Uso de las VLAN con el Equipo inalámbrico de Cisco Aironet

Contenido

Introducción

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

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

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

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 Switch de esta configuración con ninguno de estos soporte físico o software:

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

Convenciones

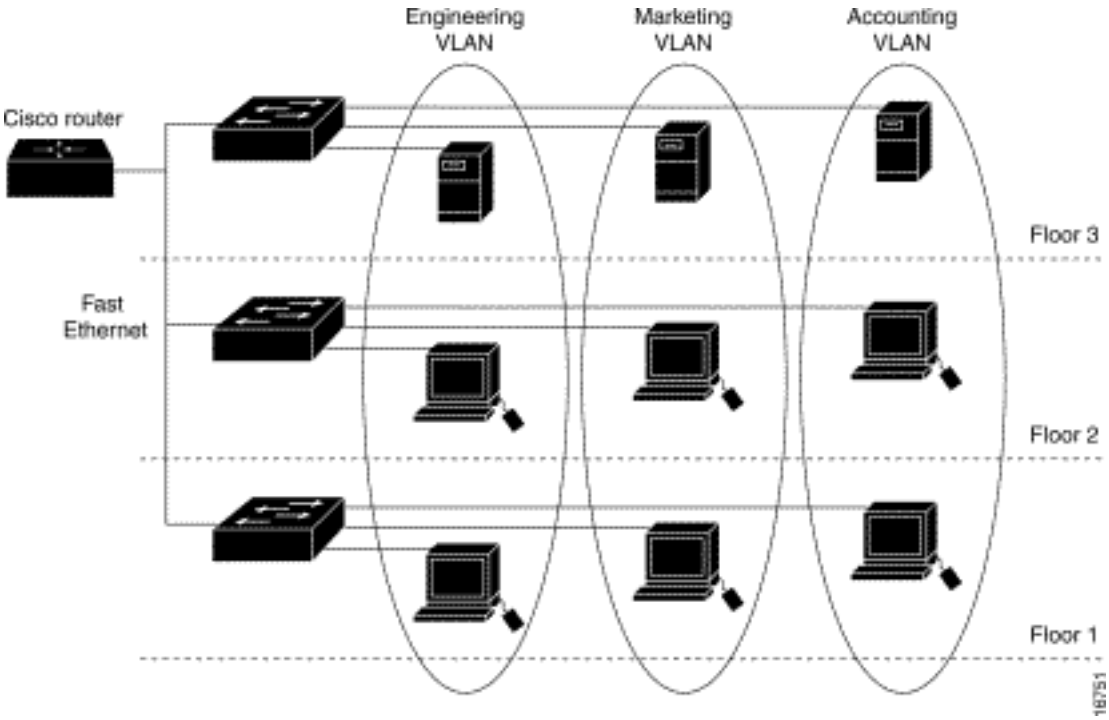
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

VLAN

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 extremos, los host o equipo de red (tal como Bridges y Routers), conectado por un solo dominio de Bridging. El dominio de Bridging se soporta en los diversos pedazos de equipo de red, tales como switches LAN, que actúan los protocolos del bridging entre ellos con un grupo separado para cada VLA N.

Cuando usted conecta un dispositivo con un Switch del Cisco Catalyst, el puerto en donde el dispositivo está conectado es un 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, usted debe cruz-conectar el chasis de switch múltiple, 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 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 un VLAN ID o un nombre, sigue que, si el SSID en un Punto de acceso se configura para reconocer un VLAN ID o un nombre específico, 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 acceder el 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 soportar hasta 16 VLA N. Usted puede asignar solamente un SSID a un VLA N.

Usted amplía los VLA N en un Wireless LAN 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 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 los Wireless Bridge, usted puede pasar los VLAN múltiples a través del link de red inalámbrica para proporcionar 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 el VLAN1 incluso si el VLAN1 no se define en el Punto de acceso.

Como consecuencia, el switch de Ethernet conecta con el Punto de acceso y genera un mensaje de advertencia. No hay pérdida de función en el Punto de acceso o el Switch, 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 VLAN nativo del Punto de acceso, que no es necesariamente VLAN1. Esto hace el switch de Ethernet 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 Switch 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 de red inalámbrica del Cisco Aironet, usted puede experimentar el funcionamiento 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 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 Workgroup BridgePuntos de acceso del repetidorNon-Root BridgeEs 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 Bridge, usted puede solamente tener una infraestructura SSID. La infraestructura SSID debe ser el SSID que correlaciona al VLAN nativo.
- Uso erróneo o diseño incorrecto de designación SSID del modo de invitadoAl 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 radiobaliza 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 OSIVersiones desaprobadas del software permit binding multiple SSID del Cisco Aironet a un VLA N. Las versiones actuales no lo hacen.
- Fallas de ruteo de la capa 3 del modelo de OSI o diseños incorrectosCada SSID y su VLA N conectado deben tener un dispositivo de ruteo y cierta fuente para dirigirse a los clientes, por ejemplo un servidor DHCP o el alcance en un servidor DHCP.
- Entienda mal o configure incorrectamente el VLAN nativoLos 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). El cliente PC es miembros de un diverso VLA N, apenas pues los teléfonos IP son miembros de otro VLA N. 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.

Significación del VLAN nativo

Cuando usted utiliza un puerto troncal del IEEE 802.1Q, todas las tramas se marcan con etiqueta a menos que ésos en el VLA N configurado como el “VLAN nativo” para el puerto. Los capítulos en el VLAN nativo son siempre untagged transmitido y son normalmente untagged recibido. Por lo tanto, cuando un AP está conectado con el switchport, el VLAN nativo configurado en el AP debe hacer juego el VLAN nativo configurado en el switchport.

Nota: Si hay una discordancía en los VLAN nativos, se caen las tramas.

Este escenario se explica mejor con un ejemplo. Si el VLAN nativo en el switchport se configura como VLAN 12 y en el AP, el VLAN nativo se configura como VLAN1, después cuando el AP envía una trama en su VLAN nativo al Switch, el Switch considera la trama como perteneciendo al VLAN 12 puesto que las tramas del VLAN 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 una trama de su VLAN nativo al AP.

La configuración del VLAN 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 AP. El repetidor AP soporta solamente el VLAN 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 Switch no pasa a y desde el AP de repetidor.

Un ejemplo para el escenario donde la discordancía en la configuración de VLAN nativa del repetidor el AP puede crear los problemas está cuando hay servidor DHCP detrás del Switch 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 DHCP porque las tramas (pedidos de DHCP en nuestro caso) del VLAN nativo del repetidor el AP (que no es lo mismo que el AP raíz y el Switch) se caen.

