Uso de VLANs com o Equipamento sem Fio Cisco Aironet.

Contents

Introduction

Este documento fornece um exemplo de configuração para usar LANs virtuais (VLANs) com equipamento sem fio Cisco Aironet.

Prerequisites

Requirements

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

- Familiaridade com equipamento sem fio Cisco Aironet
- Familiaridade com conceitos de switching de LAN de VLANs e entroncamento de VLANs

Componentes Utilizados

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

- Pontos de Acesso e Pontes Sem Fio do Cisco Aironet
- Cisco Catalyst Switches

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

Produtos Relacionados

Você pode usar o lado do switch desta configuração com qualquer um destes itens de hardware ou software:

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

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

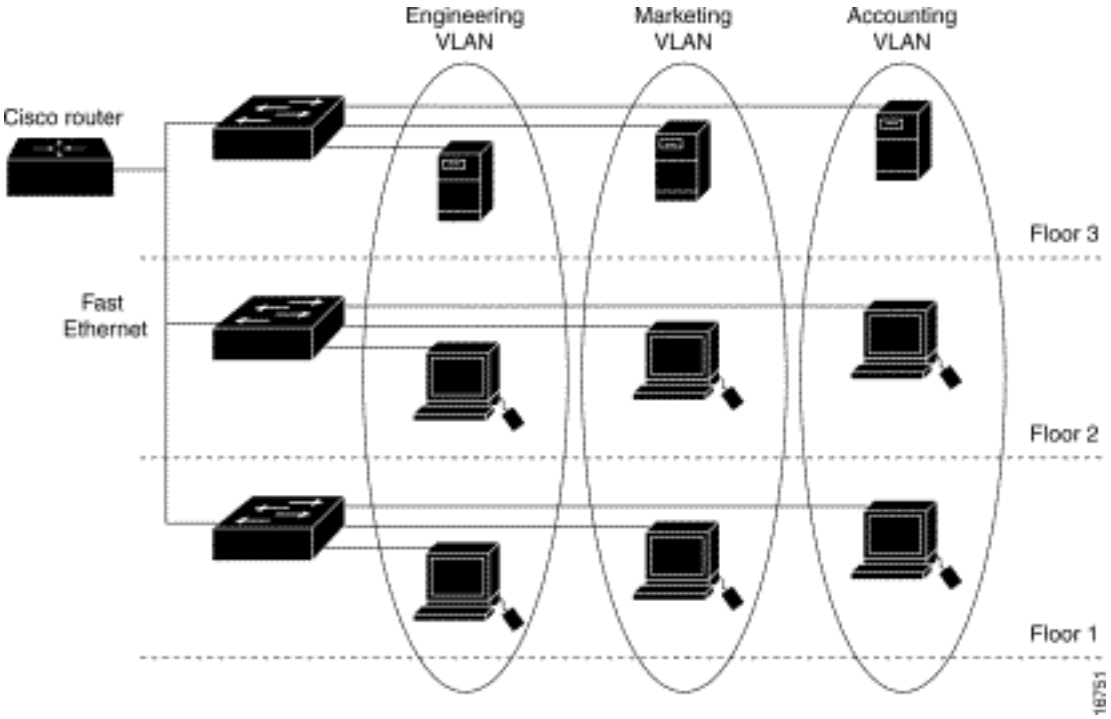
VLANs

Uma VLAN é uma rede comutada que é logicamente segmentada por funções, equipes de projetos ou aplicativos, em vez de uma base física ou geográfica. Por exemplo, todas as estações de trabalho e servidores usados por um grupo de trabalho em particular podem ser conectados à mesma VLAN, independentemente de suas conexões físicas com a rede ou do fato de que podem ser mesclados com outras equipes. Use VLANs para reconfigurar a rede por meio de software em vez de desconectar fisicamente ou mover os dispositivos ou fios.

Uma VLAN pode ser considerada um domínio de broadcast que existe dentro de um conjunto definido de switches. Uma VLAN consiste em vários sistemas finais, hosts ou equipamentos de rede (como bridges e roteadores), conectados por um único domínio de bridging. O domínio de bridging é suportado em vários equipamentos de rede, como switches LAN, que operam protocolos de bridging entre eles com um grupo separado para cada VLAN.

Quando você conecta um dispositivo a um switch Cisco Catalyst, a porta onde o dispositivo está conectado é um membro da VLAN 1. O endereço MAC desse dispositivo é uma parte do VLAN 1. É possível definir várias VLANs em um único Switch e configurar uma porta de Switch na maioria

dos modelos Catalyst como um membro de várias VLANs.



Quando o número de portas em uma rede excede a capacidade da porta do switch, você deve conectar vários chassis do switch em conexão cruzada, o que define um tronco. O tronco não é um membro de qualquer VLAN, mas uma canalização pela qual passa o tráfego de uma ou mais VLANs.

Em termos fundamentais, a chave na configuração de um ponto de acesso para se conectar a uma VLAN específica é configurar seu SSID para reconhecer essa VLAN. Como as VLANs são identificadas por um ID ou nome de VLAN, a seguir, se o SSID em um ponto de acesso é configurado para reconhecer um ID ou nome de VLAN específico, uma conexão com a VLAN é estabelecida. Quando essa conexão é feita, os dispositivos clientes sem fio associados que têm o mesmo SSID podem acessar a VLAN através do ponto de acesso. A VLAN processa dados de e para os clientes da mesma forma que processa dados de e para conexões com fio. Você pode configurar até 16 SSIDs em seu ponto de acesso, para que possa suportar até 16 VLANs. Você pode atribuir apenas um SSID a uma VLAN.

Você estende as VLANs para uma LAN sem fio ao adicionar o reconhecimento de marca IEEE 802.11Q ao ponto de acesso. Os quadros destinados a diferentes VLANs são transmitidos pelo ponto de acesso sem fio em diferentes SSIDs com diferentes chaves WEP. Somente os clientes associados a essa VLAN recebem esses pacotes. Por outro lado, os pacotes que vêm de um cliente associado a uma determinada VLAN são marcados como 802.11Q antes de serem encaminhados para a rede 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. Em redes com pontes sem fio, você pode passar várias VLANs pelo link sem fio para fornecer conectividade a uma VLAN de locais separados.

Se 802.1q for configurado na interface FastEthernet de um ponto de acesso, o ponto de acesso sempre enviará keepalives em VLAN1, mesmo que a VLAN 1 não esteja definida no ponto de acesso. Como resultado, o switch Ethernet se conecta ao ponto de acesso e gera uma mensagem de aviso. Não há perda de função no access point ou no switch, mas o log do switch contém mensagens sem significado que podem fazer com que mensagens mais importantes

sejam encapsuladas e não vistas.

Esse comportamento cria um problema quando todos os SSIDs em um ponto de acesso estão associados a redes de mobilidade. Se todos os SSIDs estiverem associados às redes de mobilidade, a porta do switch Ethernet à qual o ponto de acesso está conectado pode ser configurada como uma porta de acesso. A porta de acesso é normalmente atribuída à VLAN nativa do ponto de acesso, que não é necessariamente VLAN1. Isso faz com que o switch Ethernet gere mensagens de aviso observando que o tráfego com uma marca 802.1q é enviado do ponto de acesso.

Você pode eliminar as mensagens excessivas no switch se desativar a função de keepalive.

