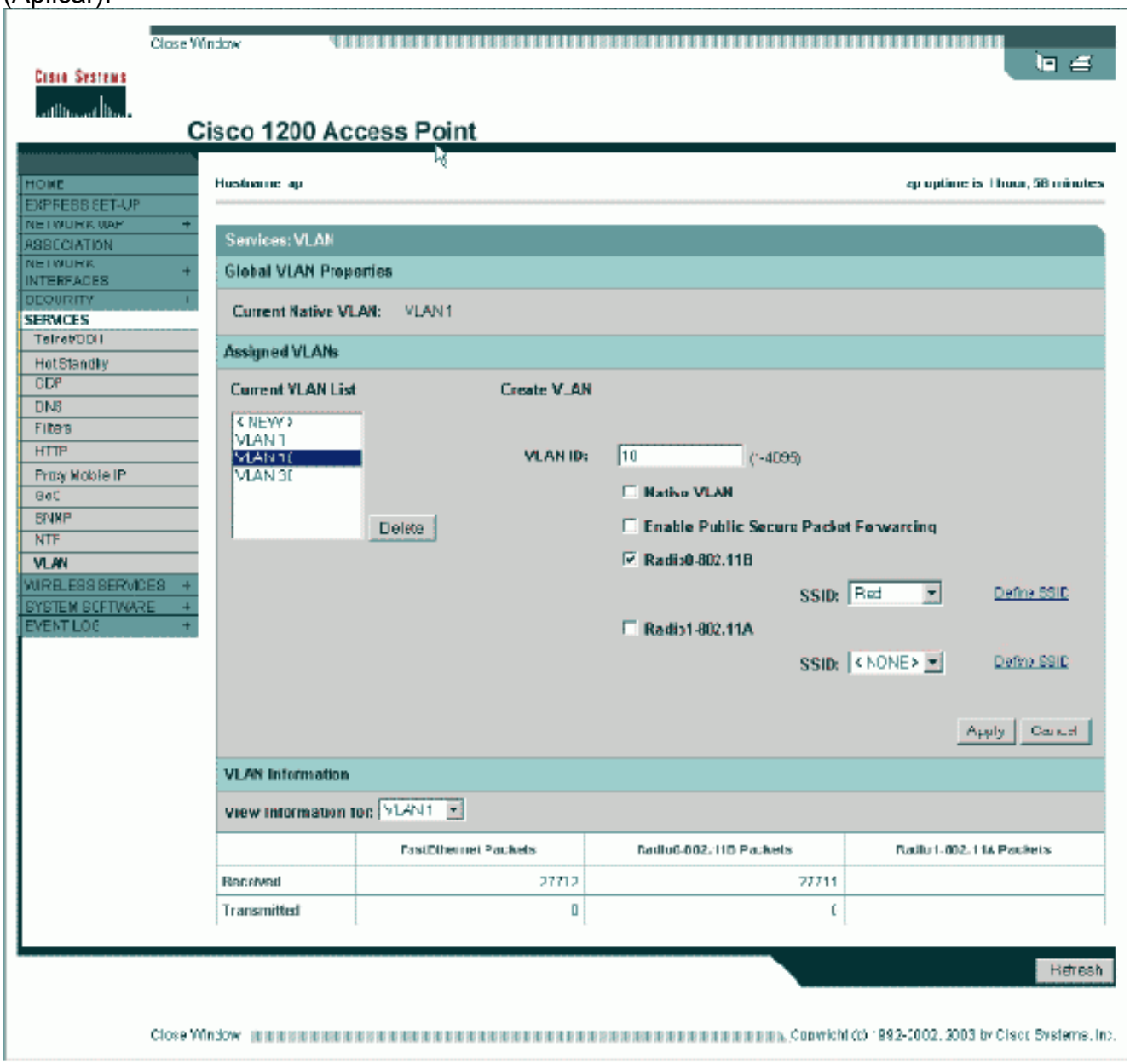


O, desde el CLI, ejecute estos comandos:

```
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
```

2. Para configurar otros VLA N, siga los siguientes pasos:De la lista actual del VLA N, seleccione **nuevo**.Ingrese el número del VLA N del VLA N deseado en el rectángulo identificación del VLA N. El número del VLA N debe hacer juego un VLA N configurado en el conmutador.Seleccione las casillas de verificación para la interfaz radio o los interfaces donde este VLA N se aplica.Haga clic en Apply (Aplicar).