También, cuando usted configura el puerto del switch, *asegúrese de que todos los VLA N que se configuran en los AP 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 Switch:

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

Por abandono, un switchport configurado como trunk 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 AP. Pode los VLA N en el Switch de modo que solamente el tráfico VLAN que el AP está interesado en los pasos con el AP evitar CPU elevada.

VLA N en los Puntos de acceso

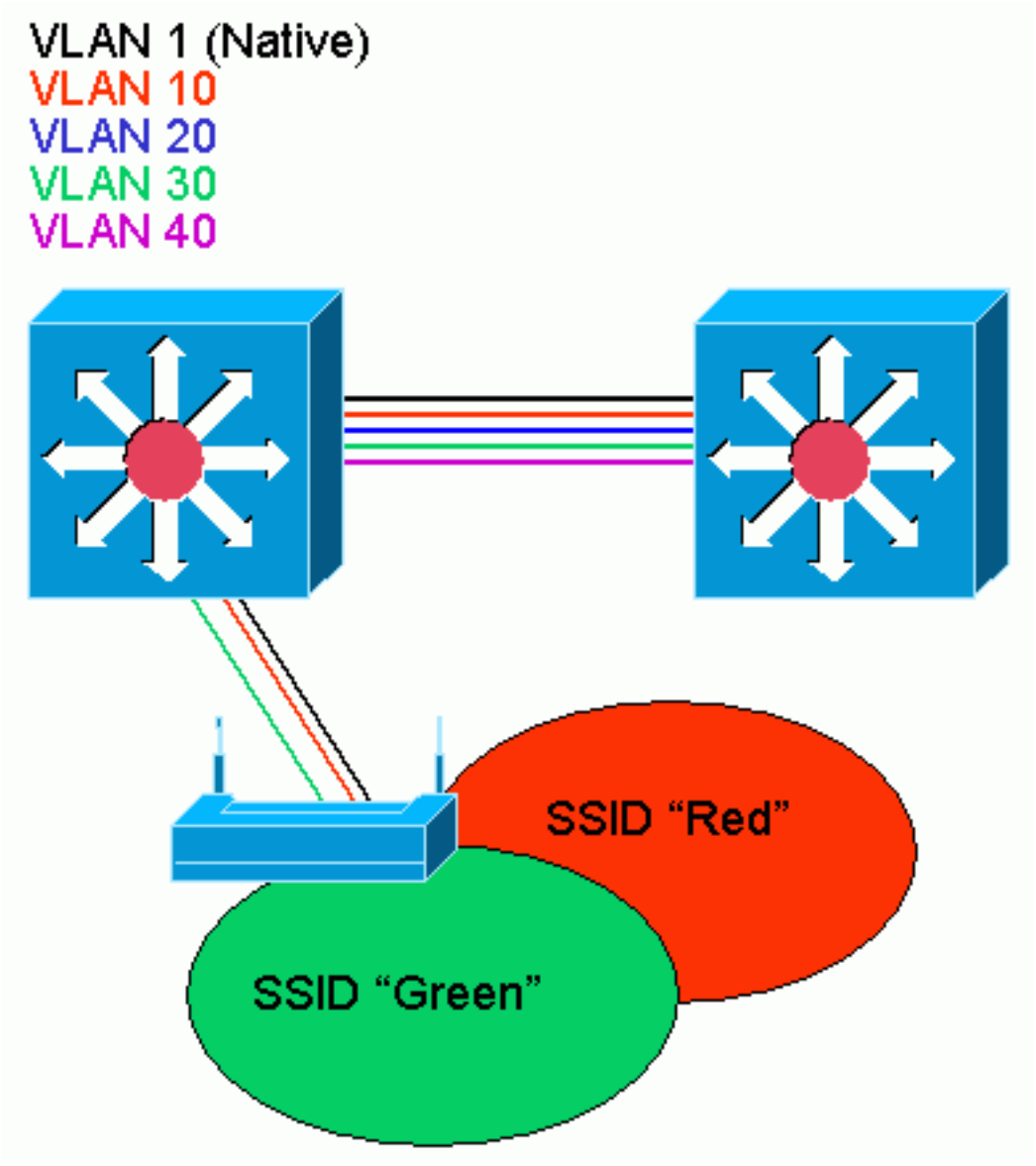
En esta sección encontrará la información para configurar las funciones descritas en este documento.

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 VLAN1 es el VLAN 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 VLAN nativo se requiere para proporcionar la capacidad de administración y las autenticaciones de cliente.