Se você ignorar pontos secundários nesses conceitos ao implantar VLANs com equipamento sem fio Cisco Aironet, poderá experimentar um desempenho inesperado, por exemplo:

- A falha ao limitar VLANs permitidas no tronco às definidas no dispositivo sem fioSe as VLANs 1, 10, 20, 30 e 40 estiverem definidas no switch, mas somente as VLANs 1, 10 e 30 estiverem definidas no equipamento sem fio, você deverá remover as outras da porta do switch de tronco.
- Utilização abusiva da designação de SSID de infraestruturaAo instalar pontos de acesso, atribua apenas o SSID da infraestrutura quando usar um SSID em:dispositivos de bridge de grupo de trabalhopontos de acesso de repetidorbridges não raizÉ um erro de configuração designar o SSID da infraestrutura para um SSID com apenas computadores laptop sem fio para clientes e causa resultados imprevisíveis.Em instalações de ponte, você pode ter apenas um SSID de infraestrutura. O SSID da infraestrutura deve ser o SSID que se correlaciona à VLAN nativa.
- Uso incorreto ou design incorreto da designação SSID do modo convidadoQuando você define múltiplos SSIDs/VLANs no equipamento sem fio Cisco Aironet, um (1) SSID pode ser atribuído como SSID modo convidado, com o broadcast SSID de sinais de rádio 802.11. Os outros SSIDs não são transmitidos. Os dispositivos clientes devem indicar o SSID para conexão.
- Falha ao reconhecer que VLANS e SSIDs múltiplos indicam sub-redes múltiplas da Camada 3 do Modelo OSIVersões obsoletas do software Cisco Aironet permitem vincular vários SSIDs a uma VLAN. As versões atuais, não.
- Falhas de roteamento de Camada 3 do Modelo OSI ou projetos incorretosCada SSID e sua VLAN vinculada devem ter um dispositivo de roteamento e alguma origem para endereçar clientes, por exemplo, um servidor DHCP ou o escopo em um servidor DHCP.
- Engano ou configuração incorreta da VLAN nativaOs roteadores e Switches que compõem a infra-estrutura física de uma rede são gerenciados em um método diferente que os PCs cliente conectados a tal infra-estrutura. O VLAN do qual essas interfaces de Switch e roteador são membros é chamado de VLAN Nativo (por padrão, VLAN 1). Os PCs clientes são membros de uma VLAN diferente, assim como os telefones IP são membros de outra VLAN. A interface administrativa do ponto de acesso ou da ponte (interface BVI1) foi considerada e numerou uma parte do VLAN Nativo, independentemente de quais VLANs ou SSIDs passaram pelo dispositivo sem fio.

Significado da VLAN nativa

Quando você usa uma porta de tronco IEEE 802.1Q, todos os quadros são marcados, exceto os

na VLAN configurada como "VLAN nativa" para a porta. Os quadros na VLAN nativa são sempre transmitidos sem marcação e normalmente recebidos sem marcação. Portanto, quando um AP é conectado à porta do switch, a VLAN nativa configurada no AP deve corresponder à VLAN nativa configurada na porta do switch.

Observação: se houver uma incompatibilidade nas VLANs nativas, os quadros serão descartados.

Esse cenário é melhor explicado com um exemplo. Se a VLAN nativa na porta do switch estiver configurada como VLAN 12 e no AP, a VLAN nativa será configurada como VLAN 1, então quando o AP enviar um quadro em sua VLAN nativa para o switch, o switch considerará o quadro como pertencente à VLAN 12, já que os quadros da VLAN nativa do AP não são marcados. Isso causa confusão na rede e resulta em problemas de conectividade. O mesmo acontece quando a porta do switch encaminha um quadro de sua VLAN nativa para o AP.

A configuração da VLAN nativa torna-se ainda mais importante quando você tem uma configuração de AP de Repetidor em sua rede sem fio. Não é possível configurar várias VLANs nos APs do repetidor. Os APs de repetidor suportam somente a VLAN nativa. Portanto, a configuração de VLAN nativa no AP raiz, a porta do switch ao qual o AP está conectado e o AP do repetidor devem ser iguais. Caso contrário, o tráfego através do switch não passa de e para o AP do repetidor.

Um exemplo para o cenário em que a incompatibilidade na configuração de VLAN nativa do AP do Repetidor pode criar problemas é quando há um servidor DHCP atrás do switch ao qual o AP raiz está conectado. Nesse caso, os clientes associados ao AP do repetidor não recebem um endereço IP do servidor DHCP porque os quadros (solicitações DHCP no nosso caso) da VLAN nativa do AP do repetidor (que não é o mesmo do AP raiz e do switch) são descartados.

Além disso, ao configurar a porta do switch, *certifique-se de que todas as VLANs configuradas nos APs sejam permitidas na porta do switch.* Por exemplo, se as VLANs 6, 7 e 8 existirem no AP (Rede sem fio), as VLANs devem ser permitidas na porta do switch. Isso pode ser feito usando este comando no switch:

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

Por padrão, uma porta de switch configurada como um tronco permite que todas as VLANs passem pela porta de tronco. Consulte Interação com Switches Relacionados para obter mais informações sobre como configurar a porta do switch.

Observação: permitir todas as VLANs no AP também pode se tornar um problema em alguns casos, especificamente se for uma rede grande. Isso pode resultar em alta utilização da CPU nos APs. Remova as VLANs no switch de modo que somente o tráfego de VLAN no qual o AP está interessado passe pelo AP para evitar a alta CPU.

VLANs em pontos de acesso

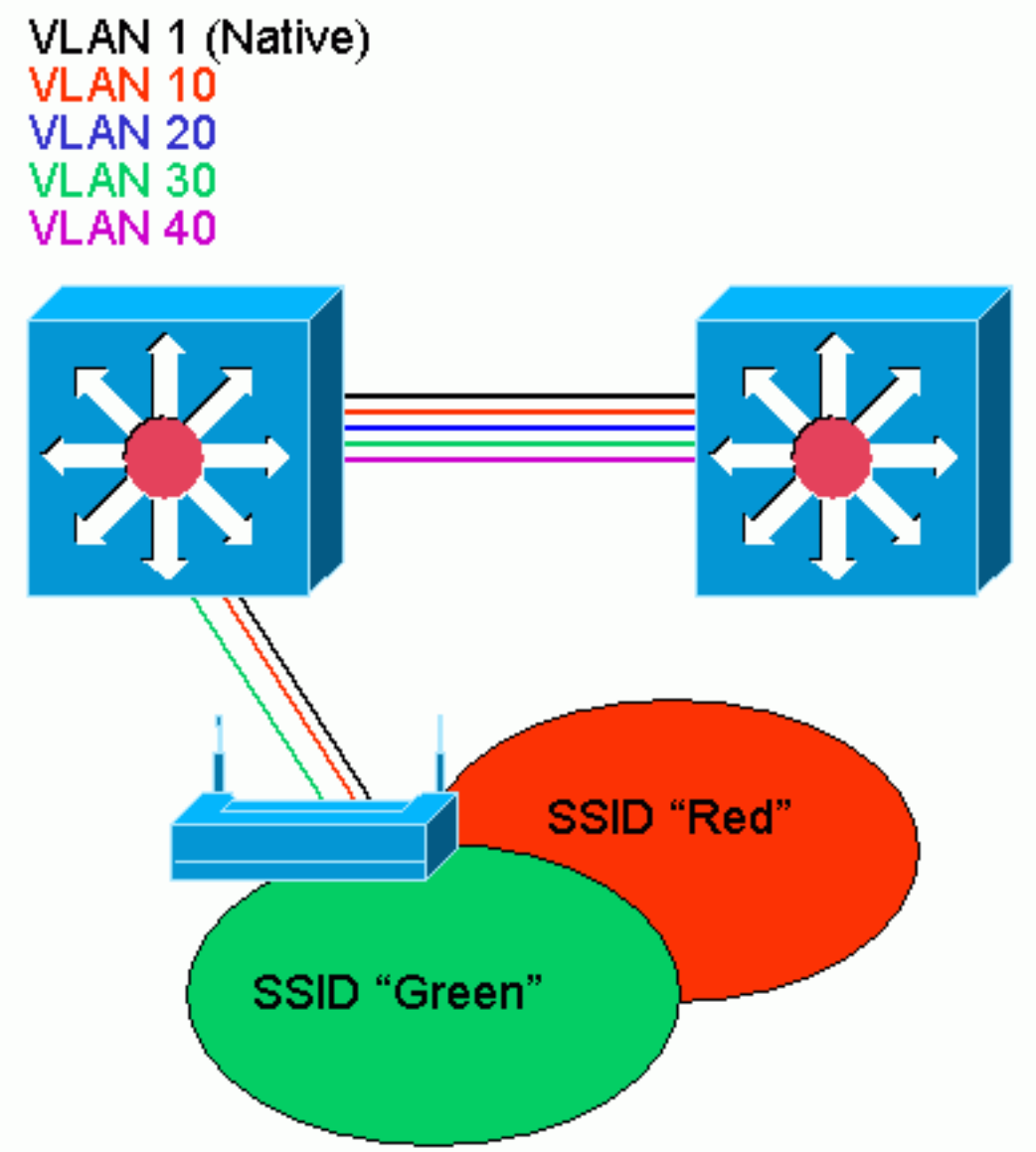
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados) .