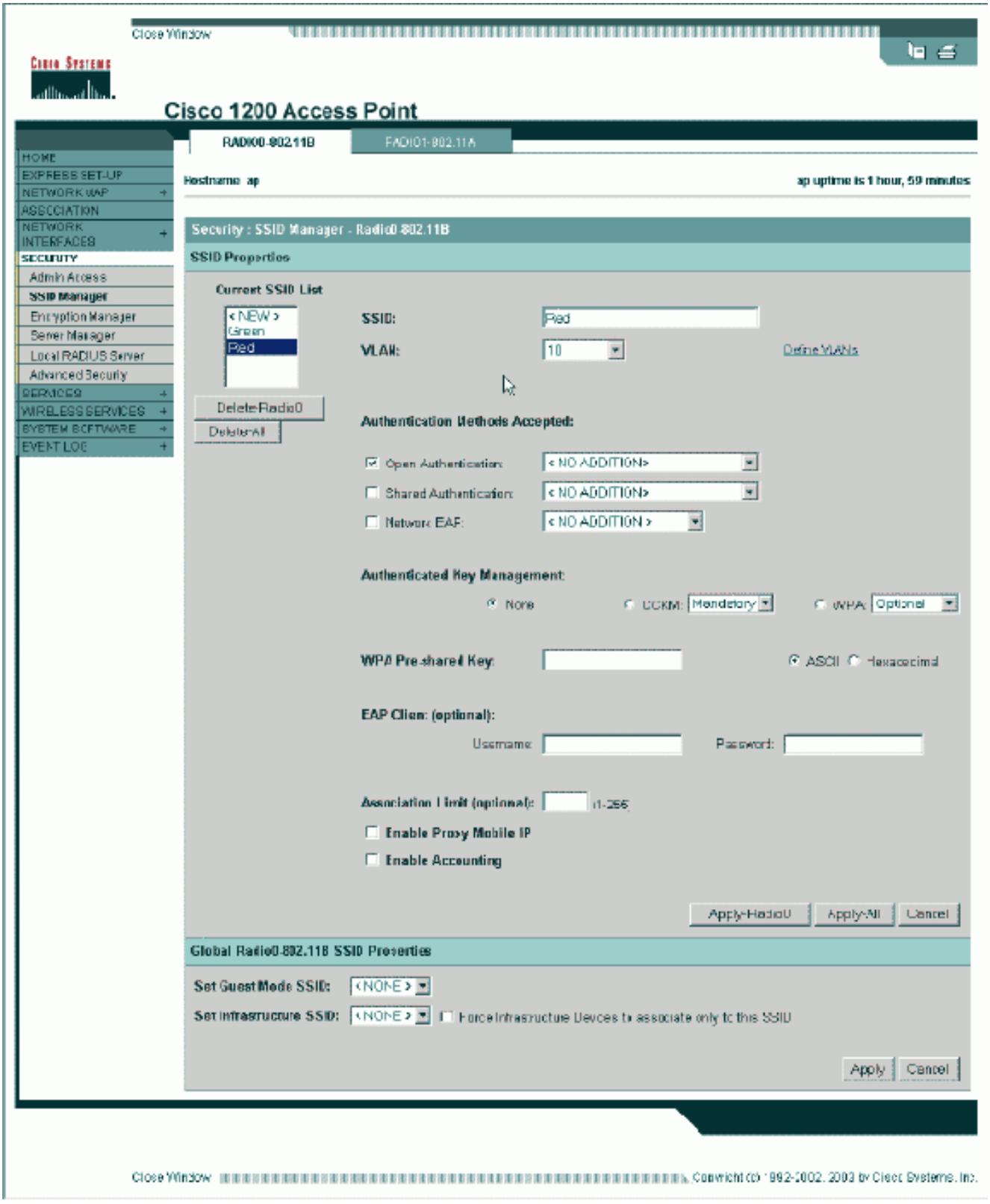
O, desde el CLI, ejecute estos comandos:

```
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
```

Relance los pasos 2a con el 2.o para cada VLA N deseado o ingrese estos comandos del CLI con los cambios apropiados al subinterface y a los números del VLA N:

```
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 los VLA N configurados a los SSID. Para hacer esto, **Seguridad del** tecleo **> administrador SSID**.**Nota:** Usted no necesita asociar cada VLA N definido en el Punto de acceso a un SSID. Por ejemplo, por razones de seguridad, la mayoría de las instalaciones del Punto de acceso no asocian un SSID al VLA N nativo.Para crear un nuevo SSID, elija **nuevo**.Ingrese el SSID deseado (con diferenciación entre mayúsculas y minúsculas) en el rectángulo SSID.Seleccione el número deseado del VLA N para asociar este SSID de la lista desplegable.**Nota:** Para guardar este documento dentro de su alcance previsto, la Seguridad para un SSID no se dirige.El tecleo **se aplica-RadioX** para crear el SSID en la radio seleccionada, o Aplicar-**todo** para crearla en todas las radios.



O del CLI, publique 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. Relance los pasos 3a con 3d para cada SSID deseado o ingrese estos comandos del CLI con los cambios apropiados 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
```

