

# Uso de VLANs com o Equipamento sem Fio Cisco Aironet.

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[VLAN](#)

[Significado do VLAN nativo](#)

[VLAN em Access point](#)

[Conceitos com Access point](#)

[Configuração do ponto de acesso](#)

[VLAN em pontes](#)

[Conceitos em pontes](#)

[Configuração de bridges](#)

[Use um servidor Radius para atribuir usuários aos VLAN](#)

[Use um servidor Radius para a atribuição dinâmica do grupo da mobilidade](#)

[Configuração do grupo de bridge em Access point e em pontes](#)

[Integrated Routing and Bridging \(IRB\)](#)

[Interação com Switches relacionado](#)

[Configuração de switch — Ósmio do catalizador](#)

[Configuração de switch — Os IO basearam Catalyst Switches](#)

[Configuração de switch — Catalizador 2900XL/3500XL](#)

[Verificar](#)

[Verifique o equipamento Wireless](#)

[Verifique o interruptor](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este original fornece uma configuração de exemplo para usar os LAN virtuais (VLAN) com equipamento Wireless do Cisco Aironet.

## [Pré-requisitos](#)

## Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Familiaridade com equipamento sem fio Cisco Aironet
- Familiaridade com os conceitos da Comutação LAN dos VLAN e do trunking VLAN

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Access point e bridges Wireless do Cisco Aironet
- Switches do Cisco catalyst

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Produtos Relacionados

Você pode usar o lado do interruptor desta configuração com qualquer um hardware ou software:

- Catalizador 6x00/5x00/4x00 que executa Cactos ou IO
- Catalizador 35x0/37x0/29xx que executa IO
- Catalizador 2900XL/3500XL que executa IO

## Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

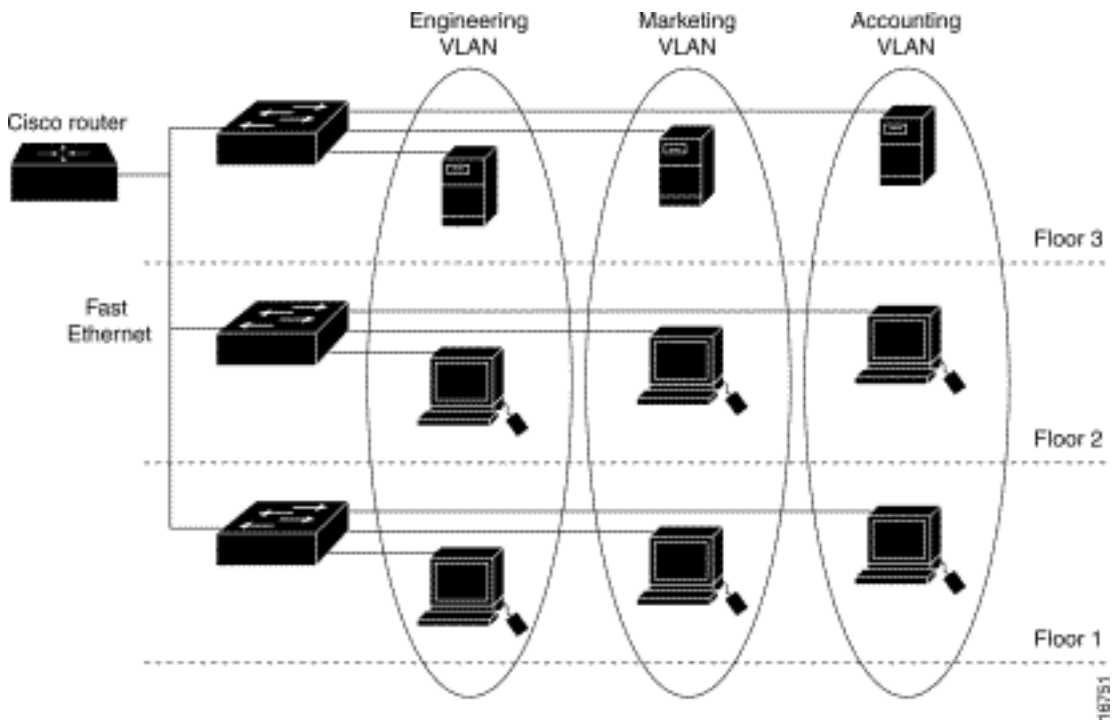
## VLAN

Um VLAN é uma rede comutada que seja segmentada logicamente por funções, por equipes de projeto, ou por aplicativos um pouco do que em uma base física ou geográfica. Por exemplo, todas as estações de trabalho e server usados por uma equipe particular do grupo de trabalho podem ser conectados ao mesmo VLAN, apesar de suas conexões física à rede ou ao fato de que podem ser misturadas com outras equipes. O uso VLAN reconfigurar a rede através do software um pouco do que fisicamente desconecta ou move os dispositivos ou os fios.

Um VLAN pode ser pensado como de um domínio de transmissão que exista dentro de um grupo definido de Switches. Um VLAN consiste em um número de sistemas finais, anfitriões ou equipamento de rede (tal como pontes e Roteadores), conectado por um único domínio de Bridging. O domínio de Bridging é apoiado em várias partes de equipamento de rede, tais como os switch LAN, que operam Bridging Protocols entre eles com um grupo separado para cada VLAN.

Quando você conecta um dispositivo a um interruptor do Cisco catalyst, a porta onde o dispositivo é conectado é um membro de VLAN 1. O MAC address desse dispositivo é parte de um VLAN1.

Você pode definir vlan múltiplos em um switch único, e você pode configurar uma porta de switch na maioria de modelos do Catalyst como um membro dos vlan múltiplos.



Quando o número de portas em uma rede excede a capacidade da porta do interruptor, você deve cruz-conectar o chassi de switch múltiplo, que define um tronco. O tronco não é um membro de nenhum VLAN, mas uma conduíte sobre que trafica passagens para uns ou vários VLAN.

Em termos fundamentais, a chave na configuração de um Access point a conectar a um VLAN específico é configurar seu SSID para reconhecer esse VLAN. Porque os VLAN são identificados por uma identificação VLAN ou por um nome, segue que, se o SSID em um Access point é configurado para reconhecer uma identificação VLAN ou um nome específico, uma conexão ao VLAN está estabelecida. Quando esta conexão é feita, os dispositivos do cliente Wireless associados que têm o mesmo SSID podem alcançar o VLAN através do Access point. O VLAN processa dados a e dos clientes a mesma maneira que processa dados a e das conexões ligadas com fio. Você pode configurar até 16 SSID em seu Access point, assim que você pode apoiar até 16 VLAN. Você pode atribuir somente um SSID a um VLAN.