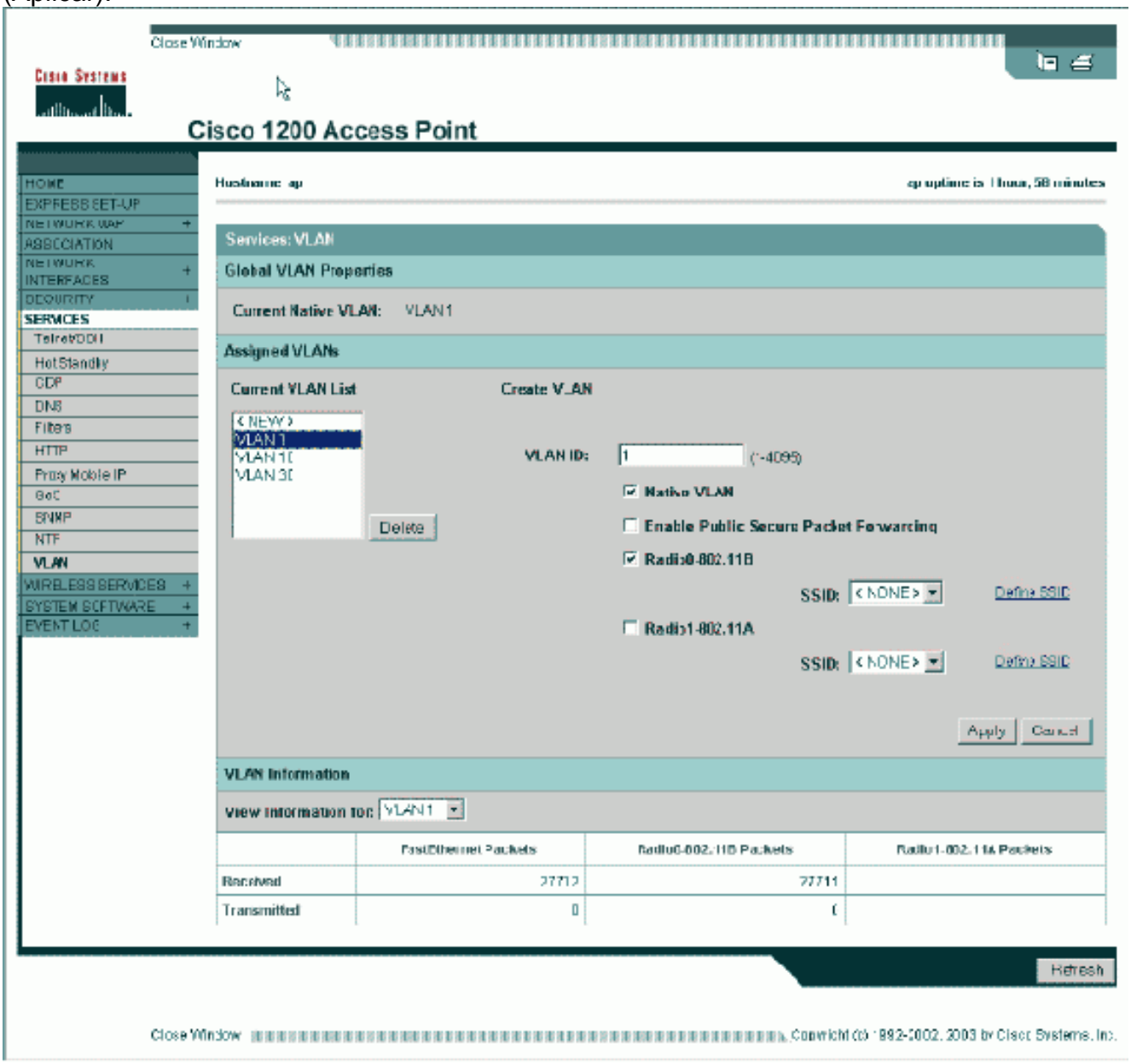


Configuración de punto de acceso

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

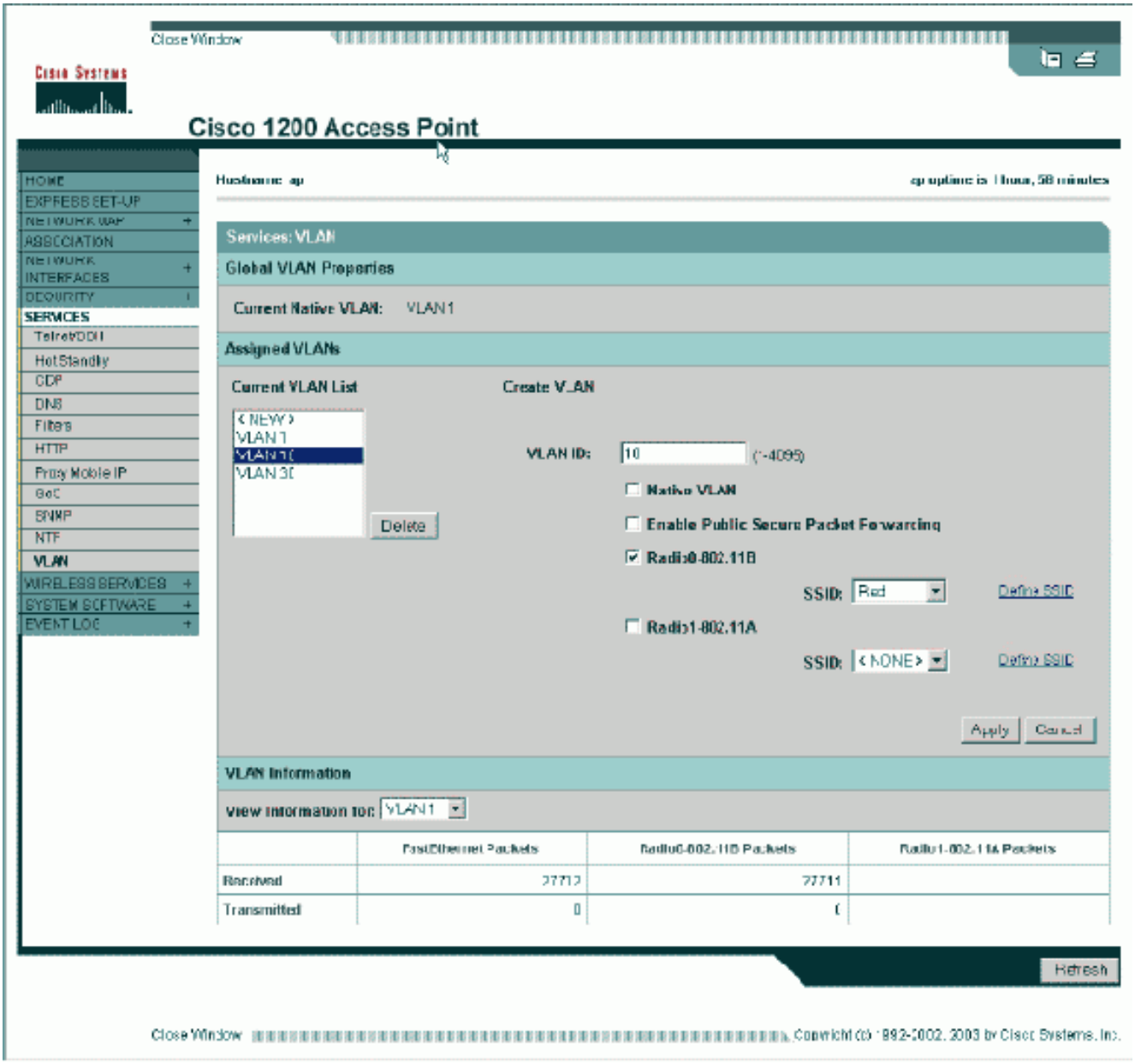
1. Del AP GUI, haga clic los servicios > el VLA N a navegar a los **servicios:** Página del **VLA N**.El primer paso es configurar el VLAN nativo. De la lista de VLAN actual, seleccione **nuevo**.Ingrese el número de VLAN de la VLAN nativa en la casilla de identificación de VLAN.

El número VLAN debe hacer juego el VLAN nativo configurado en el Switch.Porque el BVI 1 de la interfaz se asocia a la subinterfaz del VLAN nativo, la dirección IP asignada para interconectar el 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 de Catalyst que ejecuta CatOS.)Marque la casilla de verificación correspondiente a la VLAN nativa.Seleccione las casillas de verificación para la interfaz radio o las interfaces donde este VLA N se aplica.Haga clic en Apply
(Aplicar).