Conceitos com access points

Esta seção discute conceitos sobre como implantar VLANs em pontos de acesso e se refere a este diagrama de rede.

Nesta rede de exemplo, a VLAN 1 é a VLAN nativa, e as VLANs 10, 20, 30 e 40 existem e estão entroncadas em outro chassi de switch. Somente as VLANs 10 e 30 são estendidas no domínio sem fio. A VLAN nativa é necessária para fornecer recursos de gerenciamento e autenticações de clientes.

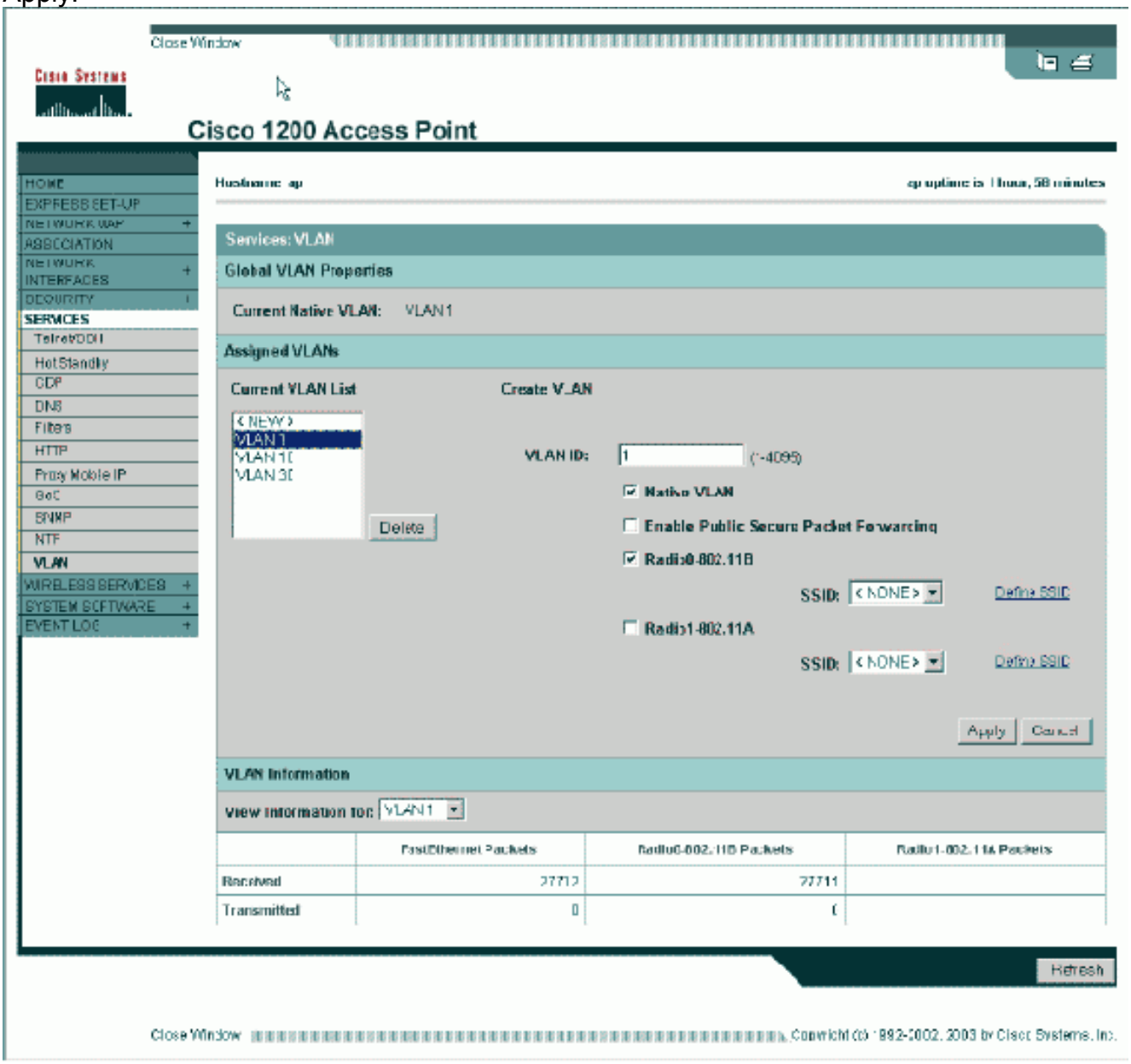


Configuração do ponto de acesso

Para configurar o ponto de acesso para VLANs, faça o seguinte:

1. Na GUI do AP, clique em Serviços > VLAN para navegar até **Serviços:** Página **VLAN** .A primeira etapa é configurar a VLAN nativa. Na Lista de VLANs atuais, selecione **Novo**.Digite o número da VLAN nativa na caixa VLAN ID. O número da VLAN deve corresponder à VLAN nativa configurada no switch.Como a interface BVI 1 está associada à subinterface da VLAN Nativa, o endereço IP atribuído à interface BVI 1 deve estar na **mesma sub-rede IP** que outros dispositivos de infraestrutura na rede (ou seja, a interface SC0 em um switch Catalyst