Você estende VLAN em um Wireless LAN quando você adiciona a conscientização da etiqueta da IEEE 802.11Q ao Access point. Os quadros destinados para VLAN diferentes são transmitidos pelo Access point sem fio em SSID diferentes com chaves de WEP diferentes. Somente os clientes associados com esse VLAN recebem aqueles pacotes. Inversamente, os pacotes que vêm de um cliente associado com um determinado VLAN são 802.11Q etiquetados antes que estejam enviados na rede ligada com fio.

Por exemplo, funcionários e visitantes podem acessar a rede sem fio de uma companhia ao mesmo tempo estar separados administrativamente. Uma VLAN mapeia para um SSID e o cliente sem fio se conecta ao SSID apropriado. Nas redes com bridges Wireless, você pode passar vlan múltiplos através do enlace Wireless a fim fornecer a Conectividade a um VLAN dos lugar separados.

Se 802.1q é configurado na interface fastethernet de um Access point, o Access point envia sempre o Keepalives no VLAN1 mesmo se o VLAN1 não é definido no Access point. Em consequência, o Switch Ethernet conecta ao Access point e gerencie um mensagem de advertência. Não há nenhuma perda de função no Access point ou no interruptor, mas o log do

switch contém as mensagens sem sentido que podem fazer com que umas mensagens mais importantes sejam envolvidas e não consideradas.

Este comportamento cria um problema quando todos os SSID em um Access point são associados às redes da mobilidade. Se todos os SSID estão associados às redes da mobilidade, a porta de Ethernet switch a que o Access point está conectado podem ser configurados como uma porta de acesso. A porta de acesso é atribuída normalmente ao VLAN nativo do Access point, que não é necessariamente VLAN1. Isto faz com que o Switch Ethernet gerencie os mensagens de advertência que notam que o tráfego com uma etiqueta 802.1q está enviado do Access point.

Você pode eliminar as mensagens excessivas no interruptor se você desabilita a função de keepalive.

Se você ignora pontos menores nestes conceitos quando você distribui VLAN com o equipamento Wireless do Cisco Aironet, você pode experimentar desempenho inesperado, por exemplo:

- A falha limitar permitiu VLAN no tronco àqueles definidos no dispositivo WirelessSe os VLAN 1, o 10, 20, 30 e 40 são definidos no interruptor, mas somente em VLAN 1, o 10 e 30 estão definidos no equipamento Wireless, você deve remover o outro da porta de switch do tronco.
- Emprego errado da designação da infraestrutura SSIDQuando você instalar Access point, simplesmente atribua a infraestrutura SSID quando você usar um SSID sobre:dispositivos do bridge de grupo de trabalhoAccess point do repetidorbridges sem raizÉ um misconfiguration para designar a infraestrutura SSID para um SSID com somente os computadores laptop sem fio para clientes, e causa resultados imprevisíveis.Nas instalações da ponte, você pode somente ter uma infraestrutura SSID. A infraestrutura SSID deve ser o SSID que correlaciona ao VLAN nativo.
- Emprego errado ou projeto incorreto da designação de SSID do modo do convidadoQuando você define SSID/VLAN múltiplos no equipamento Wireless do Cisco Aironet, um (1) SSID pode ser atribuído como o modo SSID do convidado com a transmissão SSID em balizas de rádio do 802.11. Os outros SSID não são transmissão. Os dispositivos do cliente devem indicar que SSID a conectar.
- Falha ao reconhecer que VLANs e SSIDs múltiplos indicam sub-redes múltiplas da Camada 3 do Modelo OSIAs versões suplicadas do software do Cisco Aironet permitem ligar SSID múltiplos a um VLAN. As versões atual não fazem.
- Falhas de roteamento da camada 3 do modelo OSI ou projetos incorretosCada SSID e seu VLAN ligado devem ter um dispositivo de roteamento e alguma fonte para endereçar clientes, por exemplo um servidor DHCP ou o espaço em um servidor DHCP.
- Entenda mal ou configurar incorretamente o VLAN nativoO Roteadores e o Switches que compõem a infraestrutura física de uma rede são controlados em um método diferente do que os PCs do cliente que anexam a essa infraestrutura física. O VLAN este roteador e interfaces de switch é membros de é chamado o VLAN nativo (à revelia, VLAN1). Os PCs do cliente são membros de um VLAN diferente, apenas porque os telefones IP são membros de contudo um outro VLAN. A interface administrativa do Access point ou a ponte (relação BV11) são consideradas e numeraram parte do VLAN nativo apesar de que VLAN ou SSID passam através desse dispositivo Wireless.

## [Significado do VLAN nativo](#)

Quando você usa uma porta de tronco do IEEE 802.1Q, todos os quadros estão etiquetados a não ser que aqueles no VLAN configurado como o “VLAN nativo” para a porta. Os quadros no VLAN nativo são sempre sem etiqueta transmitido e são normalmente sem etiqueta recebido. Conseqüentemente, quando um AP é conectado ao switchport, o VLAN nativo configurado no AP deve combinar o VLAN nativo configurado no switchport.

**Nota:** Se há uma má combinação nos VLAN nativos, os quadros estão deixados cair.

Esta encenação é explicada melhor com um exemplo. Se o VLAN nativo no switchport é configurado como o VLAN 12 e no AP, o VLAN nativo está configurado como o VLAN1, a seguir quando o AP envia um quadro em seu VLAN nativo ao interruptor, o interruptor considera o quadro como pertencendo ao VLAN 12 desde que os quadros do VLAN nativo do AP são sem etiqueta. Isto causa a confusão na rede e os resultados nos problemas de conectividade. O mesmo acontecer quando o switchport para a frente um quadro de seu VLAN nativo ao AP.

A configuração do VLAN nativo torna-se ainda mais importante quando você tem um AP repetidor setup em sua rede Wireless. Você não pode configurar vlan múltiplos no repetidor APs. O repetidor APs apoia somente o VLAN nativo. Conseqüentemente, a configuração de VLAN nativa na raiz AP, a porta de switch a que o AP é conectado, e o AP repetidor, deve ser a mesma. Se não o tráfego através do interruptor não passa a e do AP repetidor.