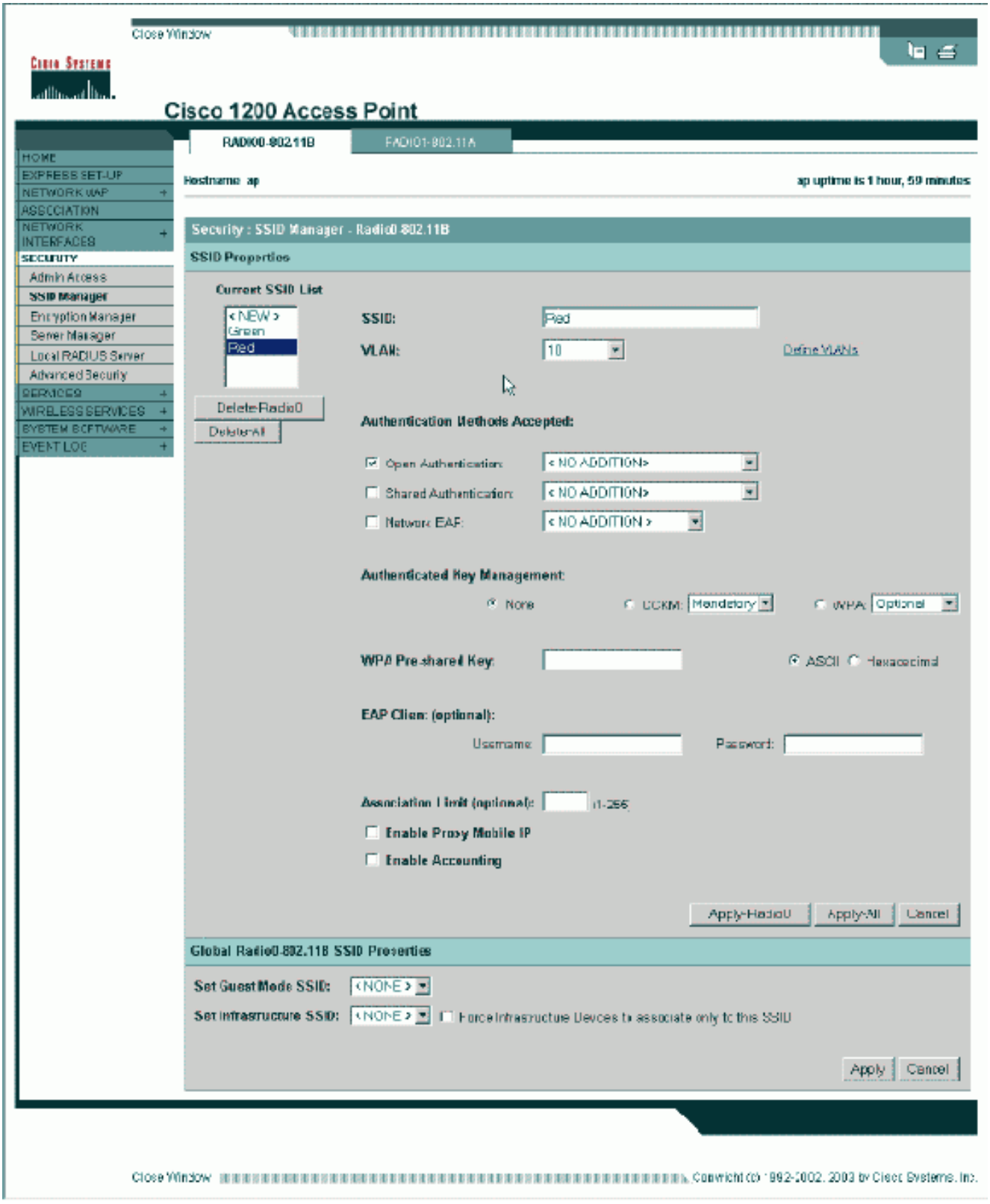
O, desde el CLI, ejecute estos comandos:`AP# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. AP(config)# **interface Dot11Radio0.1** AP(config-subif)# **encapsulation dot1Q 1 native** AP(config-subif)# **interface FastEthernet0.1** AP(config-subif)# **encapsulation dot1Q 1 native** AP(config-subif)# **end** AP# **write memory**`

2. Para configurar otros VLA N, siga los siguientes pasos:De la lista de VLAN actual, seleccione **nuevo**.Introduzca el número VLAN de la VLAN deseada en la casilla ID de VLAN. El número VLAN debe hacer juego un VLA N configurado en el Switch.Seleccione las casillas de verificación para la interfaz radio o las 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 a la subinterfaz y a los números 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 los VLAN 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 VLAN nativo.Para crear un nuevo SSID, elija **nuevo**.Ingrese el SSID deseado (caso sensible) en el rectángulo SSID.Seleccione el número deseado de VLAN para asociar este SSID con la lista desplegable.**Nota:** Para guardar este documento dentro de su alcance previsto, la Seguridad para un SSID no se dirige.Haga clic en Apply-RadioX para crear el SSID en la radio seleccionada o Apply-all para crearlo 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`

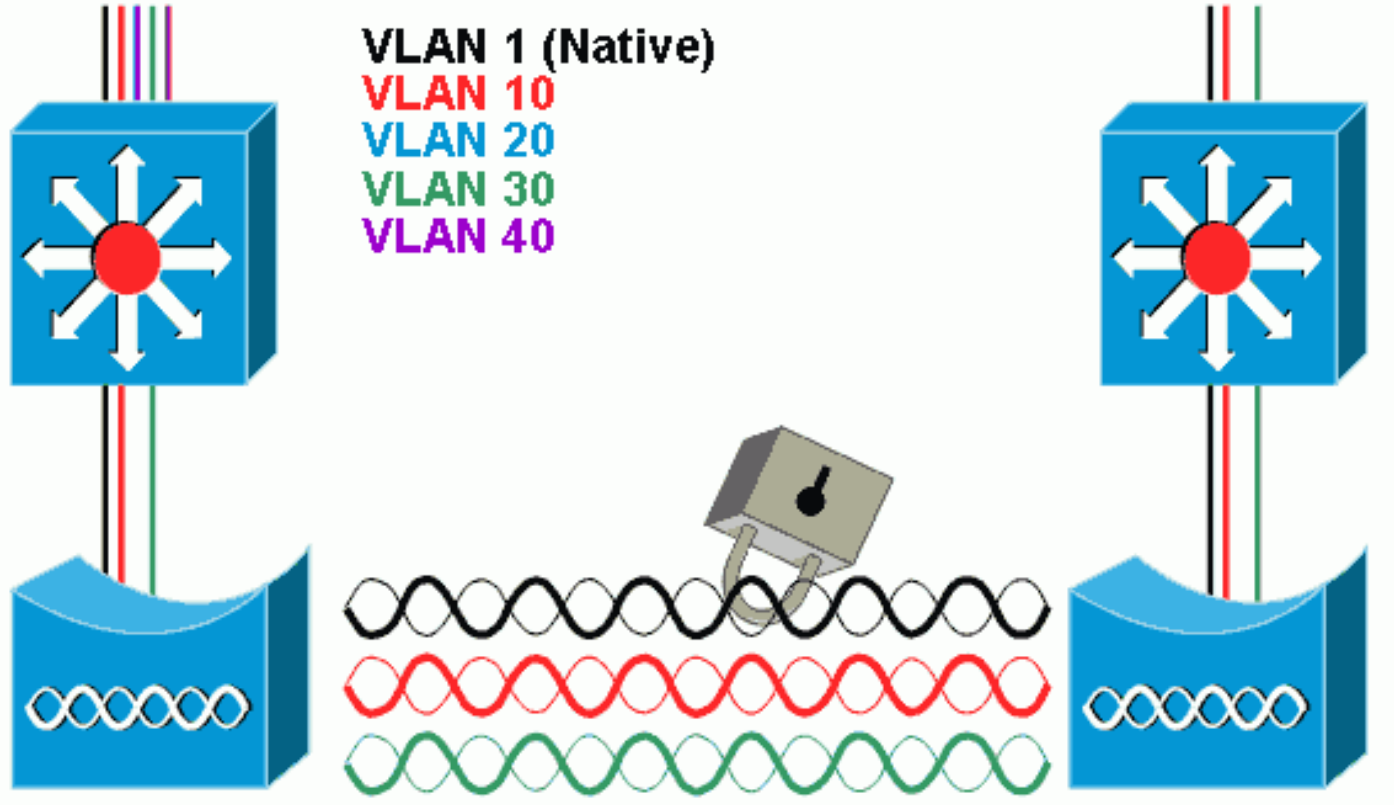
4. Relance los pasos 3a con 3d para cada SSID deseado o ingrese estos comandos del CLI con los cambios apropiados al SSID.`AP# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AP(config)# interface Dot11Radio0 AP(config-if)# ssid Green AP(config-if-ssid)# vlan 30 AP(config-if-ssid)# end AP# write memory` **Nota:** Estos ejemplos no incluyen la autenticación. Un poco de forma de autenticación (abierta, Network EAP) se requiere para que a los clientes se asocien.