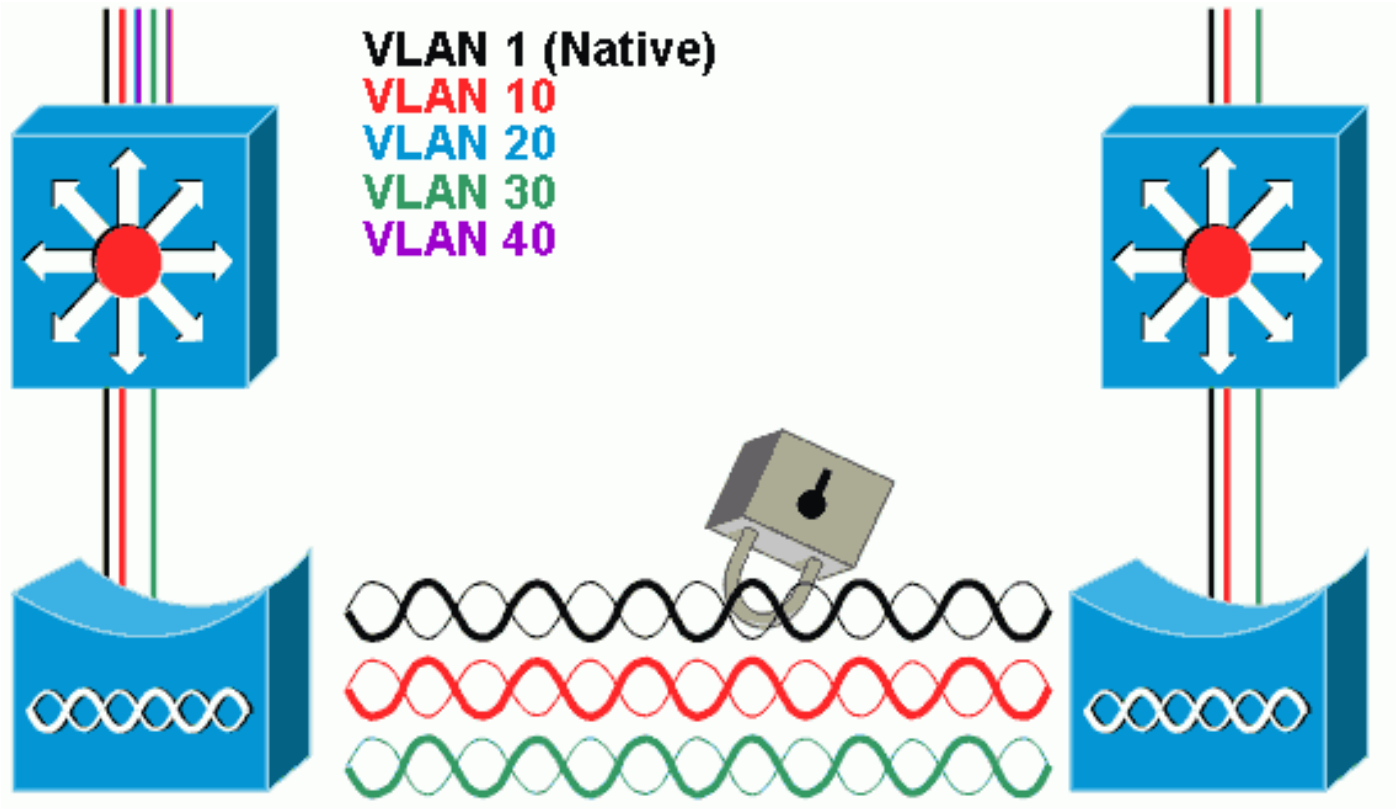
Nota: Estos ejemplos no incluyen la autenticación. Una cierta forma de autenticación (abierta, red-EAP) se requiere para que a los clientes se asocien.

VLA N en los puentes

Conceptos en los puentes

Esta sección discute los conceptos relacionados con cómo desplegar los VLA N en los puentes y refiere a este diagrama de la red.

En esta red de muestra, el VLA N 1 es el VLA N nativo, y los VLA N 10, 20, 30 y 40 existen. Solamente los VLA N 10 y 30 se amplían al otro lado del link. Se cifra el link de red inalámbrica.