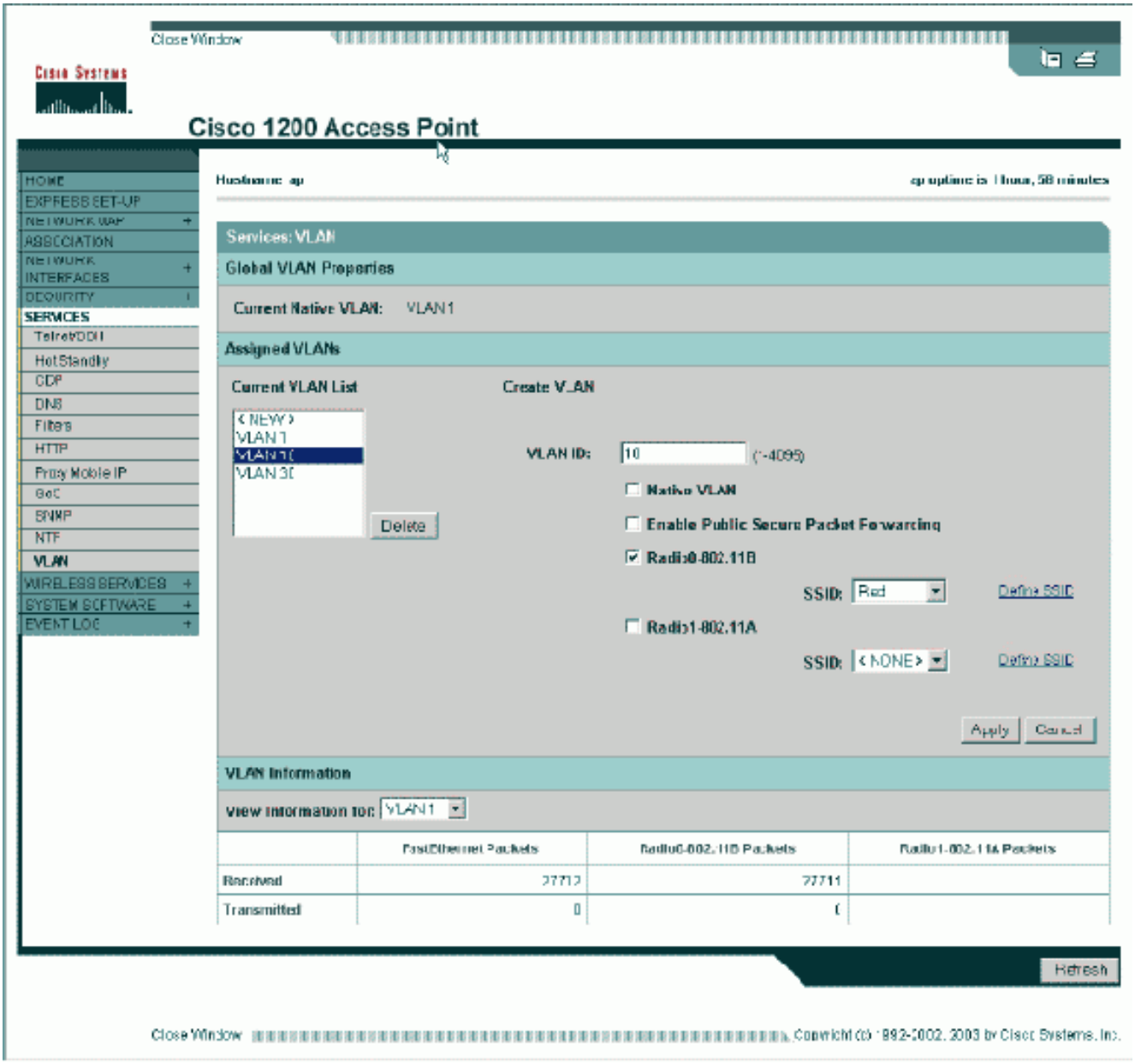
que executa CatOS).Marque a caixa de seleção da VLAN nativa.Marque as caixas de seleção para a interface de rádio ou as interfaces em que essa VLAN se aplica.Clique em Apply.



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. Para configurar outras VLANs, siga estas etapas:Na Lista de VLANs atuais, selecione **Novo**.Insira o número do VLAN desejado na caixa ID do VLAN. O número da VLAN deve corresponder a uma VLAN configurada no switch.Marque as caixas de seleção para a interface de rádio ou as interfaces em que essa VLAN se aplica.Clique em Apply.



Ou, a partir do CLI, emita estes comandos:

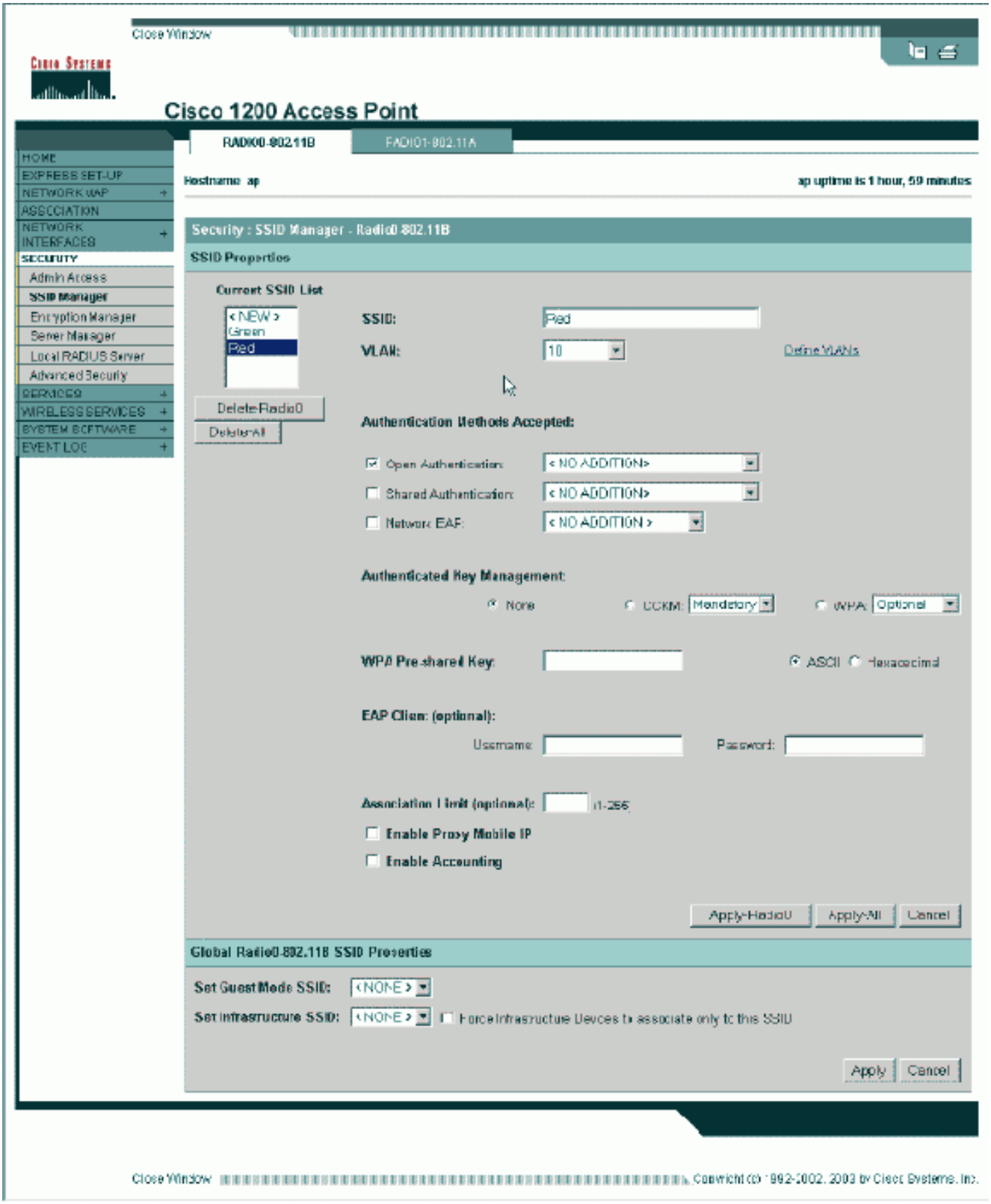
```
AP# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP(config)# interface Dot11Radio0.10
AP(config-subif)# encapsulation dot1Q 10
AP(config-subif)# interface FastEthernet0.10
AP(config-subif)# encapsulation dot1Q 10
AP(config-subif)# end
AP# write memory
```

Repita as etapas de 2a a 2d para cada VLAN desejada ou insira estes comandos do CLI com as alterações apropriadas na subinterface e nos 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 as VLANs configuradas aos SSIDs. Para fazer isso, clique em **Security > SSID Manager**.**Observação:** você não precisa associar cada VLAN definida no

ponto de acesso a um SSID. Por exemplo, por motivos de segurança, a maioria das instalações de ponto de acesso não associa um SSID à VLAN nativa.Para criar um novo SSID, escolha **Novo**.Digite o SSID desejado (diferencia maiúsculas de minúsculas) na caixa SSID.Selecione o número da VALN a ser associado a esse SSID a partir da lista suspensa.**Observação:** para manter este documento dentro do escopo pretendido, a segurança de 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.