VLA N en los Bridges

Conceptos en los Bridges

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

En esta red de muestra, el VLAN1 es el VLAN 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.



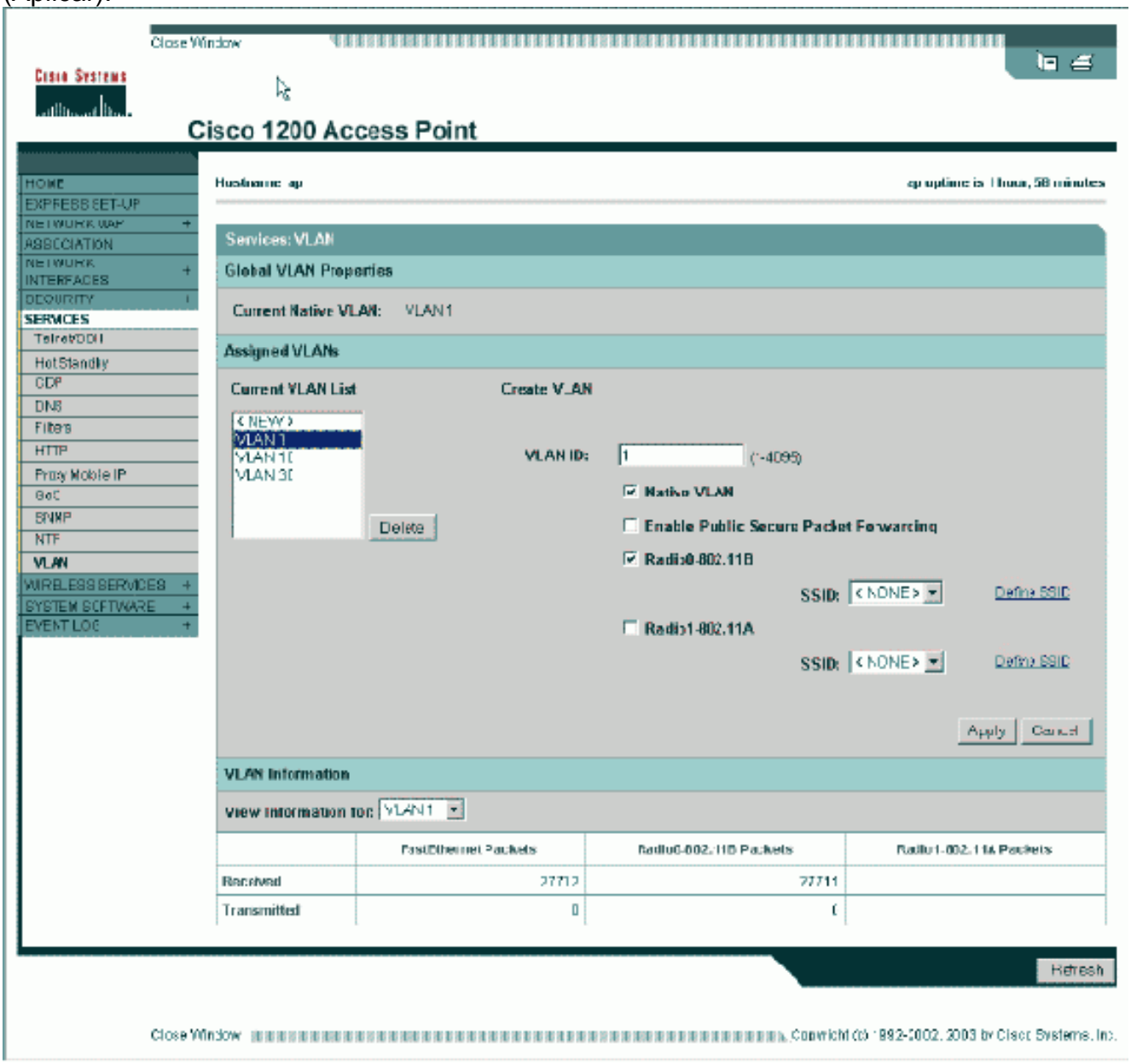
Para cifrar los datos que pasan sobre el link de radio, aplique el cifrado solamente al SSID del VLAN nativo. Ese cifrado se aplica al resto de los VLA N. Cuando usted Bridge, allí no es ninguna necesidad de asociar un SSID separado a cada VLA N. Las configuraciones de VLAN son lo mismo en la raíz y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