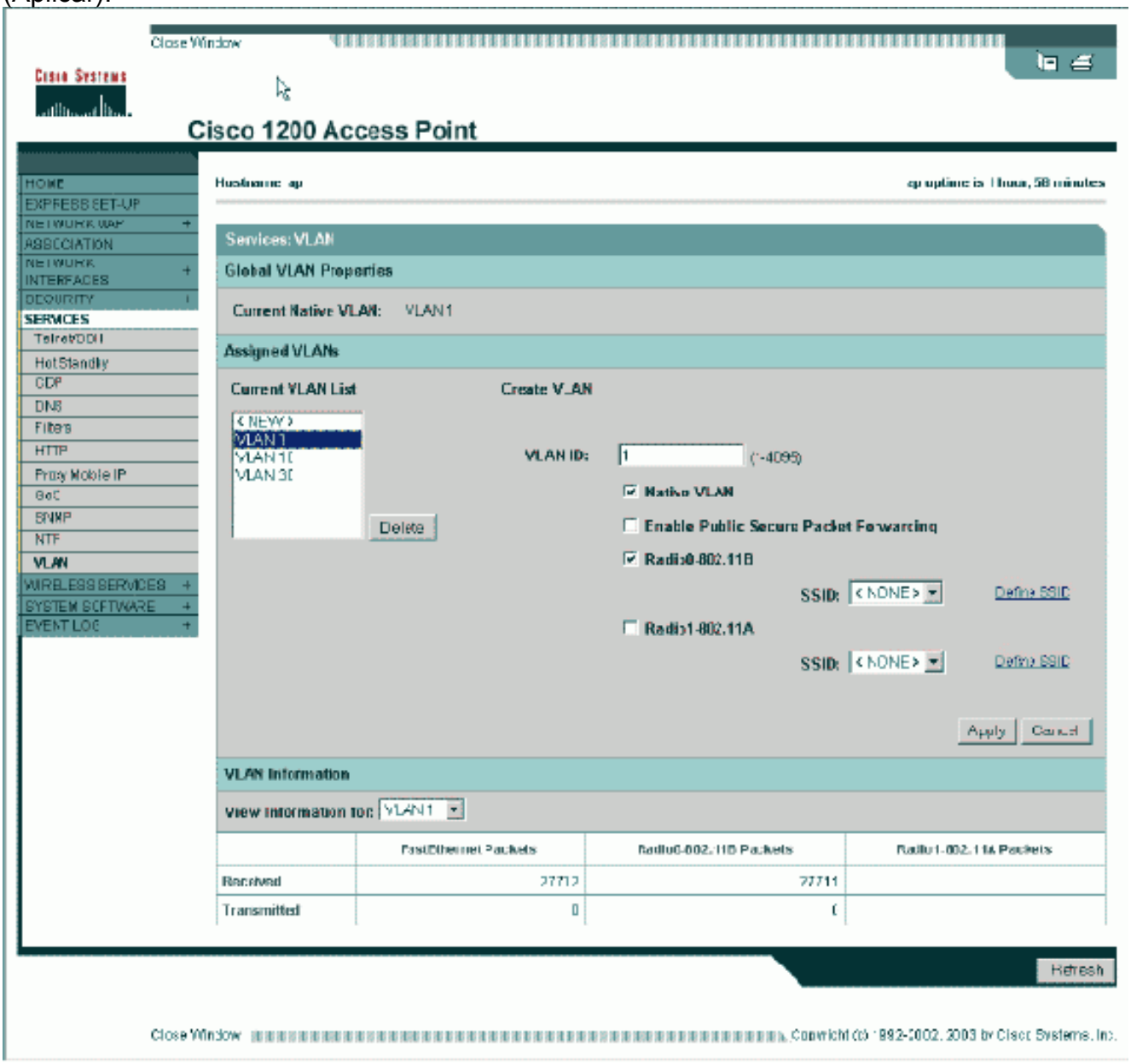


Para cifrar los datos que pasan sobre el link de radio, aplique el cifrado solamente al SSID del VLA N nativo. Ese cifrado se aplica al resto de los VLA N. Cuando usted puente, allí no es ninguna necesidad de asociar un SSID separado a cada VLA N. Las configuraciones del VLA N son lo mismo en los puentes de la raíz y de la no-raíz.

Configuración del puente

Para configurar el puente para los VLA N, como el ejemplo de diagrama de red, completa estos pasos:

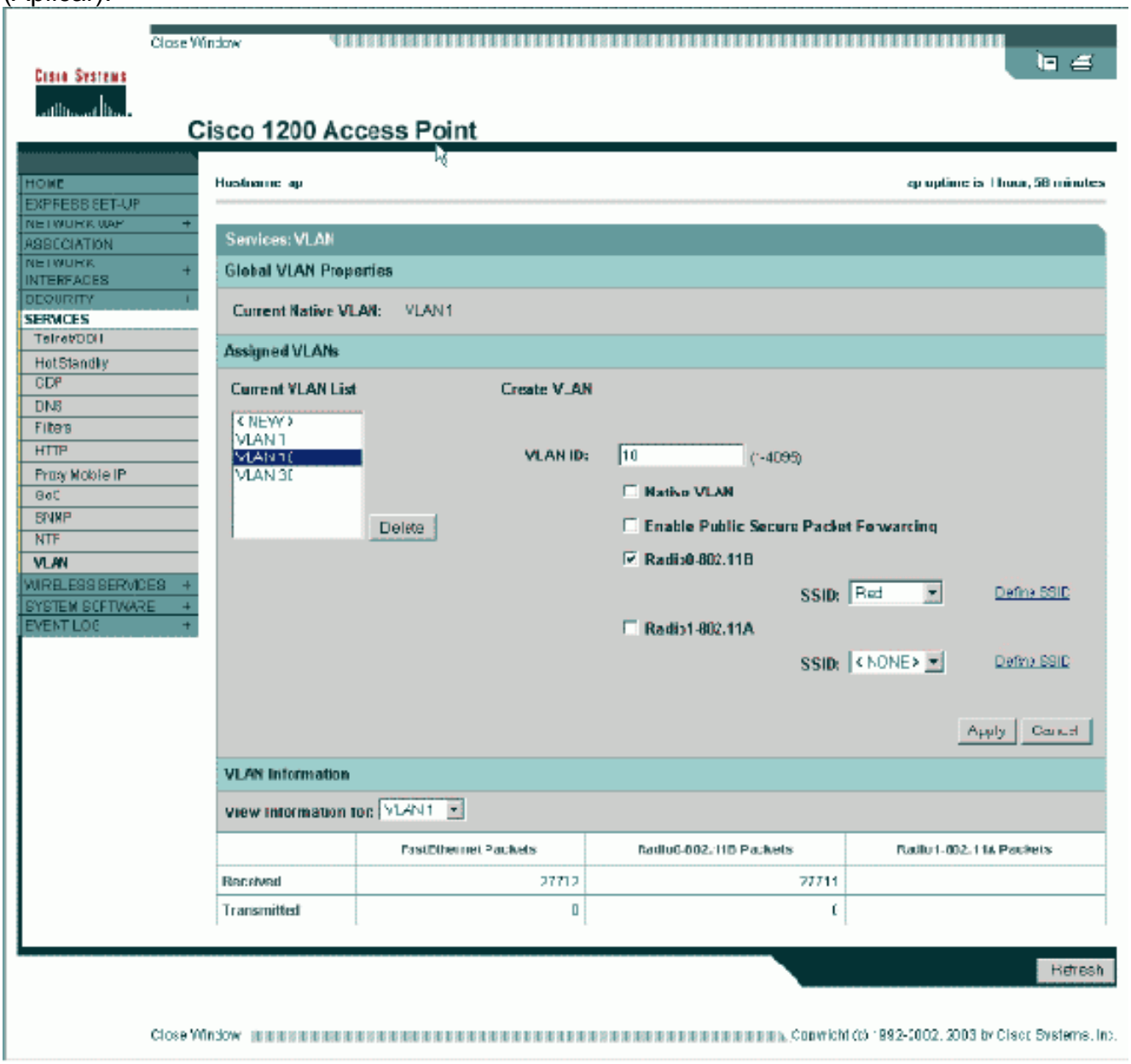
1. Del GUI AP, el tecleo **mantiene > VLA N** a navegar a los **servicios:** Página del **VLA N**.El primer paso es configurar el VLA N nativo. Para hacer esto, elija el **<New >** de la lista actual del VLA N.Ingrese el número del VLA N del VLA N nativo en el rectángulo identificación del VLA N. Esto debe hacer juego el VLA N nativo configurado en el conmutador.Porque el interfaz BVI 1 se asocia al subinterface del VLA N nativo, la dirección IP asignada para interconectar BVI 1 debe estar en la **misma subred IP** que otros dispositivos de infraestructura en la red (es decir interfaz SC0 en un conmutador del catalizador que ejecuta CatOS.)Marque la casilla de verificación correspondiente a la VLAN nativa.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 Dot11Radio0.1
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 otros VLA N, siga los siguientes pasos:De la lista actual del VLA N, seleccione **nuevo**.Ingrese el número del VLA N del VLA N deseado en el rectángulo identificación del VLA N. El número del VLA N debe hacer juego un VLA N configurado en el conmutador.Haga clic en Apply
(Aplicar).