Ou na 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 de 3a a 3d para cada SSID desejado ou insira esses comandos do CLI com as alterações apropriadas no 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
```

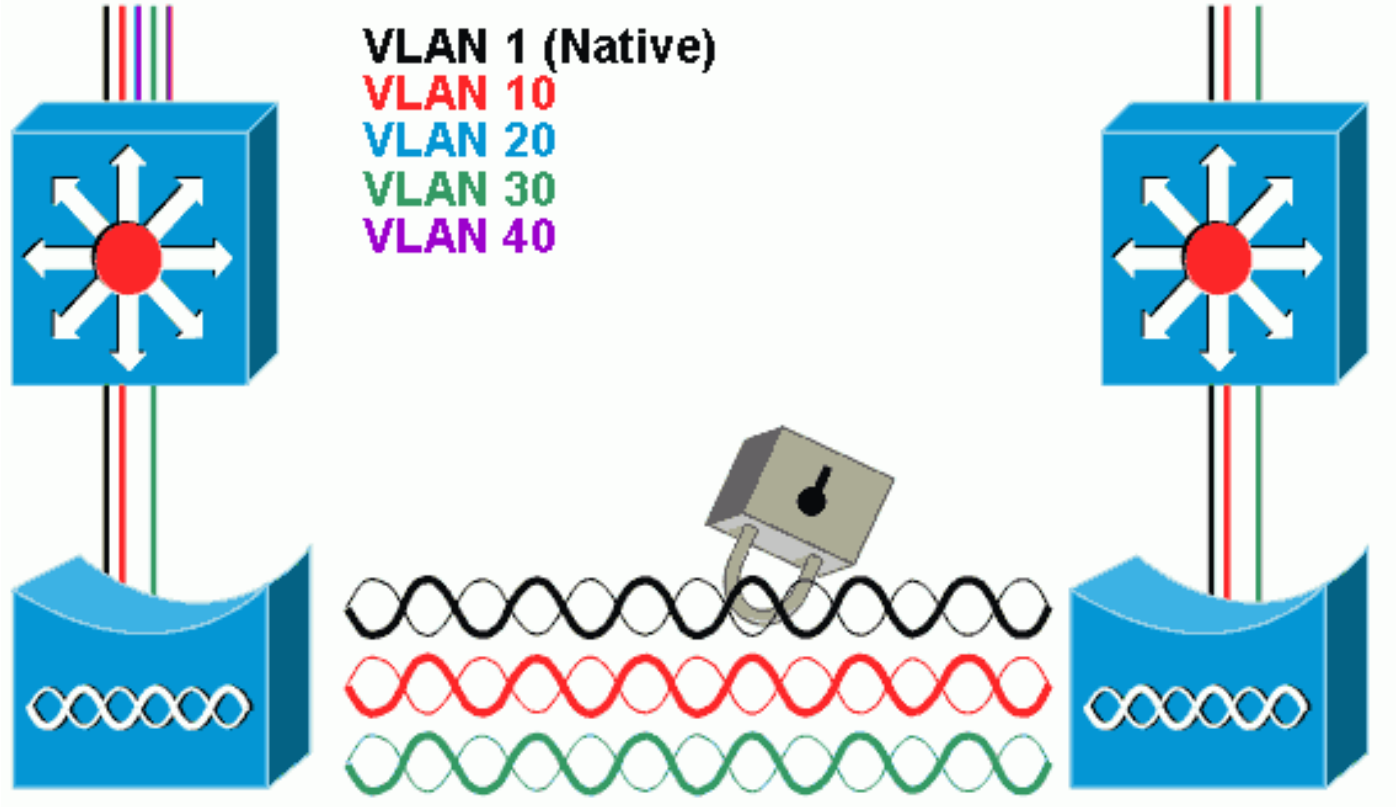
Observação: esses exemplos não incluem autenticação. Alguma forma de autenticação (aberta, EAP de rede) é necessária para que os clientes se associem.

VLANs em bridges

Conceitos em pontes

Esta seção discute conceitos relacionados a como implantar VLANs em bridges e se refere a este diagrama de rede.

Nesta rede de exemplo, a VLAN 1 é a VLAN nativa e as VLANs 10, 20, 30 e 40 existem. Somente as VLANs 10 e 30 são estendidas para o outro lado do link. O link sem fio está criptografado.



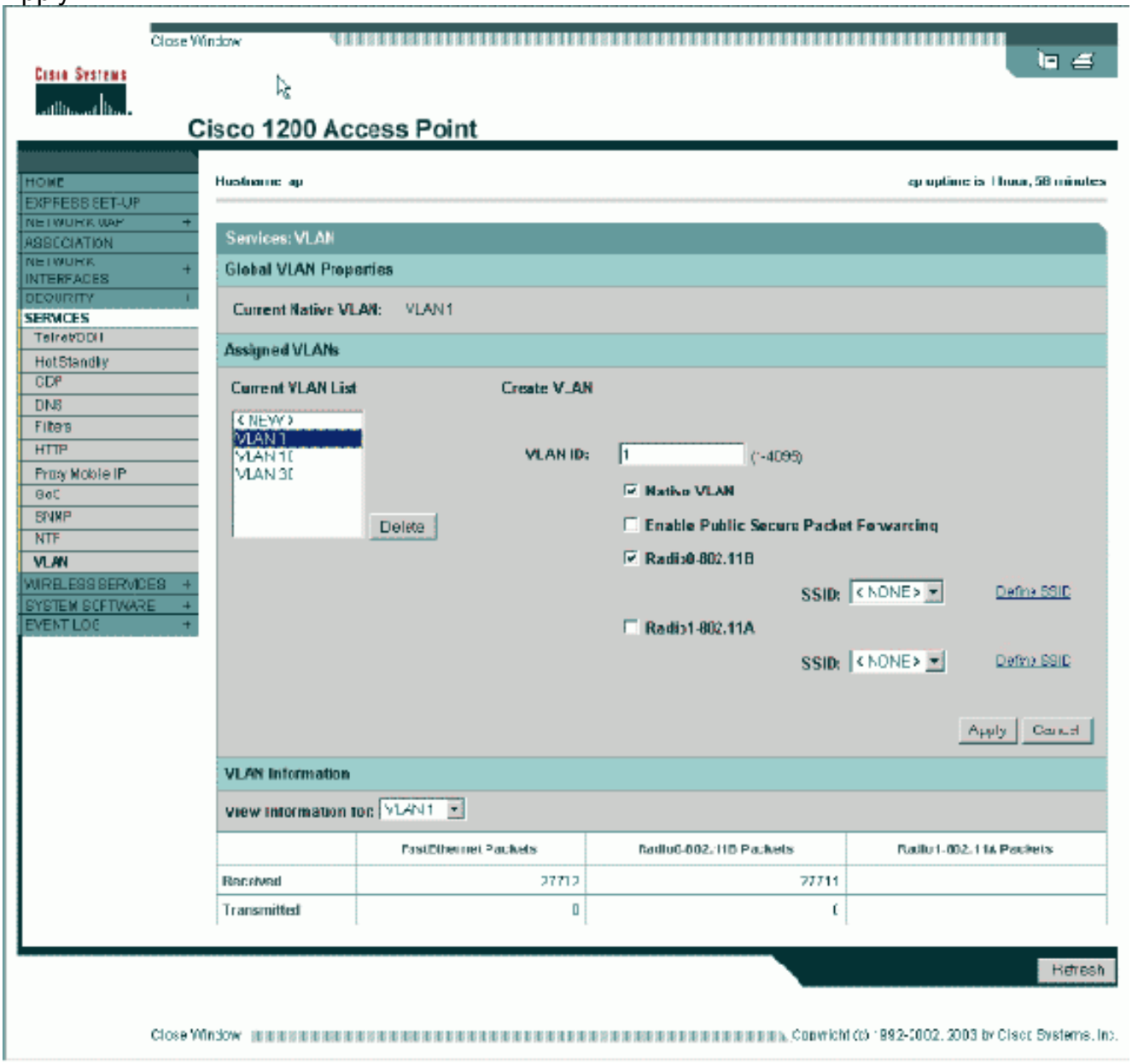
Para criptografar os dados que passam pelo link de rádio, aplique a criptografia somente ao SSID

da VLAN nativa. Essa criptografia se aplica a todas as outras VLANs. Quando você faz a ponte, não há necessidade de associar um SSID separado a cada VLAN. As configurações de VLAN são as mesmas nas bridges raiz e não raiz.

Configuração da Bridge

Para configurar a bridge para VLANs, como o diagrama de rede de exemplo, faça o seguinte:

1. Na GUI do AP, clique em **Services > VLAN** para navegar até **Services:** Página **VLAN**.A primeira etapa é configurar a VLAN nativa. Para fazer isso, escolha **<New>** na Current VLAN List.Digite o número da VLAN nativa na caixa VLAN ID. Isso deve corresponder à VLAN nativa configurada no switch.Como a interface BVI 1 está associada à subinterface da VLAN Nativa, o endereço IP atribuído à interface BVI 1 deve estar na **mesma sub-rede IP** que outros dispositivos de infraestrutura na rede (ou seja, a interface SC0 em um switch Catalyst que executa CatOS).Marque a caixa de seleção da VLAN nativa.Clique em Apply.

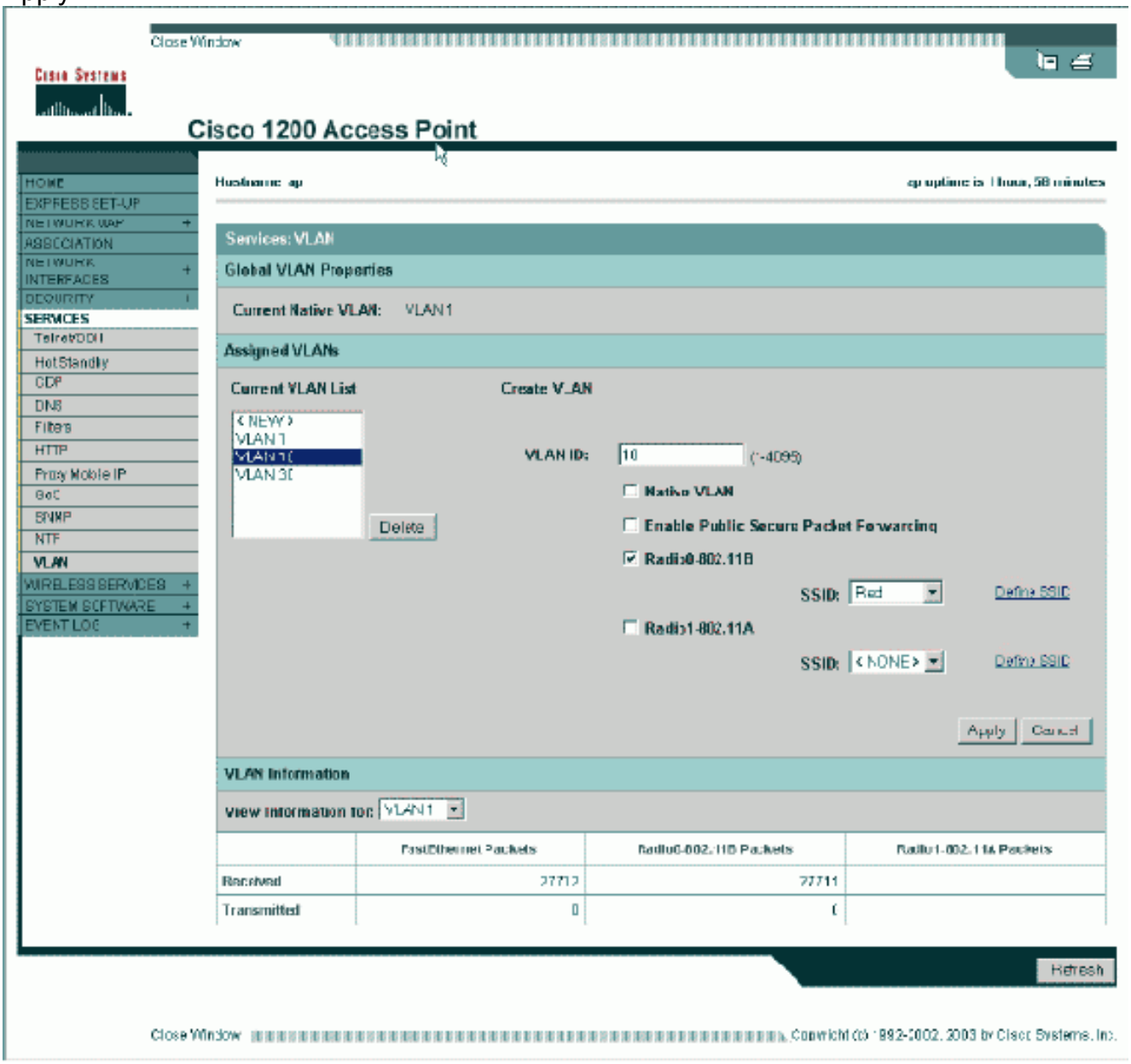


Ou, a partir do CLI, emita estes comandos:

```
bridge# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
bridge(config)# interface Dot11Radio0.1
```

```
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 outras VLANs, siga estas etapas:Na Lista de VLANs atuais, selecione **Novo**.Insira o número do VLAN desejado na caixa ID do VLAN. O número da VLAN deve corresponder a uma VLAN configurada no switch.Clique em Apply.



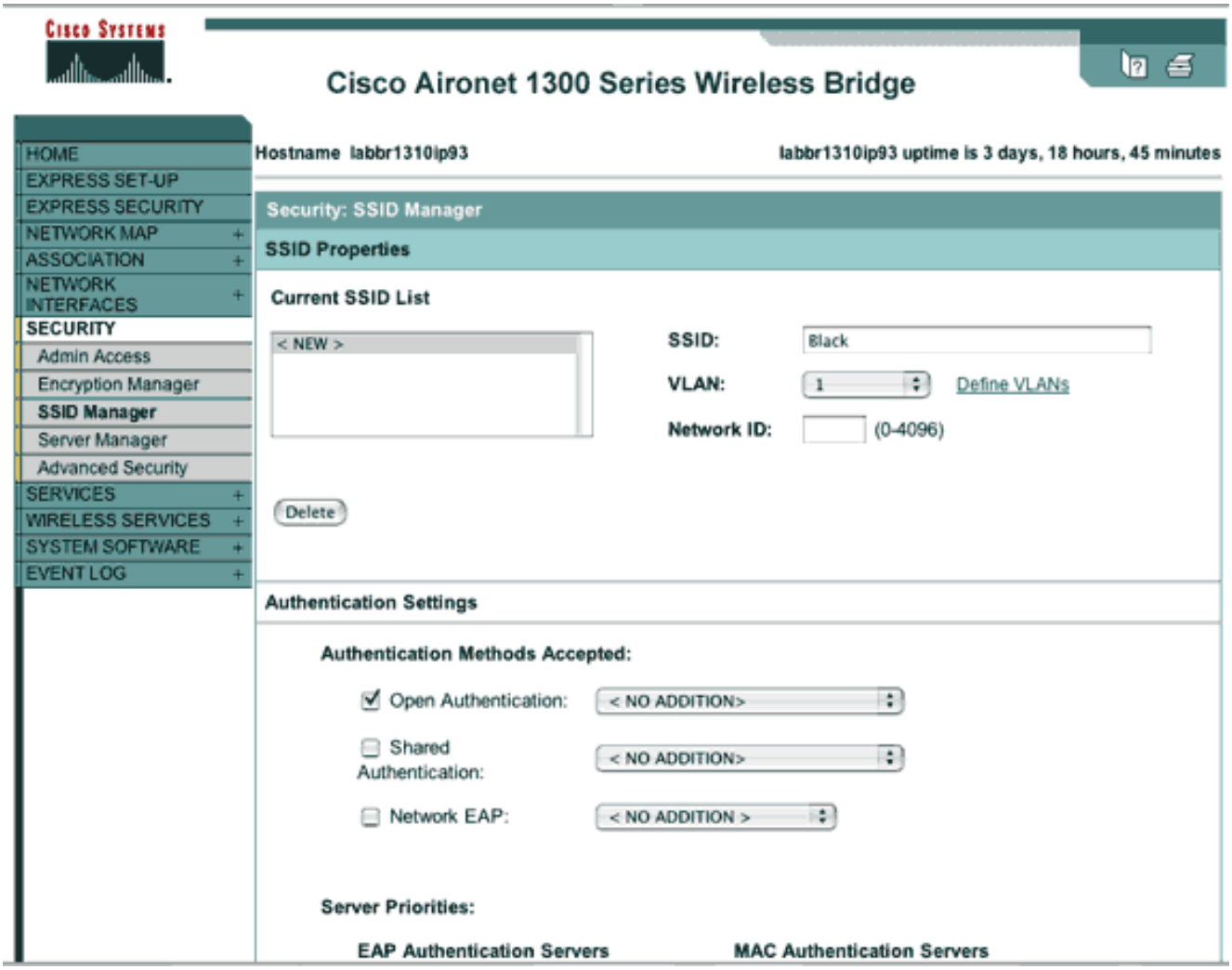
Ou, a partir do CLI, emita estes comandos:

```
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
```

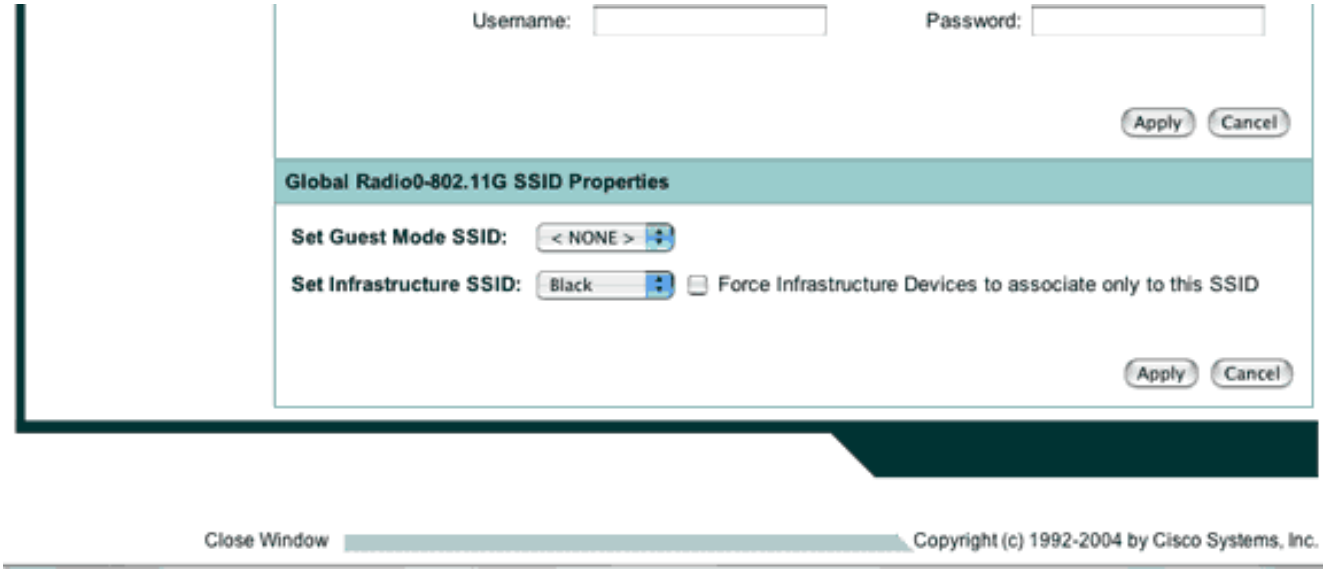
Repita as etapas de 2a a 2c para cada VLAN desejada ou insira os comandos da CLI com as alterações apropriadas na subinterface e nos números de VLAN.

```
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. No Gerenciador de SSID (no item de menu **Segurança > Gerenciador de SSID**), associe a VLAN nativa a um SSID.**Observação:** quando você faz a ponte, o único SSID que você deve associar a uma VLAN é aquele que se correlaciona à VLAN Nativa. Você deve designar esse SSID como o SSID da infraestrutura.Na Lista de SSID atual, selecione **Novo**.Digite o SSID desejado (diferencia maiúsculas de minúsculas) na caixa SSID.Selecione o número da VLAN que corresponde à VLAN nativa na lista suspensa.**Observação:** para manter este documento dentro do escopo pretendido, a segurança de um SSID não é endereçada.Clique em **Apply** para criar o SSID no rádio e associá-lo à VLAN nativa.



Role de volta para a parte inferior da página e, em **Propriedades do SSID Global Radio0-802.11G,** selecione o **SSID** na lista suspensa **Definir SSID da infraestrutura**. Clique em Apply.



Ou na 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
```

Observação: quando as VLANs estão em uso, os SSIDs são configurados na interface de rádio Dot11física, e não em qualquer subinterface lógica.**Observação:** este exemplo não inclui autenticação. As bridges raiz e não raiz exigem alguma forma de autenticação (Aberta, EAP de rede, etc.) para se associar.

Usar um servidor RADIUS para atribuir usuários a VLANs

Você pode configurar seu servidor de autenticação RADIUS para atribuir usuários ou grupos de usuários a uma VLAN específica quando eles se autenticarem na rede. Para obter informações sobre esse recurso, consulte a seção Using a RADIUS Server to Assign Users to VLANs do documento *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*.

Usar um servidor RADIUS para atribuição de grupo de mobilidade dinâmica

Você também pode configurar um servidor RADIUS para atribuir dinamicamente grupos de mobilidade a usuários ou grupos de usuários. Isso elimina a necessidade de configurar vários SSIDs no ponto de acesso. Em vez disso, você precisa configurar apenas um SSID por ponto de acesso. Para obter informações sobre esse recurso, consulte a seção Using a RADIUS Server for Dynamic Mobility Group Assignment do documento *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.4(3g)JA & 12.3(8)JEB*.

Configuração de grupo de bridge em access points e bridges

Em geral, os grupos de bridge criam domínios de switching segmentados. O tráfego é confinado aos hosts em cada grupo de bridge, mas não entre os grupos de bridge. O switch encaminha o tráfego apenas entre os hosts que formam o grupo de bridge, o que restringe o tráfego de

broadcast e multicast (inundação) apenas a esses hosts. Os grupos de pontes aliviam o congestionamento da rede e fornecem segurança de rede adicional quando segmentam o tráfego para certas áreas da rede.

Consulte a Visão geral do Bridging para obter informações detalhadas.

Em uma rede sem fio, os grupos de pontes são configurados nos pontos de acesso sem fio e nas bridges para que o tráfego de dados de uma VLAN seja transmitido da mídia sem fio para o lado com fio e vice-versa.

Execute esta etapa da CLI do AP para habilitar os grupos de bridge globalmente no ponto de acesso/ponte.

Este exemplo usa o bridge-group number 1.

Ap(configure)#**bridge** ***1***

Observação: você pode numerar seus grupos de bridge de 1 a 255.

Configure a interface de rádio e a interface Fast Ethernet do dispositivo sem fio para estar no mesmo grupo de bridge. Isso cria um caminho entre essas duas interfaces diferentes e elas estão na mesma VLAN para fins de marcação. Como resultado, os dados transmitidos do lado sem fio através da interface de rádio são transmitidos para a interface Ethernet à qual a rede com fio está conectada e vice-versa. Em outras palavras, as interfaces de rádio e Ethernet que pertencem ao mesmo grupo de bridge na verdade fazem a ponte dos dados entre elas.

Em um ponto de acesso/ponte, você precisa ter um grupo de bridge por VLAN para que o tráfego possa passar do fio para a rede sem fio e vice-versa. Quanto mais VLAN você tiver que passar tráfego pela rede sem fio, mais grupos de bridge serão necessários.

Por exemplo, se você tiver apenas uma VLAN para passar o tráfego pelo lado sem fio para o lado com fio da sua rede, configure apenas um grupo de bridge do CLI do AP/bridge. Se você tiver várias VLANs para passar o tráfego do lado sem fio para o lado com fio e vice-versa, configure grupos de bridge para cada VLAN na sub-interface de rádio, bem como a sub-interface Fast Ethernet.

1. Configure o grupo de bridge na interface sem fio com o comando de interface de rádio **bridge group 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. Configure o grupo de bridge com o mesmo número de grupo de bridge ("1" neste exemplo) na interface Fast Ethernet para que o tráfego da VLAN 1 seja passado através da interface sem fio para esse lado com fio 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
```

   Observação: quando você configura um grupo de bridge na interface de rádio, esses

comandos são definidos automaticamente.**bridge-group *1* subscriber-loop-controlbridge-group *1* block-unknown-sourceno bridge-group *1* source-learningno bridge-group *1* unicast-floodingbridge-group *1* spanning-disabledObservação:** quando você configura um grupo de bridge na interface Fast Ethernet, esses comandos são definidos automaticamente.**no bridge-group *1* source-learningbridge-group *1* spanning-disabled**

Integrated Routing and Bridging (IRB)

O roteamento e o bridging integrados permitem rotear um protocolo específico entre interfaces roteadas e grupos de bridge ou rotear um protocolo específico entre grupos de bridge. O tráfego local ou não roteável pode ser interligado entre as interfaces com bridge no mesmo grupo de bridge, enquanto o tráfego roteável pode ser roteado para outras interfaces roteadas ou grupos de bridge

Com roteamento e bridging integrados, você pode fazer o seguinte:

- Trocar pacotes de uma interface com bridge para uma interface roteada
- Trocar pacotes de uma interface roteada para uma interface interligada
- Comutar pacotes dentro do mesmo grupo de bridge

Ative o IRB nos pontos de acesso e nas bridges sem fio para rotear o tráfego entre grupos de pontes ou entre interfaces roteadas e grupos de pontes. Você precisa de um roteador externo ou um switch de Camada 3 para rotear entre grupos de bridge ou entre grupos de bridge e interfaces roteadas.

Emita este comando para ativar o IRB no AP/bridge.

AP**(configure)#bridge irb**

O roteamento e o bridging integrados usam o conceito de uma BVI (Bridge-Group Virtual Interface, interface virtual do grupo de bridge) para rotear o tráfego entre interfaces roteadas 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 suporta bridging, mas representa na verdade o grupo de bridge correspondente para interfaces roteadas dentro do roteador de switch de Camada 3. Ele tem todos os atributos da camada de rede (como um endereço da 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 essa interface virtual representa. Esse número é o link entre a interface virtual e o grupo de bridge.

Execute estas etapas para configurar o BVI em pontos de acesso e bridges.

1. Configure 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. Habilite um BVI para aceitar e rotear pacotes roteáveis 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.
```

Éimportante entender que você só precisa de um BVI para a VLAN de gerenciamento/nativa na qual o AP está localizado (neste exemplo, VLAN 1). Você não precisa de um BVI para nenhuma outra subinterface, independentemente de quantas VLANs e grupos de bridge você configura em seu AP/bridge. Isso ocorre porque você marca o tráfego em todas as outras VLANs (exceto a VLAN nativa) e o envia para o switch através de uma interface de tronco dot1q no lado com fio. Por exemplo, se você tiver 2 VLANs em sua rede, precisará de dois grupos de bridge, mas apenas um correspondente de BVI para a VLAN de gerenciamento será suficiente em sua rede sem fio.Quando você habilita o roteamento para um determinado protocolo na interface virtual do grupo de pontes, os pacotes que vêm de uma interface roteada, mas que são destinados a um host em um domínio interligado, são roteados para a interface virtual do grupo de pontes e encaminhados para a interface interligada correspondente.Todo o tráfego roteado para a interface virtual do grupo de bridge é encaminhado para o grupo de bridge correspondente como tráfego de bridge. Todo o tráfego roteável recebido em uma interface com bridge é roteado para outras interfaces roteadas como se ele fosse diretamente da interface virtual do grupo de bridge.Consulte Configurar Bridging para obter informações mais detalhadas sobre Bridging e IRB.

Interação com switches relacionados

Nesta seção, você recebe as informações para configurar ou verificar a configuração dos switches Cisco que se conectam ao equipamento sem fio Cisco Aironet.

Observação: para encontrar informações adicionais sobre os comandos usados neste documento, use a Command Lookup Tool (somente clientes registrados) .

Configuração do Switch — Catalyst OS

Para configurar um switch que executa o Catalyst OS para tronco VLANs em um ponto de acesso, a sintaxe do comando é definida como trunk <*module #/port #*> ***em dot1q*** e **set trunk <*module #/port #*> <*vlan list*>**.

Um exemplo do diagrama de rede para o exemplo é:

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

Configuração do switch—Switches Catalyst baseados em IOS

No modo de configuração de interface, insira estes comandos, se desejar:

- Configurar a porta do switch para tronco de VLANs em um ponto de acesso
- Em um switch Catalyst que executa o IOS
- O CatIOS inclui, mas não se limita a:6x004x0035x0295 x

```
switchport mode trunk
switchport trunk encapsulation dot1q
```

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

Observação: o equipamento sem fio Cisco Aironet baseado em IOS não suporta Dynamic Trunking Protocol (DTP), portanto, o switch não deve tentar negociá-lo.

Configuração do Switch — Catalyst 2900XL/3500XL

No modo de configuração de interface, insira estes comandos, se desejar configurar a porta do switch para tronco de VLANs para um ponto de acesso em um switch Catalyst 2900XL ou 3500XL que executa o IOS:

```
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

- **show vlan** — exibe todas as VLANs configuradas atualmente no ponto de acesso e seu status

```
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** —exibe informações sobre clientes associados, por SSID/VLAN

```
ap#show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [Green] :

SSID [Red] :

Others:  (not related to any ssid)

ap#
```

Verificar o Switch

- Em um switch baseado em Catalyst OS, **show trunk <*module #/port #*>**—exibe o status de um tronco em uma determinada porta

```
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)
```

- Em um switch baseado em IOS, **show interface fastethernet <*module #/port #*> trunk** —exibe o status de um tronco em uma determinada 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 switch Catalyst 2900XL/3500XL, **show interface fastethernet <*module #/port #*> switchport** —exibe o status de um tronco em uma determinada 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#
```

Troubleshoot

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

Informações Relacionadas

- Configuring VLANs (Access Point Configuration Guide)
- Configuração de VLANs (Guia de Configuração de Bridge)
- Suporte técnico de entroncamento
- Interação com switches relacionados
- Requisitos de sistema para implementar o entroncamento
- Visão geral do Bridging
- Exemplo de Tipos de Autenticação Wireless em uma Configuração de ISR Fixo
- Exemplo de configuração de tipos de autenticação sem fio em ISR fixo por meio de SDM
- Conectividade LAN sem fio usando um ISR com criptografia WEP e exemplo de configuração de autenticação LEAP
- Exemplo de Configuração de Conexão de LAN Wireless Básica
- Suporte Técnico e Documentação - Cisco Systems