Configuración de Bridge

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

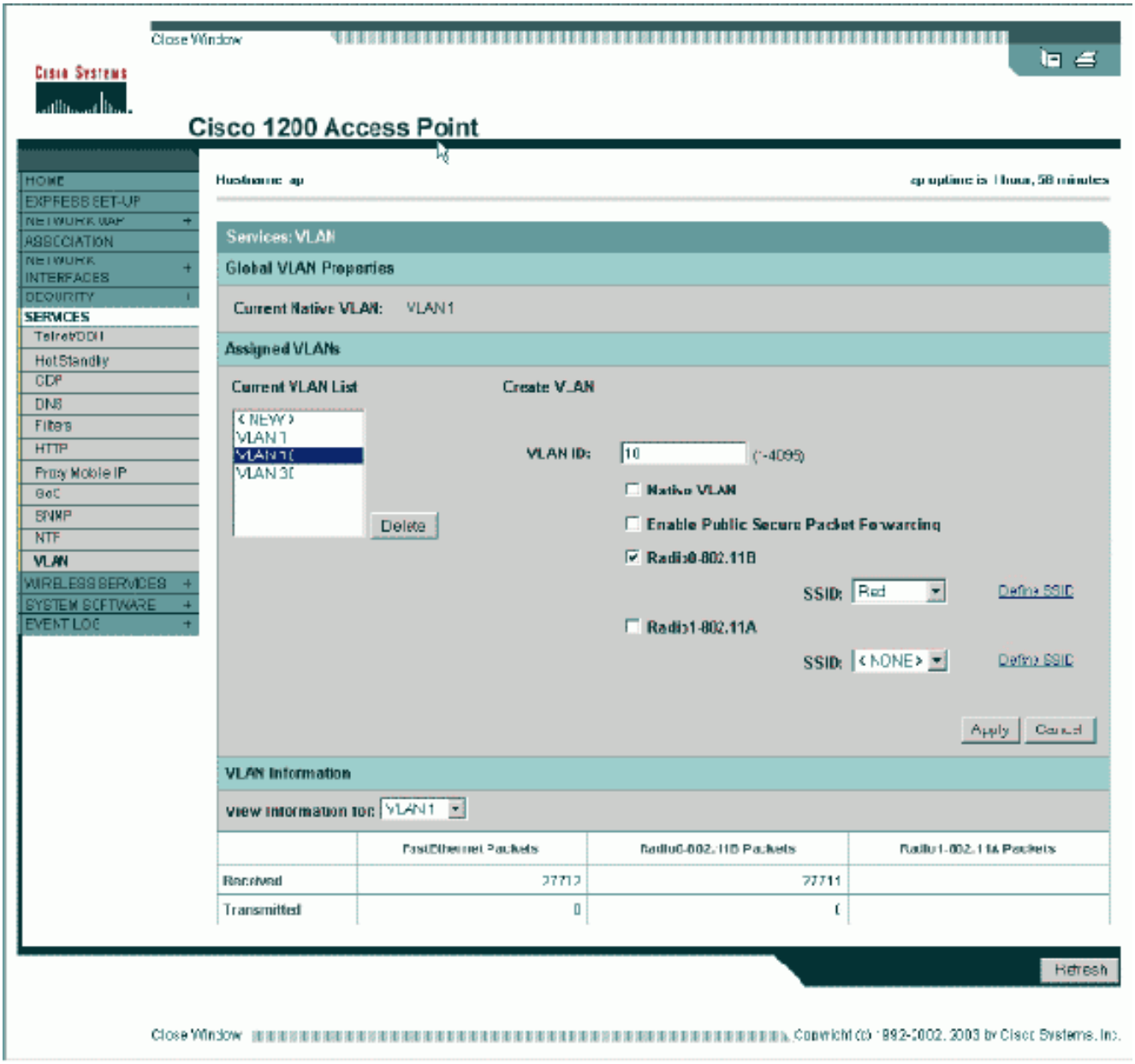
1. Del AP GUI, el tecleo **mantiene > VLA N** a navegar a los **servicios:** Página del **VLA N**.El primer paso es configurar el VLAN nativo. Para hacer esto, elija el <New > de la lista de VLAN actual.Ingrese el número de VLAN de la VLAN nativa en la casilla de identificación de VLAN. Esto debe hacer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

Apply
(Aplicar).



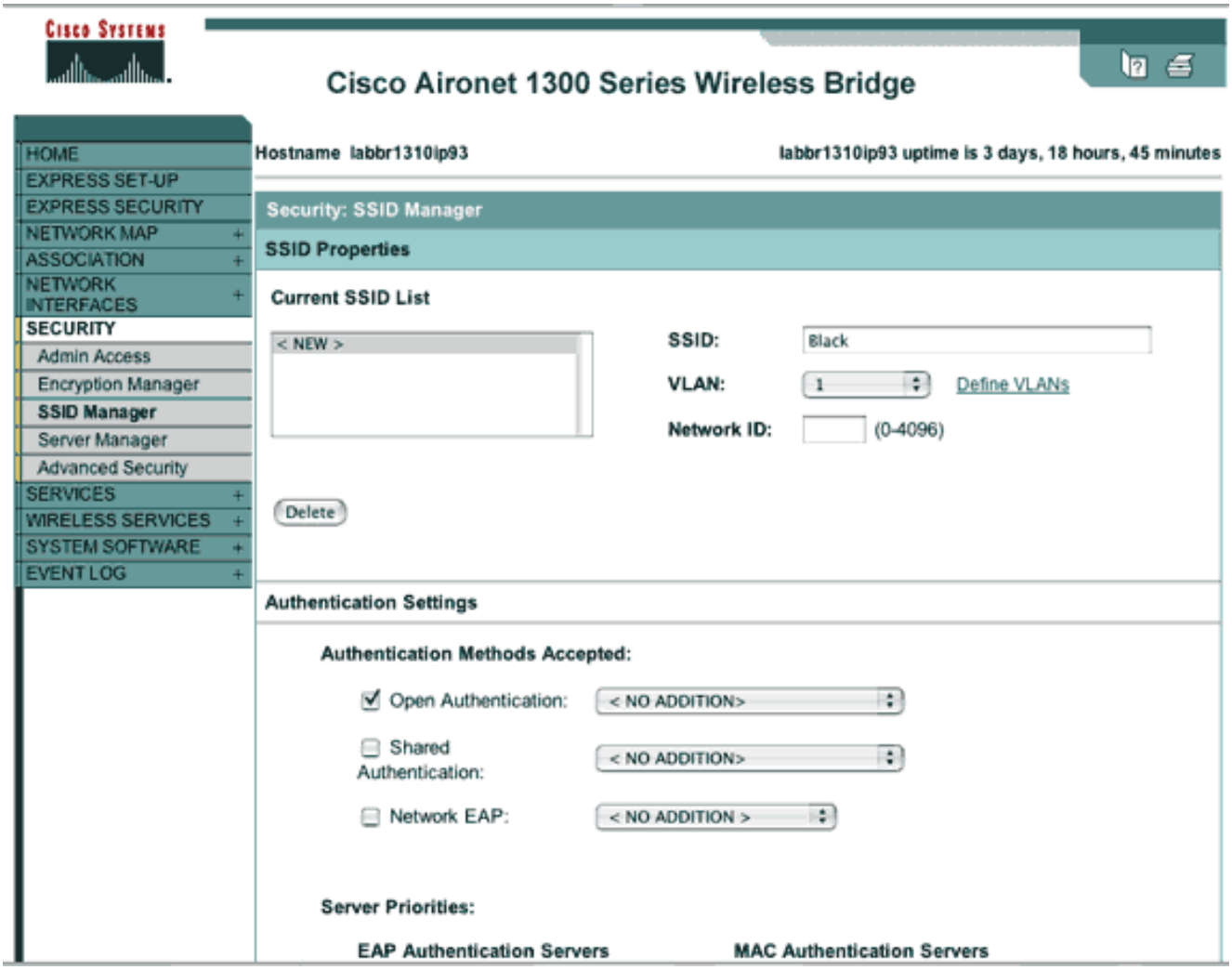
O, desde el CLI, ejecute estos comandos:`bridge# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. bridge(config)# **interface Dot11Radio0.1** bridge(config-subif)# **encapsulation dot1Q 1 native** bridge(config-subif)# **interface FastEthernet0.1** bridge(config-subif)# **encapsulation dot1Q 1 native** bridge(config-subif)# **end** bridge# **write memory**`