O, desde el CLI, ejecute estos comandos:

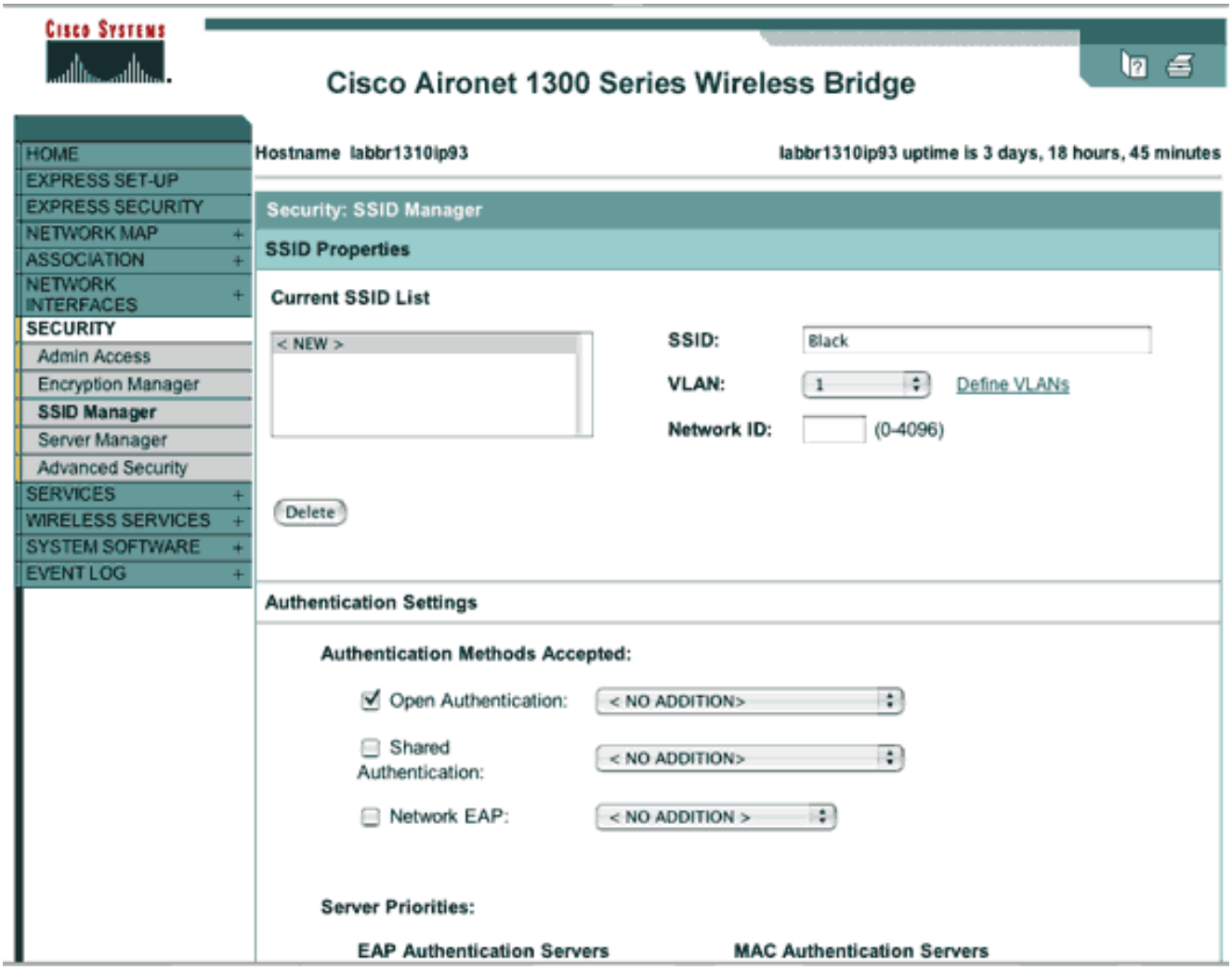
```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# interface FastEthernet0.10
bridge(config-subif)# encapsulation dot1Q 10
bridge(config-subif)# end
bridge#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

Relance los pasos 2a con 2c para cada VLA N deseado o ingrese los comandos del CLI con los cambios apropiados al subinterface y a los números del VLA N.

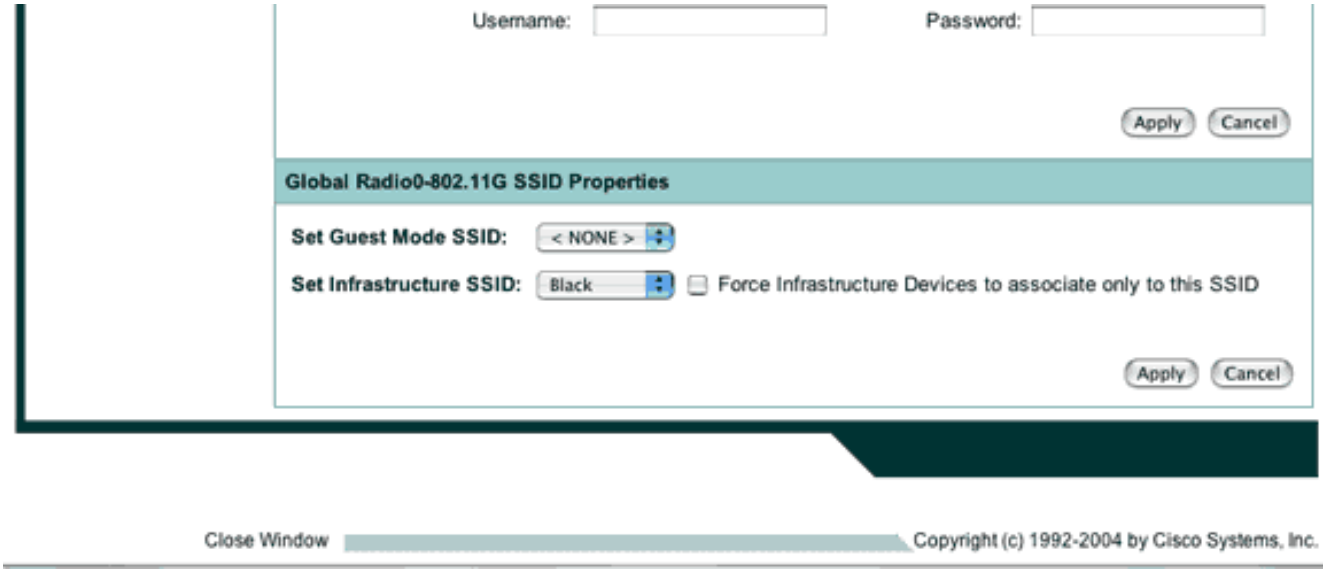
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.30
bridge(config-subif)# encapsulation dot1Q 30
bridge(config-subif)# interface FastEthernet0.30
```

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

3. Del administrador SSID (conforme al elemento de menú de la **Seguridad > del administrador SSID**,) asocie el VLA N nativo a un SSID.**Nota:** Cuando usted puente, el único SSID que usted debe asociar a un VLA N es el que correlaciona al VLA N nativo. Usted debe señalar este SSID como la infraestructura SSID.De la lista actual SSID, seleccione **nuevo**.Ingrese el SSID deseado (con diferenciación entre mayúsculas y minúsculas) en el rectángulo SSID.Seleccione el número del VLA N que correlaciona al VLA N nativo de la lista desplegable.**Nota:** Para guardar este documento dentro de su alcance previsto, la Seguridad para un SSID no se dirige.Haga clic **se aplican** para crear el SSID en la radio y para asociarlo al VLA N
nativo.



Enrolle detrás abajo a la parte inferior de la página, y bajo **Radio0-802.11G global SSID las propiedades** seleccionan el **SSID de la** lista desplegable de la **infraestructura SSID del conjunto**. Haga clic en Apply
(Aplicar).



O del CLI, publique 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 los VLA N son funcionando, los SSID se configuran bajo interfaz físico Dot11Radio, no bajo cualquier subinterfaz lógica.**Nota:** Este ejemplo no incluye la autenticación. Los puentes de la raíz y de la no-raíz requieren una cierta forma de autenticación (ábrase, red-EAP, etc.) para asociarse.