Um exemplo para a encenação onde a má combinação na configuração de VLAN nativa do AP do repetidor pode criar problemas está quando há um servidor DHCP atrás do interruptor a que a raiz AP está conectada. Neste caso os clientes associados com o AP repetidor não recebem um IP address do servidor DHCP porque os quadros (requisições DHCP em nosso caso) do VLAN nativo do AP do repetidor (que não é o mesmo que a raiz AP e o interruptor) são deixados cair.

Igualmente, quando você configura a porta de switch, *assegure-se de que todos os VLAN que são configurados nos APs estejam permitidos no switchport*. Por exemplo, se os VLAN 6, 7, e 8 existem no AP (rede Wireless) os VLAN têm que ser permitidos no switchport. Isto pode ser feito usando este comando no interruptor:

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

À revelia, um switchport configurado como um tronco permite que todos os VLAN passem através da porta de tronco. Refira a [interação com Switches relacionado](#) para obter mais informações sobre de como configurar o switchport.

**Nota:** Permitir todos os VLAN no AP pode igualmente transformar-se um problema em alguns casos, especificamente se é uma rede grande. Isto pode conduzir à utilização da alta utilização da CPU nos APs. Pode os VLAN no interruptor de modo que somente o tráfego de VLAN que o AP está interessado nas passagens com o AP evitar a alta utilização da CPU.

## [VLAN em Access point](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Para encontrar informações adicionais sobre os comandos usados neste documento, use a [Command Lookup Tool](#) ([somente clientes registrados](#)).

## Conceitos com Access point

Esta seção discute conceitos sobre como distribuir VLAN em Access point e refere este diagrama da rede.

Neste exemplo de rede, o VLAN1 é o VLAN nativo, e os VLAN 10, 20, 30 e 40 existem, e são em tronco a um outro chassi do switch. Somente os VLAN 10 e 30 são prolongados no domínio Wireless. O VLAN nativo é exigido para fornecer a potencialidade de gerenciamento e as autenticações do cliente.

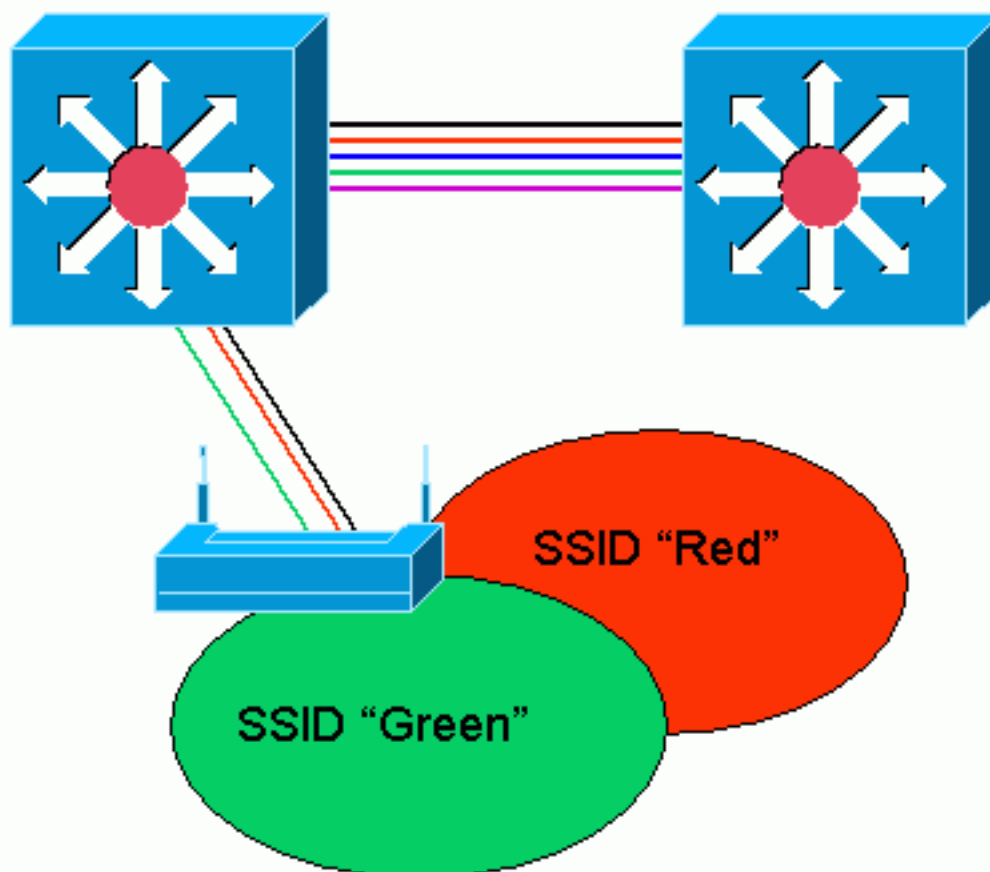
VLAN 1 (Native)

VLAN 10

VLAN 20

VLAN 30

VLAN 40

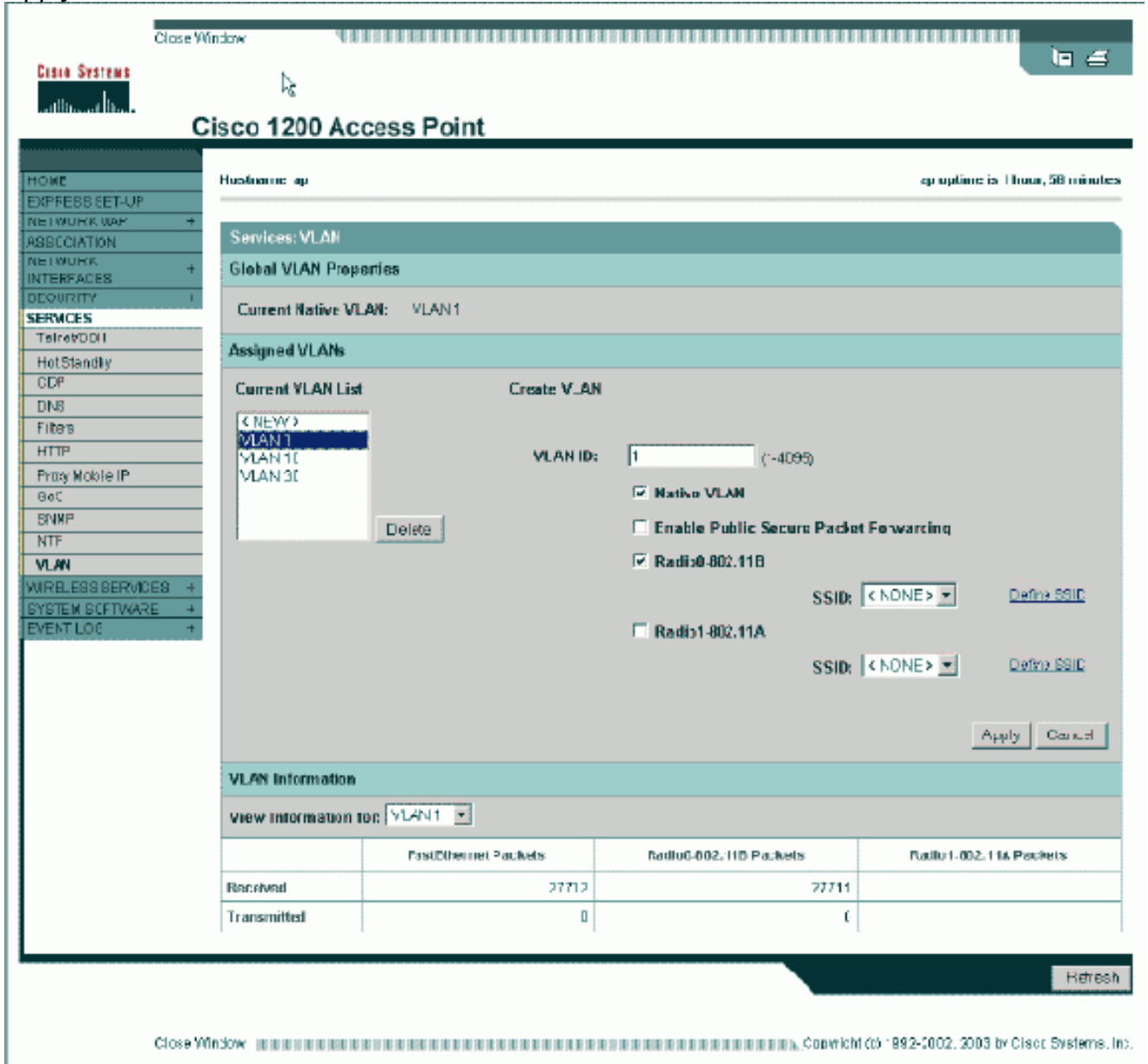


### Configuração do ponto de acesso

A fim configurar o Access point para VLAN, termine estas etapas:

1. Do AP GUI, clique os serviços > o VLAN a navegar aos **serviços**: Página **VLAN**.A primeira etapa é configurar o VLAN nativo. Da lista de VLAN atual, selecione **novo**. Digite o número da VLAN nativa na caixa VLAN ID. O número de VLAN deve combinar o VLAN nativo configurado no interruptor. Porque a relação BVI1 é associada ao subinterface do VLAN nativo, o IP address atribuído para conectar o BVI1 deve estar na **mesma sub-rede IP** que outros dispositivos de infraestrutura na rede (isto é, a relação SC0 em um Catalyst Switch

que executa Cactos.) Marque a caixa de seleção da VLAN nativa. Selecione caixas de seleção para a interface de rádio ou as relações onde este VLAN se aplica. Clique em Apply.



Ou, a partir do CLI, emita estes 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. A fim configurar outros VLAN, siga estas etapas: Da lista de VLAN atual, selecione novo. Insira o número do VLAN desejado na caixa ID do VLAN. O número de VLAN deve combinar um VLAN configurado no interruptor. Selecione caixas de seleção para a interface de rádio ou as relações onde este VLAN se aplica. Clique em Apply.

The screenshot shows the Cisco 1200 Access Point configuration web interface. The main content area is titled "Services: VLAN" and "Global VLAN Properties". It shows the "Current Native VLAN" as "VLAN 1". Under "Assigned VLANs", there is a "Current VLAN List" with a dropdown menu showing "VLAN 1" selected. To the right, there is a "Create VLAN" section with a "VLAN ID" field set to "10" (range 1-4095). There are checkboxes for "Native VLAN", "Enable Public Secure Packet Forwarding", "Radio 0-802.11B" (checked), and "Radio 1-802.11A". SSID fields are visible for each radio, with "Radio 0-802.11B" set to "Rad" and "Radio 1-802.11A" set to "< NONE >". At the bottom, the "VLAN Information" section shows a table for "VLAN 1" with columns for "FastEthernet Packets", "Radio 0-802.11B Packets", and "Radio 1-802.11A Packets". The table shows 77712 packets received and 0 transmitted for FastEthernet, and 77711 packets received and 0 transmitted for Radio 0-802.11B.

Ou, a partir do CLI, emita estes 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 as etapas 2a com o 2d para cada VLAN desejado ou incorpore estes comandos do CLI com mudanças apropriadas ao subinterface e aos 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. A próxima etapa é associar os VLAN configurados aos SSID. A fim fazer isto, **Segurança do clique > gerenciador de SSID**. Nota: Você não precisa de associar cada VLAN definido no



Access point com um SSID. Por exemplo, por razões de segurança, a maioria de instalações do Access point não associam um SSID com o VLAN nativo. A fim de criar um SSID novo, escolha **novo**. Incorpore o SSID desejado (diferença maiúscula e minúscula) à caixa SSID. Selecione o número da VLAN a ser associado a esse SSID a partir da lista suspensa. **Nota:** A fim de manter este original dentro de seu espaço pretendido, a Segurança para um SSID não é endereçada. Clique em Apply-RadioX para criar o SSID no rádio selecionado, ou Apply-all para criá-lo em todos os rádios.

The screenshot displays the Cisco 1200 Access Point web interface. The top navigation bar includes 'HOME', 'EXPRESS SETUP', 'NETWORK WAP', 'ASSOCIATION', 'NETWORK INTERFACES', 'SECURITY', 'SERVICES', 'WIRELESS SERVICES', 'SYSTEM SOFTWARE', and 'EVENT LOG'. The main content area is titled 'Cisco 1200 Access Point' and 'Security: SSID Manager - Radio0 802.11B'. The 'SSID Properties' section shows a 'Current SSID List' with a table containing '<NEW>', 'Green', and 'Red'. Below this are fields for 'SSID:' (set to 'Red'), 'VLAN:' (set to '10'), and 'Authentication Methods Accepted:' with checkboxes for 'Open Authentication', 'Shared Authentication', and 'Network EAP'. There are also sections for 'Authenticated Key Management' with radio buttons for 'None', 'UCKM: Mandatory', and 'WPA: Optional', and 'WPA Pre-shared Key' with radio buttons for 'ASCII' and 'Hexadecimal'. The 'Global Radio0 802.11B SSID Properties' section has dropdowns for 'Set Guest Mode SSID:' and 'Set Infrastructure SSID:', both set to '<NONE>', and a checkbox for 'Force Infrastructure Devices to associate only to this SSID'. Buttons for 'Apply-Radio0', 'Apply-All', 'Cancel', 'Delete-Radio0', and 'Delete-All' are visible.

Ou do CLI, emita estes 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 as etapas 3a com 3d para cada SSID desejado ou incorpore estes comandos do CLI com mudanças apropriadas ao 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
```

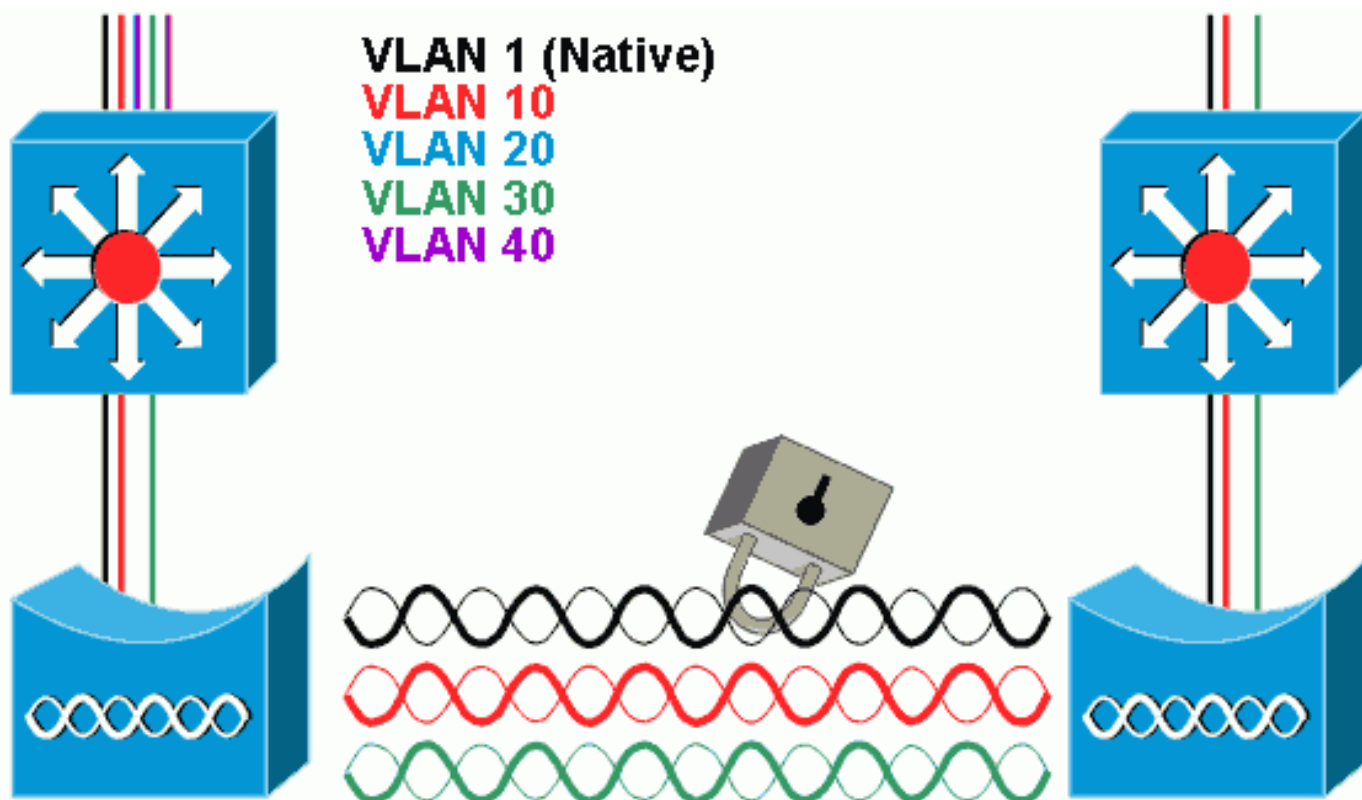
**Nota:** Estes exemplos não incluem a autenticação. Algum formulário de autenticação (aberto, Rede EAP) é exigido para que os clientes associem.

## VLAN em pontes

### Conceitos em pontes

Esta seção discute os conceitos relativos a como distribuir VLAN em pontes e refere este diagrama da rede.

Neste exemplo de rede, o VLAN1 é o VLAN nativo, e os VLAN 10, 20, 30 e 40 existem. Somente os VLAN 10 e 30 são estendidos ao outro lado da relação. O enlace Wireless é cifrado.



A fim cifrar os dados que passam sobre o link de rádio, aplique a criptografia somente ao SSID do

VLAN nativo. Essa criptografia aplica-se a todos VLAN restantes. Quando você ponte, lá não for nenhuma necessidade de associar um SSID separado com cada VLAN. As configurações de VLAN são as mesmas na raiz e em bridges sem raiz.

## Configuração de bridges

A fim configurar a ponte para VLAN, como o exemplo de diagrama de rede, termina estas etapas:

1. Do AP GUI, o clique **presta serviços de manutenção > VLAN** a navegar aos **serviços: Página VLAN**. A primeira etapa é configurar o VLAN nativo. A fim fazer isto, escolha o <New > da lista de VLAN atual. Digite o número da VLAN nativa na caixa VLAN ID. Isto deve combinar o VLAN nativo configurado no interruptor. Porque a relação BVI1 é associada ao subinterface do VLAN nativo, o IP address atribuído para conectar o BVI1 deve estar na **mesma sub-rede IP** que outros dispositivos de infraestrutura na rede (isto é a relação SC0 em um Catalyst Switch que executa Cactos.) Marque a caixa de seleção da VLAN nativa. Clique em Apply.

The screenshot displays the Cisco 1200 Access Point GUI for configuring VLANs. The interface includes a navigation menu on the left 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 shows 'Global VLAN Properties' with 'Current Native VLAN: VLAN1'. Under 'Assigned VLANs', there is a 'Current VLAN List' and a 'Create VLAN' section. The 'Create VLAN' section includes a 'VLAN ID' field set to '1', checkboxes for 'Native VLAN' (checked), 'Enable Public Secure Packet Forwarding' (unchecked), and 'Radio0-802.11B' (checked). There are two 'SSID' fields, both set to '<NONE>'. At the bottom, there is a 'VLAN Information' table showing statistics for 'FastEthernet Packets', 'Radio0-802.11B Packets', and 'Radio1-802.11A Packets'.

	FastEthernet Packets	Radio0-802.11B Packets	Radio1-802.11A Packets
Received	77712	77711	
Transmitted	0	0	

Ou, a partir do CLI, emita estes comandos:

```
bridge# configure terminal
```

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

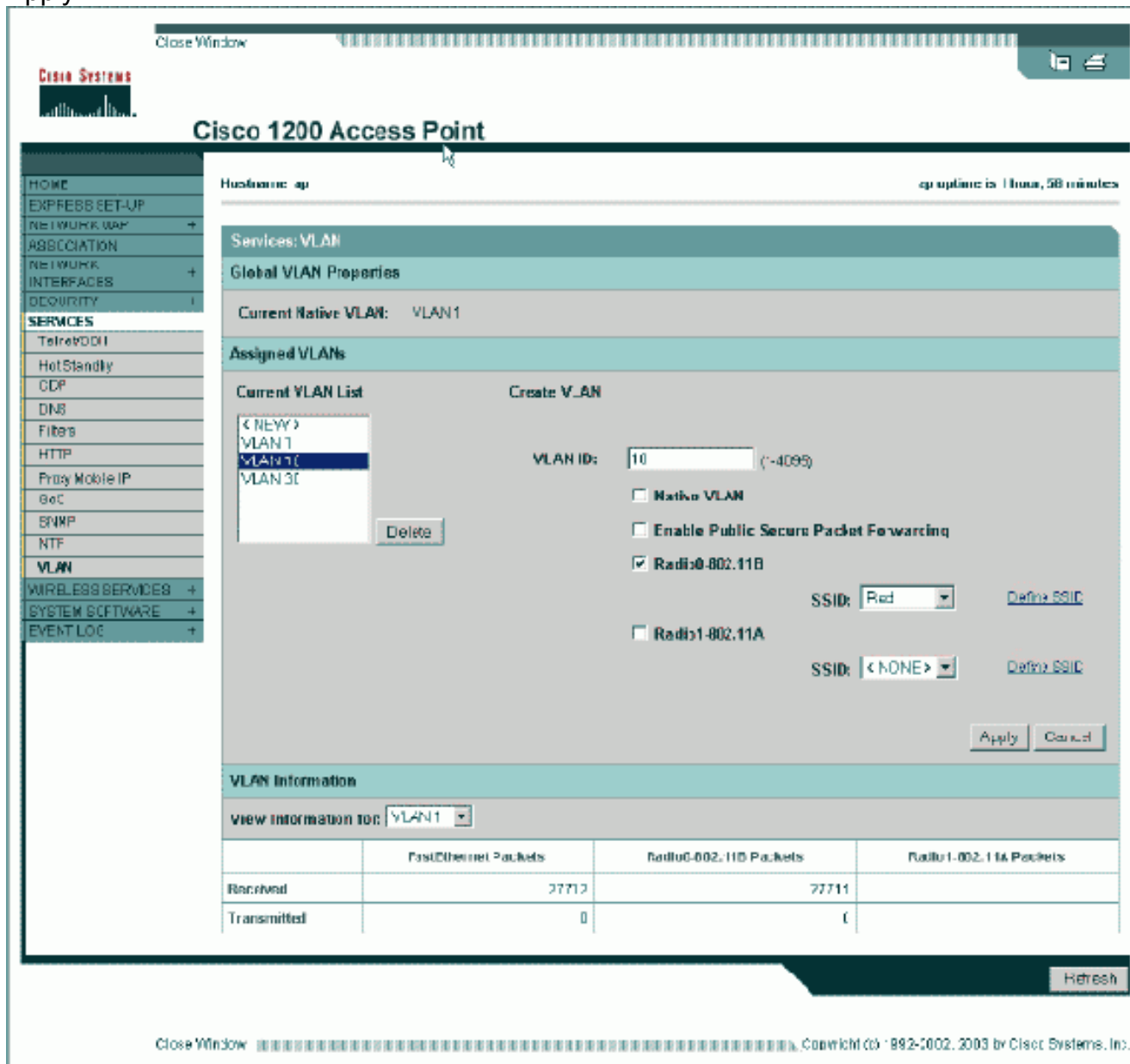
```
bridge(config)# interface Dot11Radio0.1
```

```

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. A fim configurar outros VLAN, siga estas etapas:Da lista de VLAN atual, selecione **nov**.Insira o número do VLAN desejado na caixa ID do VLAN. O número de VLAN deve combinar um VLAN configurado no interruptor.Clique em **Apply**.



Ou, a partir do CLI, emita estes 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 as etapas 2a com 2c para cada VLAN desejado ou incorpore os comandos do CLI com mudanças apropriadas ao subinterface e aos 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. Do gerenciador de SSID (sob o item de menu da **Segurança > do gerenciador de SSID,**) associe o VLAN nativo com um SSID. **Nota:** Quando você ponte, o único SSID que você deve associar com um VLAN for esse que correlaciona ao VLAN nativo. Você deve designar este SSID como a infraestrutura SSID. Da lista atual SSID, selecione **novo**. Incorpore o SSID desejado (diferencia maiúscula e minúscula) à caixa SSID. Selecione o número de VLAN que correlaciona ao VLAN nativo da lista suspensa. **Nota:** A fim manter este original dentro de seu espaço pretendido, a Segurança para um SSID não é endereçada. Clique **aplicam-se** para criar o SSID no rádio e para associá-lo ao VLAN nativo.

The screenshot shows the Cisco Aironet 1300 Series Wireless Bridge web interface. The page title is "Cisco Aironet 1300 Series Wireless Bridge". The hostname is "labbr1310ip93" and the uptime is "3 days, 18 hours, 45 minutes". The navigation menu on the left includes: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (highlighted), Admin Access, Encryption Manager, SSID Manager (selected), Server Manager, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Security: SSID Manager" and "SSID Properties". It features a "Current SSID List" table with a single entry: "< NEW >". To the right of the table are input fields for "SSID:" (containing "Black"), "VLAN:" (containing "1" with a dropdown arrow and a "Define VLANs" link), and "Network ID:" (containing "0-4096"). A "Delete" button is located below the table. Below the table is the "Authentication Settings" section, which includes "Authentication Methods Accepted:" with three options: "Open Authentication:" (checked), "Shared Authentication:" (unchecked), and "Network EAP:" (unchecked). Each option has a dropdown menu set to "< NO ADDITION >". At the bottom, there are sections for "Server Priorities:" with "EAP Authentication Servers" and "MAC Authentication Servers".

Enrole para trás para baixo a parte inferior da página, e sob o **Radio0-802.11G global SSID as propriedades** selecionam o **SSID da** lista suspensa da **infraestrutura SSID** do grupo. Clique em **Apply**.

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.

Ou do CLI, emita estes 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:** Quando os VLAN estão no uso, os SSID estão configurados sob a relação física Dot11Radio, não sob toda a subinterface lógica. **Nota:** Este exemplo não inclui a autenticação. A raiz e os bridges sem raiz exigem algum formulário de autenticação (abra, Rede EAP, etc.) a fim associar.

## [Use um servidor RADIUS para atribuir usuários aos VLAN](#)

Você pode configurar seu servidor de autenticação RADIUS para atribuir usuários ou grupos de usuários a um VLAN específico quando autenticam à rede. Para obter informações sobre esta característica, refira a seção [usando um servidor RADIUS para atribuir usuários aos VLAN do manual de configuração do software do Cisco IOS do original para Access point do Cisco Aironet, 12.4\(3g\)JA & 12.3\(8\)JEB](#).

## [Use um servidor RADIUS para a atribuição dinâmica do grupo da mobilidade](#)

Você pode igualmente configurar um servidor RADIUS para atribuir dinamicamente Grupos de mobilidade aos usuários ou aos grupos de usuário. Isto elimina a necessidade de configurar SSID múltiplos no Access point. Em lugar de, você precisa de configurar somente um SSID pelo Access point. Para obter informações sobre esta característica, refira a seção [usando um servidor RADIUS para a atribuição dinâmica do grupo da mobilidade do manual de configuração do software do Cisco IOS do original para Access point do Cisco Aironet, 12.4\(3g\)JA & 12.3\(8\)JEB](#).

## [Configuração do grupo de bridge em Access point e em pontes](#)

Geralmente, os grupos de bridge criam domínios de comutação segmentados. O tráfego é limitado aos anfitriões dentro de cada grupo de bridge, mas não entre os grupos de bridge. O interruptor trafica para a frente somente entre os anfitriões que compõem o grupo de bridge, que

restringe a transmissão e o tráfego multicast (inundação) somente 2 aqueles anfitriões. Os grupos de bridge aliviam o congestionamento de rede e fornecem a segurança de rede adicional quando segmentam o tráfego a determinadas áreas da rede.

Refira a [construção de uma ponte sobre da vista geral](#) para a informação detalhada.

Em uma rede Wireless, os grupos de bridge são configurados nos pontos de acesso Wireless e nas pontes para que o tráfego de dados de um VLAN a ser transmitido e vice-versa dos media sem fio à face da tela.

Execute esta etapa do AP CLI a fim permitir globalmente grupos de bridge na bridge/ponte de acesso.

Este exemplo usa o bridge-group number 1.

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

**Nota:** Você pode numerar seus grupos de bridge de 1 a 255.

Configurar a interface de rádio e a interface rápida de Ethernet do dispositivo Wireless para estar no mesmo grupo de bridge. Isto cria um trajeto entre estas duas relações diferentes, e estão no mesmo VLAN para etiquetar finalidades. Em consequência, os dados transmitidos do lado sem fio através da interface de rádio são transmitidos à interface Ethernet a que a rede ligada com fio é conectada e vice-versa. Ou seja rádio e interfaces Ethernet que pertencem à mesma ponte do grupo de bridge realmente os dados entre eles.

Em uma bridge/ponte de acesso, você precisa de ter um grupo de bridge pelo VLAN de modo que o tráfego possa passar do fio ao Sem fio e vice-versa. Mais o VLAN você tem essa necessidade de passar o tráfego através do Sem fio, mais grupos de bridge são precisados.

Por exemplo, se você tem somente um VLAN para passar o tráfego através do Sem fio à face da tela de sua rede, configurar somente um grupo de bridge do CLI do AP/bridge. Se você tem os vlan múltiplos para passar e vice-versa o tráfego do Sem fio à face da tela, configurar grupos de bridge para cada VLAN na secundário-relação de rádio, assim como a secundário-relação do Fast Ethernet.

1. Configurar o grupo de bridge na relação sem fio com o comando interface do **grupo de bridge dot11radio**. Este é um exemplo.

```
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. Configurar o grupo de bridge com o mesmo número de grupo de bridge ("1" neste exemplo) na interface rápida de Ethernet de modo que o tráfego VLAN1 seja passado através da relação sem fio a esta face da tela e 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:** Quando você configura um grupo de bridge na interface de rádio, estes comandos

estão ajustados automaticamente. **Subscriber-loop-control do ponte-grupo 1** **bloco-desconhecido-fonte do ponte-grupo 1** **nenhum ponte-grupo 1** **que aprende nenhuma inundação unicast do ponte-grupo 1** **medir-enfermos do ponte-grupo 1** **Nota:** Quando você configura um grupo de bridge na interface rápida de Ethernet, estes comandos estão ajustados automaticamente. **nenhum ponte-grupo 1** **que aprende medir-enfermos do ponte-grupo 1**

## [Integrated Routing and Bridging \(IRB\)](#)

O Integrated Routing and Bridging torna possível distribuir um protocolo específico entre interfaces roteada e grupos de bridge, ou distribui um protocolo específico entre grupos de bridge. O Local ou o tráfego irrastrável podem ser construídos uma ponte sobre entre as interfaces interligada no mesmo grupo de bridge, quando o tráfego do roteável puder ser distribuído a outros interfaces roteada ou grupos de bridge

Com Integrated Routing and Bridging, você pode fazer este:

- Comute pacotes de uma interface interligada a uma interface roteada
- Comute pacotes de uma interface roteada a uma interface interligada
- Comute pacotes dentro do mesmo grupo de bridge

Permita o IRB nos pontos de acesso Wireless e nas pontes a fim distribuir seu tráfego entre grupos de bridge ou entre interfaces roteada e grupos de bridge. Você precisa um roteador externo ou um switch de camada 3 a fim distribuir entre grupos de bridge ou entre grupos de bridge e interfaces roteada.

Emita este comando a fim permitir o IRB no AP/bridge.

**Irb do #bridge de AP(configure)**

O Integrated Routing and Bridging usa o conceito de um Bridge Group Virtual Interface (BVI) a fim distribuir o tráfego entre interfaces roteada e grupos de bridge ou entre grupos de bridge.

Um BVI é uma interface virtual dentro do roteador do switch de camada 3 que atua como uma interface roteada normal. Um BVI não apoia a construção de uma ponte sobre mas representa realmente o grupo de bridge correspondente às interfaces roteada dentro do roteador do switch de camada 3. Tem todos os atributos da camada de rede (tais como um endereço de camada de rede e filtros) que se aplicam ao grupo de bridge correspondente. O número de interface atribuído a esta interface virtual corresponde ao grupo de bridge que esta interface virtual representa. Este número é a relação entre a interface virtual e o grupo de bridge.

Execute estas etapas a fim configurar o BVI em Access point e em pontes.

1. Configurar o BVI e atribua o número correspondente do grupo de bridge ao BVI. Este exemplo atribui o grupo de bridge número 1 ao 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 um BVI de aceitar e distribuir os pacotes do roteável recebidos de seu grupo de bridge correspondente.

```
Ap(config)# bridge 1 route ip!---
!--- This example enables the BVI to accept and route the IP packet.
```



É importante compreender que você precisa somente um BVI para o Gerenciamento/VLAN nativo em que o AP é ficado situado (neste exemplo, VLAN1). Você não precisa um BVI para nenhum outro subinterface, independentemente de quantos VLAN e os grupos de bridge você configura em seu AP/bridge. Isto é porque você etiqueta o tráfego em todos VLAN restantes (exceto o VLAN nativo) e lhe envia para fora ao interruptor embora uma relação do em tronco do dot1q na face da tela. Por exemplo, se você tem 2 VLAN em sua rede, você precisa dois grupos de bridge, mas somente um correspondente BVI ao VLAN de gerenciamento é suficiente em sua rede Wireless. Quando você permite o roteamento para um protocolo dado no Bridge Group Virtual Interface, os pacotes que vêm de uma interface roteada, mas são destinados para um host em um domínio interligado, estão distribuídos ao Bridge Group Virtual Interface e enviados à interface interligada correspondente. Todo o tráfego que é distribuído ao Bridge Group Virtual Interface é enviado ao grupo de bridge correspondente como o tráfego interligado. Todo o tráfego do roteável recebido em uma interface interligada é distribuído a outras interfaces roteada como se vem diretamente do Bridge Group Virtual Interface. Consulte [para configurar a construção de uma ponte sobre](#) para informações mais detalhadas sobre a construção de uma ponte sobre e do IRB.

## Interação com Switches relacionado

Nesta seção, você é apresentado com a informação para configurar, ou verifica a configuração dos switch Cisco que conectam ao Cisco Aironet o equipamento Wireless.

**Nota:** Para encontrar informações adicionais sobre os comandos usados neste documento, use a [Command Lookup Tool](#) ([somente clientes registrados](#)).

## Configuração de switch — Ósmio do catalizador

A fim configurar um interruptor que execute o ósmio do catalizador ao tronco VLAN a um Access point, a sintaxe de comando é *#> **ajustado do** <module #/port do tronco no dot1q e na lista <vlan do #> do <module #/port do tronco do grupo >*.

Um exemplo ao exemplo de diagrama de rede, é:

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

## Configuração de switch — Os IO basearam Catalyst Switches

Do modo de configuração da interface, incorpore estes comandos, se você quer a:

- Configurar o switchport ao tronco VLAN a um Access point
- Em um Catalyst Switch que executa IO
- O CatIOS inclui mas não é limitado 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:** O equipamento Wireless baseado IO do Cisco Aironet não apoia o Dynamic Trunking Protocol (DTP), assim que o interruptor não deve tentar negociá-lo.

## Configuração de switch — Catalizador 2900XL/3500XL

Do modo de configuração da interface, incorpore estes comandos, se você quer configurar o switchport ao tronco VLAN a um Access point em um Catalyst 2900XL ou 3500XL Switch que execute IO:

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

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

## Verifique o equipamento Wireless

- **mostra vlan** — indica todos os VLAN configurados atualmente no Access point, e seu 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#

- **mostre associações do dot11** — informação dos indicadores sobre clientes associados, pelo SSID/VLAN

```
ap#show dot11 associations
```

```
802.11 Client Stations on Dot11Radio0:
```

```
SSID [Green] :
```

```
SSID [Red] :
```

```
Others: (not related to any ssid)
```

ap#

## Verifique o interruptor

- Em um ósmio do catalizador baseou o interruptor, **mostram o #> do <module #/port do tronco** — indica o estado de um tronco em uma porta dada

```
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)
```

- No os IO baseados comutam, **mostram o tronco do #> do <module #/port do fastethernet da relação** — indica o estado de um tronco em uma dada interface

```
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#

- Em um interruptor do catalizador 2900XL/3500XL, **mostre o switchport do #> do <module #/port do fastethernet da relação** — indica o estado de um tronco em uma dada interface

```
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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- [Configurando VLAN \(guia de configuração do ponto de acesso\)](#)
- [Configurando VLAN \(guia de configuração de bridges\)](#)
- [Suporte técnico de entroncamento](#)
- [Interação com Switches relacionado](#)
- [Requisitos de sistema para implementar o entroncamento](#)
- [Vista geral da construção de uma ponte sobre](#)
- [Tipos do autenticação sem fio em um exemplo de configuração fixo ISR](#)
- [Tipos do autenticação sem fio em ISR fixo com o exemplo da configuração de SDM](#)
- [Conectividade do Wireless LAN usando um ISR com exemplo de configuração da criptografia de WEP e da autenticação de leap](#)
- [Exemplo de Configuração de Conexão de LAN Wireless Básica](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)