2. Para configurar otros VLA N, siga los siguientes pasos:De la lista de VLAN actual, seleccione **nuevo**.Introduzca el número VLAN de la VLAN deseada en la casilla ID de VLAN. El número VLAN debe hacer juego un VLA N configurado en el Switch.Haga clic en Apply (Aplicar).

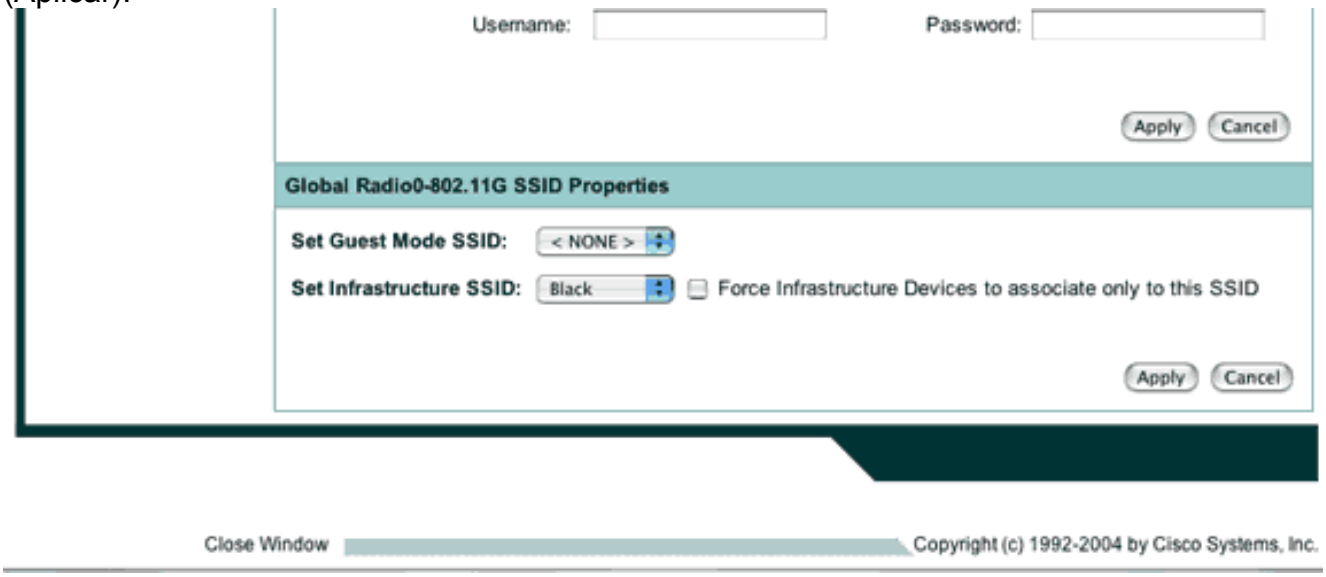


O, desde el CLI, ejecute estos comandos:`bridge# **configure terminal** Enter configuration commands, one per line. End with CNTL/Z. bridge(config)# **interface Dot11Radio0.10** bridge(config-subif)# **encapsulation dot1Q 10** bridge(config-subif)# **interface FastEthernet0.10** bridge(config-subif)# **encapsulation dot1Q 10** bridge(config-subif)# **end** bridge# **write memory**` Relance los pasos 2a con 2c para cada VLA N deseado o ingrese los comandos del CLI con los cambios apropiados a la subinterfaz y a los números 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. Del administrador SSID (conforme al elemento de menú de la **Seguridad > del administrador SSID**,) asocie el VLAN nativo a un SSID.**Nota:** Cuando usted Bridge, el único SSID que usted debe asociar a un VLA N es el que correlaciona al VLAN nativo. Usted debe señalar este SSID como la infraestructura SSID.De la lista actual SSID, seleccione **nuevo**.Ingrese el SSID deseado (caso sensible) en el rectángulo SSID.Seleccione el número VLAN que correlaciona al VLAN 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 VLAN nativo.



Navegue detrás abajo a la parte inferior de la página, y bajo el **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 física Dot11Radio, no bajo cualquier subinterfaz lógica.**Nota:** Este ejemplo no incluye la autenticación. La raíz y los Non-Root Bridge requieren un poco de forma de autenticación

(ábrase, Network 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 del Cisco IOS Software del* documento *para los Puntos de acceso del Cisco Aironet, 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 del Cisco IOS Software del* documento *para los Puntos de acceso del Cisco Aironet, 12.4(3g)JA y 12.3(8)JEB*.

Configuración del Grupo de Bridge en los Puntos de acceso y los Bridges

Los Grupos de Bridge crean generalmente dividido en segmentos conmutando los dominios. El tráfico se confina a los host dentro de cada Grupo de Bridge, pero no entre los Grupos de Bridge. El Switch adelante trafica solamente entre los host que componen el Grupo de Bridge, que restringe el broadcast y el tráfico Multicast (inundación) solamente a esos host. Los Grupos de Bridge alivian la congestión de red y proporcionan la seguridad de la red adicional cuando dividen el tráfico en segmentos a ciertas áreas de la red.

Refiera a la descripción del bridging para la información detallada.

En una red inalámbrica, configuran a los Grupos de Bridge en los untos de acceso de red inalámbrica y los Bridges 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 habilitar a los Grupos de Bridge global en el puente de/punto de acceso.

Este ejemplo utiliza el bridge-group number 1.

Ap(configure)#bridge *1*

Nota: Usted puede numerar a sus Grupos de Bridge a partir de la 1 a 255.

Configure la interfaz radio y la interfaz Fast Ethernet del dispositivo de red inalámbrica para estar en el mismo Grupo de Bridge. Esto crea una trayectoria entre estas dos diversas interfaces, y están en el mismo VLA N para marcar los propósitos con etiqueta. Como consecuencia, los datos transmitidos del lado de la Tecnología inalámbrica a través de la interfaz radio se transmiten a la

interfaz de Ethernet con la cual la red alámbrica está conectada y vice versa. Es decir radio y interfaces de Ethernet que pertenecen al mismo Bridge del Grupo de Bridge realmente los datos entre ellos.

En un puente de/punto de acceso, usted necesita tener un Grupo de Bridge 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 de Bridge 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, configuración solamente un Grupo de Bridge 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 de Bridge para cada VLA N en la sub-interfaz de radio, así como la sub-interfaz de los fast ethernet.

1. Configure al Grupo de Bridge en la interfaz inalámbrica con el comando interface del **Grupo de Bridge** dot11radio.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 al Grupo de Bridge con el mismo número de Grupo de Bridge (el "1" en este ejemplo) en la interfaz Fast Ethernet para pasar el tráfico del VLAN1 a través de la interfaz inalámbrica 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 a un Grupo de Bridge en la interfaz radio, estos comandos se fijan automáticamente.**Subscriber-loop-control del bridge-group** *1***bridge-group** *1 bloque-desconocido*-**fuenteningún bridge-group** *1 fuente*-**que aprendeningún bridge-group** *1* **Inundación de unidifusiónbridge-group** *1 atravesar*-**minusválidoNota:** Cuando usted configura a un Grupo de Bridge en la interfaz Fast Ethernet, estos comandos se fijan automáticamente.**ningún bridge-group** *1 fuente*-**que aprendebridge-group** *1 atravesar*-**minusválido**

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 interligar entre las interfaces Bridged en el mismo Grupo de Bridge, mientras que el tráfico del routable se puede rutear a otras interfaces ruteadas o Grupos de Bridge

Con los Ruteo y Bridging integrados, 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 al IRB en los untos de acceso de red inalámbrica y los Bridges para rutear su tráfico entre los Grupos de Bridge o entre las interfaces ruteadas y los Grupos de Bridge. Usted necesita un router externo o un switch de la capa 3 para rutear entre los Grupos de Bridge o entre los Grupos de Bridge y las interfaces ruteadas.

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

Irb del #bridge de AP(configure)

Los Ruteo y Bridging integrados utilizan el concepto de un (BVI) del Interfaz Virtual de Bridge-Group para rutear el tráfico entre las interfaces ruteadas y los Grupos de Bridge o entre los Grupos de Bridge.

Un BVI es una interfaz virtual dentro del router del switch de la capa 3 que actúa como una interfaz ruteada normal. Un BVI no soporta el bridging sino representa realmente al Grupo de Bridge correspondiente a las interfaces ruteadas 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 de Bridge 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 los Bridges.

1. Configure el BVI y asigne el número correspondiente del Grupo de Bridge al BVI. Este ejemplo asigna el Grupo de Bridge número 1 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 para validar y para rutear los paquetes enrutables recibidos de su Grupo de Bridge correspondiente.`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 VLAN nativo en quienes el AP está situado (en este ejemplo, el VLA N 1). Usted no necesitan un BVI para ninguna otra subinterfaz, con independencia de cuántos VLA N y los Grupos de Bridge usted configura en su AP/bridge. Esto es porque usted marca el tráfico con etiqueta en el resto de los VLA N (excepto el VLAN nativo) y le manda al Switch sin embargo una interfaz trunked del dot1q sobre la cara tela. Por ejemplo, si usted tiene 2 VLA N en su red, usted necesita a dos Grupos de Bridge, pero solamente un correspondiente BVI al VLAN de administración es suficiente en su red inalámbrica.Cuando usted habilita la encaminamiento para un protocolo dado en el Interfaz Virtual de Bridge Group, los paquetes que vienen de una interfaz ruteada, pero son destinados para un host en un dominio Bridged, se rutean al Interfaz Virtual de Bridge Group y se remiten a la interfaz Bridged correspondiente.Todo el tráfico que se rutea al Interfaz Virtual de Bridge Group se remite al Grupo de Bridge correspondiente como tráfico Bridged. Todo el tráfico del routable recibido en una interfaz Bridged se rutea a otras interfaces ruteadas como si venga directamente del Interfaz Virtual de Bridge Group.Refiera al bridging de la configuración para información más detallada sobre el bridging y el IRB.

Interacción con el Switches relacionado

En esta sección, le presentan con la información para configurar, o verifique la configuración de los switches Cisco que conectan con el Cisco Aironet el equipo de red inalámbrica.

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

Configuración del switch - Catalyst OS

Para configurar un Switch que funcione con el Catalyst OS a los VLA N del trunk a un Punto de acceso, la sintaxis de los comandos es **trunk determinado <module -/port -> en el dot1q** y el **trunk 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 — El IOS basó los switches de Catalyst

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

- Configure el switchport a los VLA N del trunk a un Punto de acceso
- En un switch de Catalyst que ejecuta el IOS
- 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 de red inalámbrica basado IOS del Cisco Aironet no soporta el Dynamic Trunking Protocol (DTP), así que el Switch no debe intentar negociarlo.

Configuración de switch - Catalyst 2900XL/3500XL

Del modo de configuración de la interfaz, ingrese estos comandos, si usted quiere configurar el switchport a los VLA N del trunk a un Punto de acceso en un Catalyst 2900XL o 3500XL Switch que ejecute 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#`
- 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 del Catalyst OS, **muestre el trunk <module -/port ->** — visualiza el estatus 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 IOS, **muestre el trunk del FastEthernet de la interfaz <module -/port ->** — visualiza el estatus 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 Catalyst 2900XL/3500XL Switch, **muestre el switchport del FastEthernet de la interfaz <module -/port ->** — visualiza el estatus 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#
```

Troubleshooting

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

Información Relacionada

- Configuración de las VLAN (Pautas de configuración del punto de acceso)
- Configurando los VLA N (guía de configuración de Bridge)
- Soporte técnico de conexión troncal
- Interacción con el Switches relacionado
- Requisitos del Sistema para Implementar el Trunking
- Descripción General del Bridging
- Tipos de autenticación inalámbricos en un ejemplo de configuración fijo ISR
- Tipos de autenticación inalámbricos en el ISR fijo con el ejemplo de la configuración de SDM
- Conectividad del Wireless LAN usando un ISR con el ejemplo de 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