Utilice a un servidor de RADIUS para asignar a los usuarios a los VLA N

Usted puede configurar a su servidor de autenticación de RADIUS para asignar los usuarios o a los grupos de usuarios a un VLA N específico cuando autentican a la red. Para la información sobre esta característica, refiera a la sección usando un servidor de RADIUS para asignar a los usuarios a los VLA N de la *guía de configuración de software del Cisco IOS del* documento *para las puntas de acceso Aironet de Cisco, 12.4(3g)JA y 12.3(8)JEB*.

Utilice a un servidor de RADIUS para la asignación dinámica del grupo de la movilidad

Usted puede también configurar a un servidor de RADIUS para asignar dinámicamente a los Grupos de movilidad a los usuarios o a los grupos de usuarios. Esto elimina la necesidad de configurar los SSID múltiples en el Punto de acceso. En lugar, usted necesita configurar solamente un SSID por el Punto de acceso. Para la información sobre esta característica, refiera a la sección usando un servidor de RADIUS para la asignación dinámica del grupo de la movilidad de la *guía de configuración de software del Cisco IOS del* documento *para las puntas de acceso Aironet de Cisco, 12.4(3g)JA y 12.3(8)JEB*.

Puentee la configuración de grupo en los Puntos de acceso y los puentes

Los grupos del puente crean generalmente los dominios que cambian divididos en segmentos. El tráfico se confina a los host dentro de cada grupo del puente, pero no entre los grupos del puente. El conmutador adelante trafica solamente entre los host que componen el grupo del puente, que restringe la difusión y el tráfico Multicast (inundación) solamente a esos host. Los grupos del puente alivian la congestión de red y proporcionan a la seguridad de la red adicional cuando dividen el tráfico en segmentos a ciertas áreas de la red.

Refiera a puentear la descripción para la información detallada.

En una red inalámbrica, los grupos del puente se configuran en los untos de acceso de red inalámbrica y los puentes para que el tráfico de datos de un VLA N que se transmitirá de los media inalámbricos a la cara tela y vice versa.

Realice este paso del AP CLI para activar los grupos del puente global en el Punto de acceso/puente.

Este ejemplo utiliza el puente-grupo número 1.

Ap(configure)#bridge *1*

Nota: Usted puede numerar sus grupos del puente a partir de la 1 a 255.

Configure la interfaz radio y el interfaz rápido de los Ethernetes del dispositivo de red inalámbrica para estar en el mismo grupo del puente. Esto crea una trayectoria entre estos dos diversos interfaces, y están en el mismo VLA N para marcar los propósitos con etiqueta. Como consecuencia, los datos transmitidos del lado inalámbrico a través de la interfaz radio se transmiten al interfaz de los Ethernetes con el cual la red alámbrica está conectada y vice versa. Es decir radio e interfaces de los Ethernetes que pertenecen al mismo puente del grupo del puente realmente los datos entre ellos.

En un Punto de acceso/puente, usted necesita tener un grupo del puente por el VLA N de modo que el tráfico pueda pasar del alambre a la Tecnología inalámbrica y vice versa. Más el VLA N usted tiene esa necesidad de pasar el tráfico a través de la Tecnología inalámbrica, más grupos del puente es necesario.

Por ejemplo, si usted tiene solamente un VLA N para pasar el tráfico a través de la Tecnología inalámbrica a la cara tela de su red, configure solamente un grupo del puente del CLI del AP/bridge. Si usted tiene VLAN múltiples para pasar el tráfico de la Tecnología inalámbrica a la cara tela y vice versa, configure los grupos del puente para cada VLA N en el sub-interfaz de radio, así como el sub-interfaz rápido de los Ethernetes.

1. Configure el grupo del puente en el interfaz inalámbrico con el comando interface del **grupo** dot11radio del **puente**.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 del puente con el mismo número de grupo del puente (el "1" en este ejemplo) en el interfaz rápido de los Ethernetes para pasar el VLA N 1 tráfico a través del interfaz inalámbrico a esta cara tela y vice versa.

```
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 usted configura un grupo del puente en la interfaz radio, estos comandos se fijan automáticamente.**suscriptor-loop-control del puente-grupo *1*bloque-desconocido-fuente del puente-grupo *1*ningún puente-grupo *1 fuente*-que aprendeninguna Inundación de unidifusión del puente-grupo *1*atravesar-minusválidos del puente-grupo *1*Nota:** Cuando usted configura un grupo del puente en el interfaz rápido de los Ethernetes, estos comandos se fijan automáticamente.**ningún puente-grupo *1 fuente*-que aprendeatravesar-minusválidos del puente-grupo *1***

Integrated Routing and Bridging (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 Local o el tráfico no enrutable se puede puentear entre los interfaces puenteados en el mismo grupo del puente, mientras que el tráfico routable se puede encaminar a otros interfaces o grupos encaminados del puente

Con la encaminamiento integrada y puentear, usted puede hacer esto:

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

Permita a IRB en los untos de acceso de red inalámbrica y los puentes para encaminar su tráfico entre los grupos del puente o entre los interfaces y los grupos encaminados del puente. Usted necesita un router externo o un switch de la capa 3 para encaminar entre los grupos del puente o entre los grupos del puente y los interfaces encaminados.

Publique este comando para activar IRB en el AP/bridge.

Irb del #bridge de AP(configure)

La encaminamiento integrada y el puentear utiliza el concepto de una interfaz virtual del Puente-grupo (BVI) para encaminar el tráfico entre los interfaces y los grupos encaminados del puente o entre los grupos del puente.

Un BVI es una interfaz virtual dentro del router del switch de la capa 3 que actúa como un interfaz encaminado normal. Un BVI no utiliza puentear sino representa realmente el grupo correspondiente del puente a los interfaces encaminados dentro del router del switch de la capa 3. Tiene todos los atributos de la capa de red (tales como una dirección de capa de red y filtros) que se aplican al grupo correspondiente del puente. 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 los puentes.

1. Configure el BVI y asigne el número correspondiente del grupo del puente al BVI. Este ejemplo asigna el número de grupo 1 del puente al 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. Permita a un BVI validar y encaminar los paquetes enrutables recibidos de su grupo correspondiente del puente.
   ```
   Ap(config)# bridge 1 route ip!---
   !--- This example enables the BVI to accept and route the IP packet.
   ```
   Es importante entender que usted necesita solamente un BVI para la Administración/el VLA N nativo en quienes el AP está situado (en este ejemplo, el VLA N 1). Usted no necesita un BVI para ningún otro subinterface, con independencia de cuántos VLA N y del puente le agrupa configuran en su AP/bridge. Esto es porque usted marca el tráfico con etiqueta en el resto de los VLA N (excepto el VLA N nativo) y le manda al conmutador sin embargo un interfaz trunked dot1q sobre la cara tela. Por ejemplo, si usted tiene 2 VLA N en su red, usted necesita dos grupos del puente, pero solamente un correspondiente BVI al VLAN de administración es suficiente en su red inalámbrica.Cuando usted activa la encaminamiento para un protocolo dado en la interfaz virtual del grupo del puente, los paquetes que vienen de un interfaz encaminado, pero son destinados para un host en un dominio puenteado, se encaminan a la interfaz virtual del grupo del puente y se remiten al interfaz puenteado correspondiente.Todo el tráfico que se encamina a la interfaz virtual del grupo del puente se remite al grupo correspondiente del puente mientras que tráfico puenteado. Todo el tráfico routable recibido en un interfaz puenteado se encamina a otros interfaces encaminados como si venga directamente de la interfaz virtual del grupo del puente.Refiérase configuran puentear para información más detallada sobre puentear e IRB.

Interacción con el Switches relacionado

En esta sección, le presentan con la información para configurar, o verifique la configuración del Switches de Cisco que conecta con el equipo del Aironet de red inalámbrica de Cisco.

Nota: Para encontrar la información adicional en los comandos usados en este documento, use la Command Lookup Tool (clientes registrados solamente).

Configuración del switch — OS del catalizador

Para configurar un conmutador que funcione con el OS del catalizador a los VLA N del tronco a un Punto de acceso, la sintaxis de ordenes es **tronco determinado <module -/port -> en dot1q** y el **tronco del conjunto <module -/port -> <vlan list>**.

Un ejemplo al ejemplo de diagrama de red, es:

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

Configuración del switch — Switches del catalizador basado IOS

Del modo de configuración de la interfaz, ingrese estos comandos, si usted quiere a:

- Configure el switchport a los VLA N del tronco a un Punto de acceso

- En un catalizador cambie que IOS de los funcionamientos
- El CatIOS incluye pero no se limita a:6x004x0035x0295x

```
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 basado IOS del Aironet de red inalámbrica de Cisco no utiliza el Dynamic Trunking Protocol (DTP), así que el conmutador no debe intentar negociarlo.

Configuración del switch — Catalizador 2900XL/3500XL

Del modo de configuración de la interfaz, ingrese estos comandos, si usted quiere configurar el switchport a los VLA N del tronco a un Punto de acceso en un Catalyst 2900XL o 3500XL Switch que funcione con el 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.

Verifique el equipo de red inalámbrica

- **demostración vlan** — visualiza todos los VLA N configurados actualmente en el Punto de acceso, y su estatus

```
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#
```

- **muestre las asociaciones dot11** — información de las visualizaciones sobre los clientes asociados, por el SSID/VLAN

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others:  (not related to any ssid)

ap#
```

Verifique el conmutador

- En un switch basado OS del catalizador, **muestre el tronco <module -/port ->** — visualiza el estatus de un tronco 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 IOS, **muestre el tronco del fastethernet del interfaz <module -/port ->** — visualiza el estatus de un tronco 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 conmutador del catalizador 2900XL/3500XL, **muestre el switchport del fastethernet del interfaz <module -/port ->** — visualiza el estatus de un tronco 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#
```

Troubleshooting

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

Información Relacionada

- Configurando los VLA N (guía de Configuración de punto de acceso)
- Configurando los VLA N (guía de configuración del puente)
- Soporte técnico del enlace
- Interacción con el Switches relacionado
- Requisitos del sistema para implementar el link troncal
- Descripción General del Bridging
- Tipos inalámbricos de la autenticación en un ejemplo fijo de la configuración ISR
- Tipos inalámbricos de la autenticación en ISR fijo con el ejemplo de la configuración de SDM
- Conectividad inalámbrica LAN usando un ISR con el ejemplo de la configuración de la encripción WEP y de la autenticación LEAP
- Ejemplo de Configuración de Conexión LAN de Elementos Básicos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems