

Como criar uma rede de voz básica usando Raspberry Pi

Objetivo

Este documento fornece instruções sobre como configurar uma rede de voz básica com Raspberry Pi como o servidor de comunicação usando Asterisks. A rede local virtual (VLAN) e a qualidade de serviço (QoS) serão usadas para ajudar a priorizar o tráfego separando o tráfego de voz e de dados. O objetivo dessa rede é configurar testes internos. Esses testes o ajudarão a dimensionar sua rede adequadamente, verificar se você tem largura de banda suficiente para o volume de voz esperado e encontrar qualquer outra contenção possível entre os equipamentos. Ele também pode ajudar a determinar se você deseja hospedá-lo localmente ou na nuvem. Quando uma empresa tiver atingido um determinado tamanho, ela poderá preferir ter seu próprio controlador de chamadas local, como PBX ou PBX IP. Isso tornaria as chamadas internas mais eficientes, já que as chamadas entre os telefones dentro da empresa não precisariam ser roteadas para fora do prédio e depois de volta para dentro.

Observação importante: o Raspberry Pi não é um produto suportado pela Cisco, este documento é apenas para fins de suporte e não é um documento de solução.

Introdução

Para que uma empresa realize negócios eficazes, os funcionários precisam ter acesso a uma rede de voz. Isso facilita a comunicação entre funcionários e seus clientes, além de permitir que os funcionários se comuniquem internamente. Cada funcionário pode receber um telefone fixo e/ou celular, mas isso pode ficar bem caro. Em vez disso, as empresas costumam optar por configurar uma rede de voz que utilize o Voice over Internet Protocol (VoIP).

A tecnologia VoIP permite que você use a Internet para fazer e receber chamadas telefônicas de qualquer local, para qualquer local do mundo com tarifas de longa distância mínimas, se houver. Isso pode ser utilizado em qualquer dispositivo que use a Internet.

O VoIP pode economizar o dinheiro de uma empresa e, ao mesmo tempo, aumentar a produtividade, a comunicação e a satisfação do cliente. Os funcionários podem utilizar diferentes recursos, como roteamento de chamadas, música em espera e correio de voz integrado.

Um recurso comum de VoIP que muitas empresas usam é o roteamento de chamadas, também conhecido como distribuidor automático de chamadas. O roteamento de chamadas distribui as chamadas recebidas para o próximo agente disponível em vez de enviá-las para o correio de voz. Isso garante que as chamadas dos clientes sejam atendidas da forma mais eficiente possível. Após o horário comercial, as chamadas podem ser enviadas diretamente para o correio de voz.

Adicionar usuários e atualizar recursos é um processo simples, que é útil quando sua empresa está se expandindo ou suas necessidades mudam. Diferentemente de um sistema telefônico tradicional, não é necessário fazer cabeamento caro.

Para configurar uma rede VoIP, você tem opções a considerar. Você pode hospedar um serviço de VoIP para seu próprio sistema telefônico usando KSU, PBX (Private Branch Exchange) sem KSU ou outro sistema de VoIP.

Seu orçamento, número de funcionários e locais, serviços disponíveis na sua área e o crescimento da

empresa devem ser considerados. Talvez seja necessário disponibilizar treinamento e equipamentos adicionais, como fones de ouvido. O VoIP pode aumentar o uso de dados e talvez seja necessário aumentar a largura de banda para considerar o tráfego da rede de voz.

Você também deve planejar um backup, "Plano B", caso sua rede fique inativa. Se você perder energia, o sistema VoIP não será conectado. Essa redundância deve ser implementada para restaurar imediatamente os serviços telefônicos e evitar a interrupção da produtividade da empresa.

Neste artigo, implantaremos nosso próprio sistema de telefonia usando o Asterisk, um PBX em um Raspberry Pi.

Observação: depois de concluir essas etapas e se quiser ter a capacidade de chamar sua rede interna, você precisará escolher um ISP (Provedor de serviços de telefonia via Internet).

Definições

Uma rede local virtual (VLAN) permite segmentar logicamente uma rede de área local (LAN) em diferentes domínios de transmissão. Nos cenários em que dados confidenciais podem ser transmitidos em uma rede, as VLANs podem ser criadas para aumentar a segurança, designando uma transmissão para uma VLAN específica. Os usuários em uma VLAN específica são os únicos que podem acessar e manipular dados nessa VLAN. As VLANs também podem ser usadas para melhorar o desempenho, reduzindo a necessidade de enviar broadcasts e multicasts para destinos desnecessários.

Todas as portas, por padrão, são atribuídas à VLAN 1, portanto, depois de configurar VLANs diferentes, você precisa atribuir manualmente cada porta à VLAN apropriada.

Cada VLAN deve ser configurada com um ID de VLAN (VID) exclusivo com um valor de 1 a 4094. O dispositivo reserva o VID 4095 como a VLAN de descarte. Todos os pacotes classificados para a VLAN de descarte são descartados no ingresso e não são encaminhados para uma porta.

A qualidade de serviço (QoS) permite priorizar o tráfego para diferentes aplicativos, usuários ou fluxos de dados. Ele também pode ser usado para garantir o desempenho em um nível especificado, afetando assim a QoS do cliente. A QoS é geralmente afetada pelos seguintes fatores: instabilidade, latência e perda de pacotes. Na maioria das vezes, o vídeo ou VoIP recebe prioridade, pois são mais afetados pela QoS.

O PBX (Private Branch Exchange) é um sistema de comutação telefônica que gerencia chamadas de entrada e saída para usuários internos em uma empresa. Um PBX é conectado ao sistema telefônico público e roteia automaticamente as chamadas recebidas para ramais específicos. Ele também compartilha e gerencia várias linhas. Um sistema de PABX típico para pequenas empresas inclui linhas telefônicas internas e externas, um servidor de computador que gerencia comutação e roteamento de chamadas e um console para controle manual.

Um **PBX IP** pode fazer tudo o que um PBX tradicional de pequena empresa pode fazer e muito mais. Ele executa a comutação e a conexão de VoIP, bem como chamadas de linha fixa. Um sistema de PABX IP é executado em uma rede de dados IP, o que economiza custos e minimiza o gerenciamento da rede. Você pode usar telefones IP, softphones (que não exigem nenhum hardware de telefone além de um fone de ouvido de computador e microfone) e telefones fixos em um sistema telefônico PBX IP.

O Raspberry Pi é um computador pequeno, barato e portátil que funciona como um computador de mesa.

Asterisk é uma estrutura de código aberto que pode fazer um computador, como um Raspberry Pi, em

um servidor de comunicação. Isso permite que você crie seu próprio sistema telefônico PBX comercial. Neste artigo, o Asterisk usa o FreePBX como uma interface gráfica de usuário (GUI) que controla e gerencia o Asterisk, onde você pode configurar extensões, usuários, etc.

Dispositivos aplicáveis

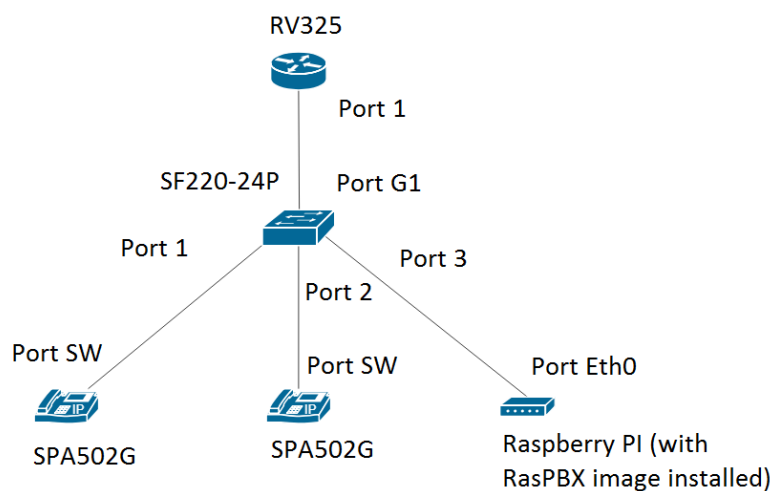
- Router
- Switch Power over Ethernet (PoE)
- Raspberry Pi (modelos Pi 3 B+, Pi 3, Pi 3, B+, B e A)
- 2 ou mais telefones IP Cisco SPA/MPP

Versão de software

- 14.0.1.20 (PBX livre)
- 13.20.0 (Asterisco)
- 1.1.1.06 (Roteador RV325)
- 1.1.4.1 (SF220-24P)
- 7.1.3 (SPA502G)

Para configurar a rede de voz básica com Raspberry Pi, siga as diretrizes abaixo:

Topologia:



A imagem do RasPBX pode ser encontrada [aqui](#). Esta imagem precisa ser instalada no Raspberry Pi.

Nota: Neste documento, o Raspberry Pi com a imagem RasPBX já está configurado. Para acessar a GUI do Raspberry Pi, digite <http://raspbx.local> ou o endereço IP do Raspberry Pi em seu navegador para configurar o PBX. O login padrão do FreePBX é usuário: **admin** senha: **admin**. Além disso, o Raspberry Pi foi pré-configurado para ter um endereço IP estático.

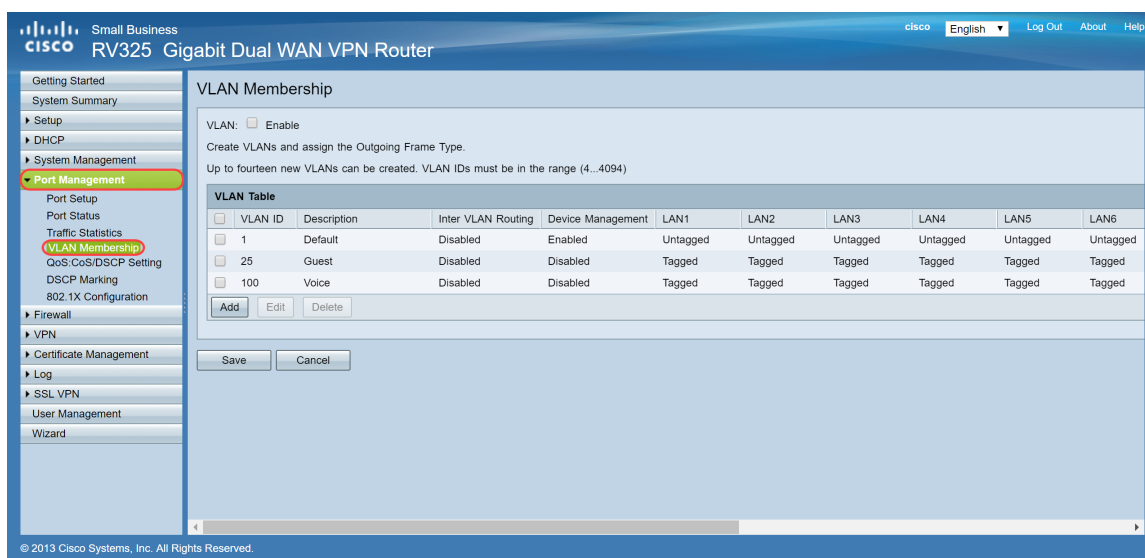
Table Of Contents

1. [Configurando VLANs no roteador](#)
2. [Configurando telefones SPA/MPP](#)
3. [Configurando VLANs em um Switch](#)
4. [Configurando VLANs de voz em um switch](#)
5. [Definindo as configurações de interface em um switch](#)
6. [Configurando a participação de VLAN de porta em um switch](#)
7. [Como alterar o endereço IP do Raspberry Pi para uma sub-rede diferente](#)
8. [Conclusão](#)

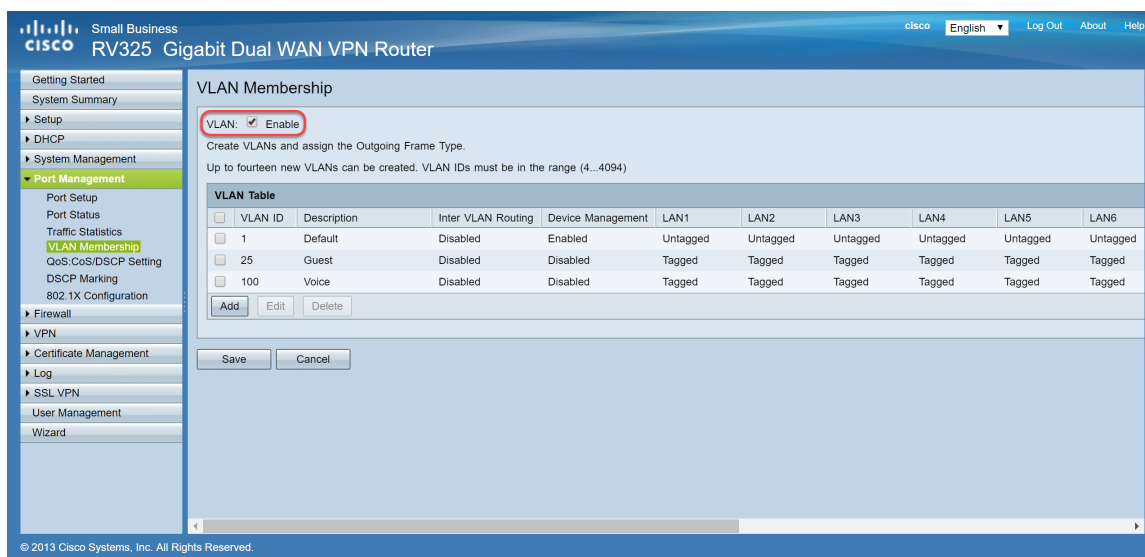
Configurando VLANs no roteador

Etapa 1. Faça login no utilitário baseado na Web e navegue até **Port Management > VLAN Membership**.

Nota: Isso pode variar dependendo do modelo. Neste exemplo, RV325 é usado. Para obter mais informações sobre como acessar a página de configuração baseada na Web, clique [aqui](#).



Etapa 2. Marque a caixa de seleção **Enable** para ativar a VLAN no roteador.

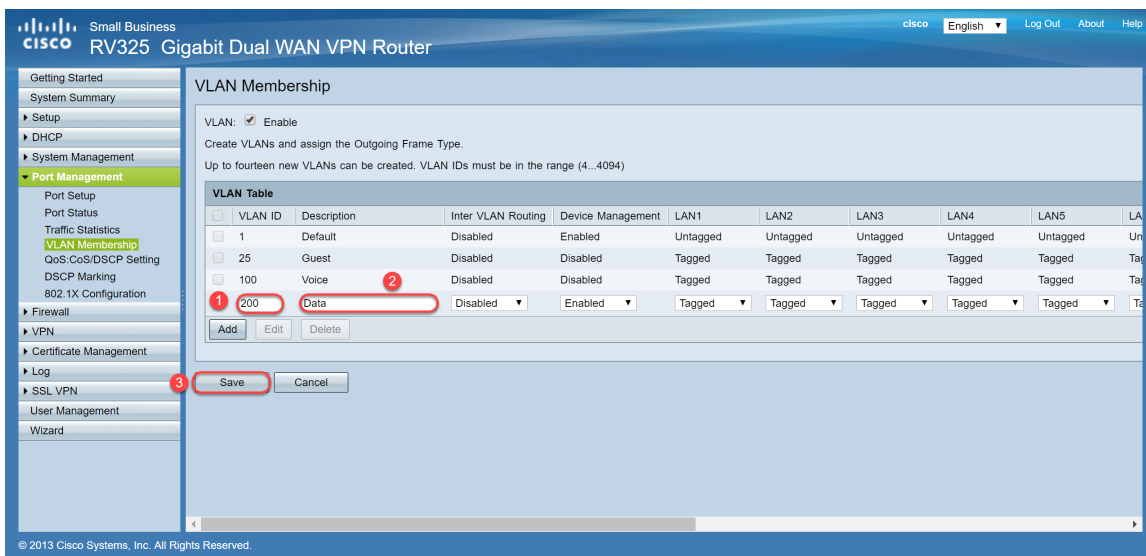


Etapa 3. Na seção *Tabela de VLAN*, clique em **Adicionar** para criar um novo ID de VLAN.

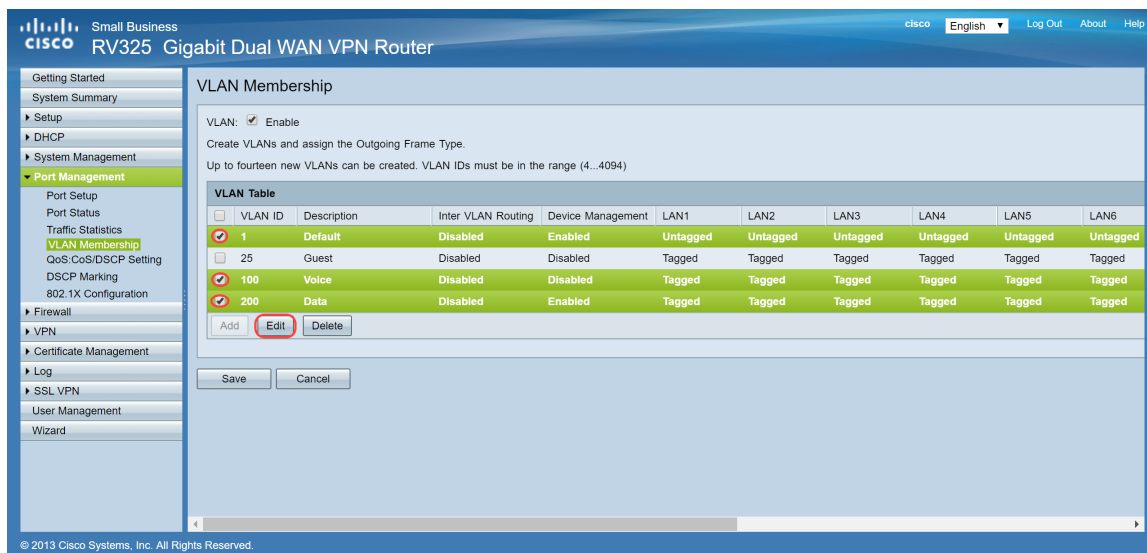


Etapa 4. Insira um número de VLAN no campo *VLAN ID*. As IDs de VLAN devem estar no intervalo de 4 a 4094. Neste exemplo, 200 é usado para dados como VLAN ID. Em seguida, insira uma descrição para a VLAN no campo *Description*. Os dados são inseridos como exemplo de descrição. Em seguida, clique em **Salvar**.

Observação: a VLAN 100 para voz foi criada por padrão neste roteador. Até quatorze novas VLANs podem ser criadas.



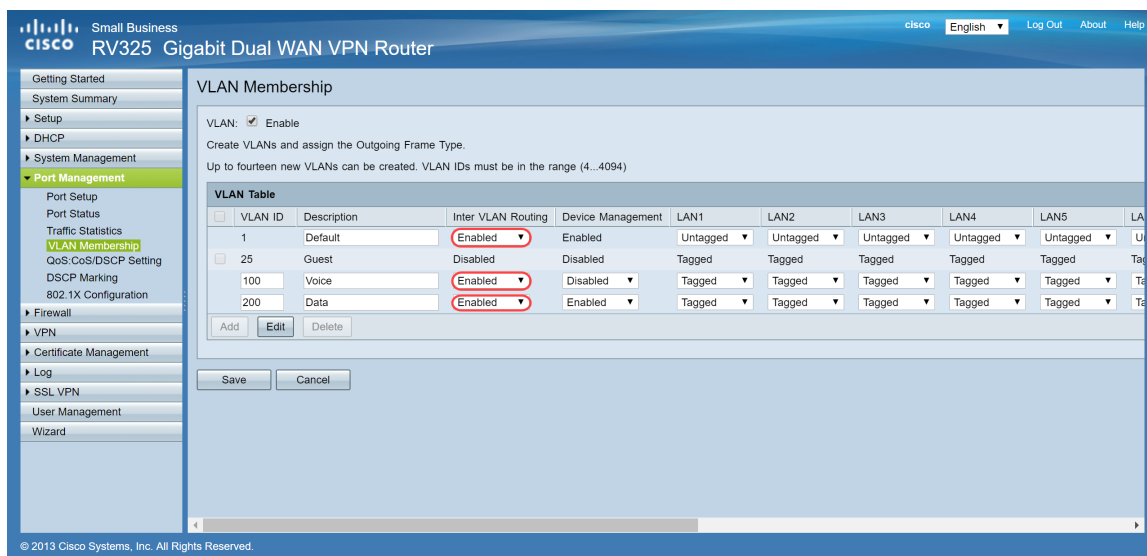
Etapa 5. Para editar uma VLAN, marque a caixa de seleção da VLAN apropriada. Neste exemplo, as VLANs 1, 100 e 200 serão editadas. Em seguida, clique em **Edit** para editar as VLANs.



Etapa 6. (Opcional) Na lista suspensa *Inter VLAN Routing*, escolha **Enabled** ou **Disabled** para rotear pacotes de uma VLAN para outra VLAN. Essa habilitação é útil porque os administradores de rede internos poderão acessar remotamente seus dispositivos para ajudar a solucionar seus problemas. Isso reduzirá o tempo de ter que comutar constantemente VLANs para acessar os dispositivos.

- Desativado - Representa que o Inter VLAN Routing está inativo
- Enabled - Representa que o Inter VLAN Routing está ativo nessa VLAN. O roteamento entre VLANs roteia os pacotes somente entre as VLANs que o têm ativado.

Observação: neste exemplo, habilitaremos o Roteamento entre VLANs para VLAN ID 1, 100 e 200.



Passo 7. Escolha a opção desejada na lista suspensa para a porta LAN à qual você está conectado e a configuração deve corresponder à porta conectada. Se você estiver conectado com mais de uma porta, será necessário escolher as mesmas configurações para cada porta conectada. O padrão está marcado, mas para VLAN 1 não está.

Observação: se você ativar o roteamento entre VLANs na Etapa 6, terá que marcar a VLAN para distinguir o tráfego.

Marcado

- Representa a associação entre a porta e a VLAN como marcada.
- Marcado é usado para determinar a VLAN à qual o tráfego pertence através do ID de VLAN

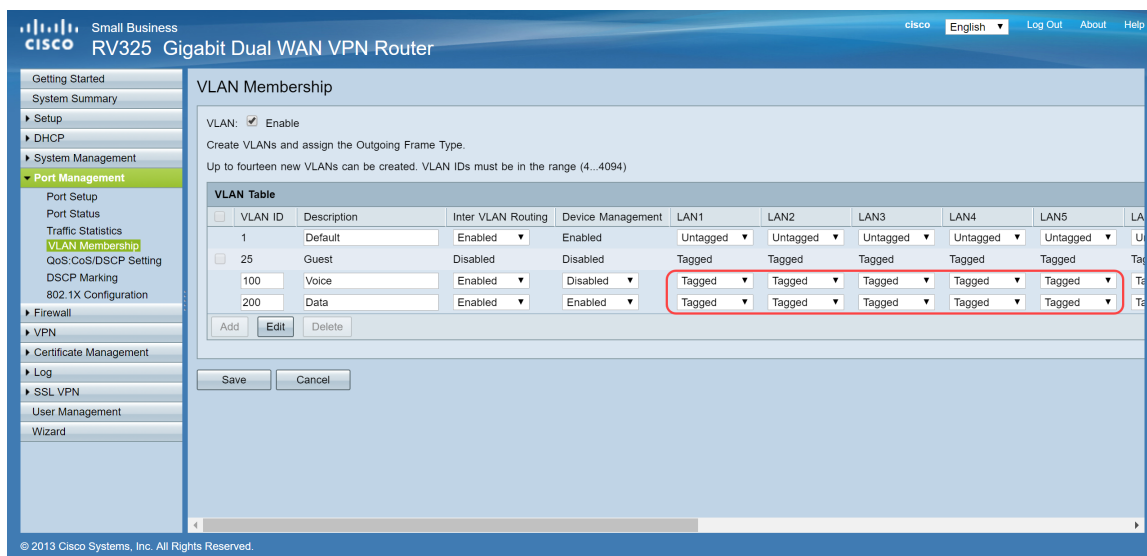
exclusivo quando várias VLANs são criadas para a mesma porta.

Sem rótulo

- Representa que a associação entre a porta e a VLAN não está marcada.
- É usado quando apenas uma VLAN é criada e o tráfego reconhece a VLAN. Somente uma VLAN pode ser marcada como não marcada para cada porta LAN.
- Se a VLAN padrão estiver na porta, ela deve sempre estar sem rótulo, mesmo que a porta tenha várias VLANs.

Excluído

- Representa que a interface não é um membro da VLAN.
- Se você escolher essa opção, o tráfego será desativado entre a VLAN e a porta.



Etapa 8. Clique em **Save (Salvar)** para salvar as configurações.

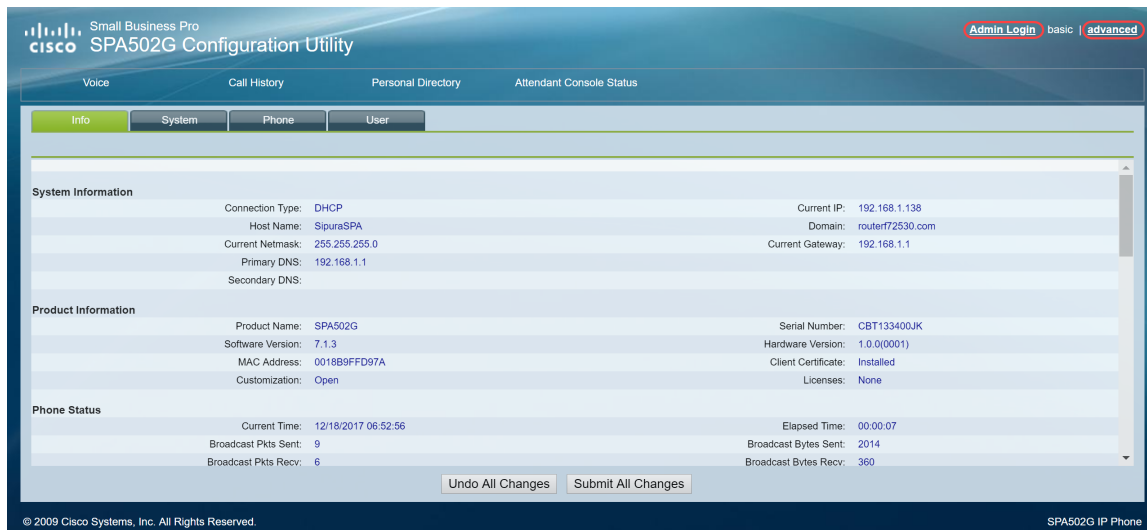
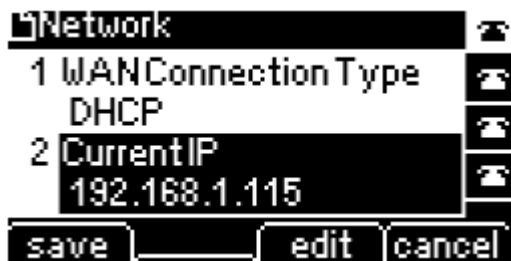
Nota: No roteador, você pode fazer login no utilitário baseado na Web e navegar até **DHCP > DHCP Setup** para configurar as VLANs para uma sub-rede específica desejada. Por padrão, as VLANs são configuradas para estar em uma sub-rede diferente.

Configurando telefones SPA/MPP

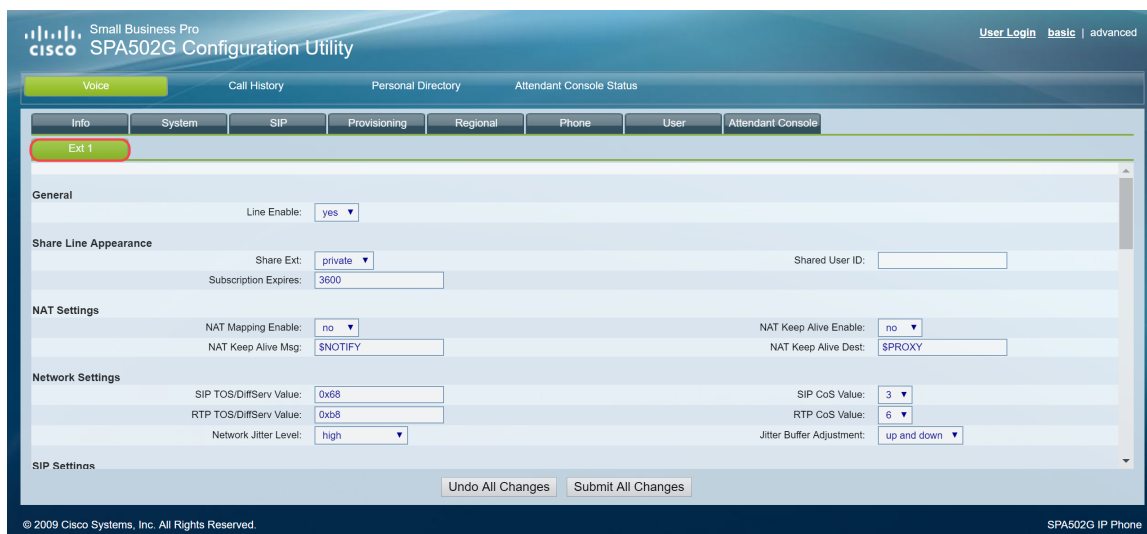
Os usuários também podem configurar os telefones para obter um perfil de um local de perfil configurado manualmente, um local encontrado através da opção de DHCP 150 ou de um servidor Cisco EDOS. Veja a seguir um exemplo de configuração manual.

Etapa 1. Insira o endereço IP do SPA/MPP em seu navegador, navegue até **Admin Login** e depois **advanced**.

Nota: A configuração do telefone SPA/MPP pode variar dependendo do modelo. Neste exemplo, estamos usando o SPA502G. Para encontrar o endereço IP do telefone IP, navegue para **DHCP > DHCP Status** no roteador (pode variar dependendo do modelo). Outra maneira é pressionar o botão **Setup** e navegar para **Network** no telefone Cisco (os menus e as opções podem variar dependendo do modelo do telefone).



Etapa 2. Navegue até **Voice > Ext 1**, a página do ramal será aberta.



Etapa 3. Na seção *Proxy and Registration*, digite o servidor proxy no campo *Proxy*. Neste exemplo, o endereço do Raspberry Pi (192.168.3.10) será usado como o servidor proxy. A VLAN 100 está na sub-rede com 192.168.3.x.

Nota: Você estará configurando o endereço IP do Raspberry Pi mais adiante neste artigo, se você quiser saber mais, clique no link a ser redirecionado para essa seção: [Alterando o endereço do Raspberry Pi para estar em uma sub-rede diferente](#).

Small Business Pro
cisco SPA502G Configuration Utility

User Login basic advanced

Voice Call History Personal Directory Attendant Console Status

Info System SIP Provisioning Regional Phone User Attendant Console

Ext 1

CFWD Notifier:

Proxy and Registration

Proxy: Use Outbound Proxy:

Outbound Proxy: Use OB Proxy In Dialog:

Register: Make Call Without Reg:

Register Expires: Ans Call Without Reg:

Use DNS SRV: DNS SRV Auto Prefix:

Proxy Fallback Intvl: Proxy Redundancy Method:

Subscriber Information

Display Name: User ID:

Password: Use Auth ID:

Auth ID:

Mini Certificate:

SRTP Private Key:

Undo All Changes Submit All Changes

© 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone

Etapa 4. Em *Subscriber Information*, insira o nome de exibição e a ID de usuário (número do ramal) do ramal compartilhado. Neste exemplo, usaremos o ramal 1003.

Observação: o ramal 1003 já foi criado e configurado no Raspberry Pi.

Small Business Pro
cisco SPA502G Configuration Utility

User Login basic advanced

Voice Call History Personal Directory Attendant Console Status

Info System SIP Provisioning Regional Phone User Attendant Console

Ext 1

Register Expires: Ans Call Without Reg:

Use DNS SRV: DNS SRV Auto Prefix:

Proxy Fallback Intvl: Proxy Redundancy Method:

Subscriber Information

Display Name: User ID:

Password: Use Auth ID:

Auth ID:

Mini Certificate:

SRTP Private Key:

Audio Configuration

Preferred Codec: Use Pref Codec Only:

Second Preferred Codec: Third Preferred Codec:

G729a Enable: G722 Enable:

G726-16 Enable: G726-24 Enable:

G726-32 Enable: G726-40 Enable:

Undo All Changes Submit All Changes

© 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone

Etapa 5. Digite a senha do ramal que você configurou na seção do ramal Raspberry Pi. Isso também é conhecido como *Secret* na seção *Edit Extension* no Raspberry Pi. Neste exemplo, a senha **12345** foi usada.

Nota: A senha **12345** foi usada apenas como exemplo; uma senha mais complexa é recomendada.

Small Business Pro
cisco SPA502G Configuration Utility

User Login basic advanced

Voice Call History Personal Directory Attendant Console Status

Info System SIP Provisioning Regional Phone User Attendant Console

Ext 1

Register Expires: 3600
 Use DNS SRV: no
 Proxy Fallback Intvl: 3600

Ans Call Without Reg: no
 DNS SRV Auto Prefix: no
 Proxy Redundancy Method: Normal

Subscriber Information

Display Name: 1003
 Password: 12345
 Auth ID: **12345**
 Mini Certificate:
 SRTP Private Key:

User ID: 1003
 Use Auth ID: no

Audio Configuration

Preferred Codec: G711u
 Second Preferred Codec: Unspecified
 G729a Enable: yes
 G726-16 Enable: yes
 G726-32 Enable: yes

Use Pref Codec Only: no
 Third Preferred Codec: Unspecified
 G722 Enable: yes
 G726-24 Enable: yes
 G726-40 Enable: yes

Undo All Changes Submit All Changes

© 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone

Etapa 6. Escolha a opção desejada na lista suspensa *Usar ID de autenticação*. As opções são **Yes** e **No**. Para habilitar a autenticação do Session Initiation Protocol (SIP), na qual as mensagens SIP podem ser desafiadas a determinar se estão autorizadas antes de poderem transmitir, escolha **Yes** na lista suspensa **Auth ID**. Neste exemplo, escolhemos **Sim**.

Small Business Pro
cisco SPA502G Configuration Utility

User Login basic advanced

Voice Call History Personal Directory Attendant Console Status

Info System SIP Provisioning Regional Phone User Attendant Console

Ext 1

Register Expires: 3600
 Use DNS SRV: no
 Proxy Fallback Intvl: 3600

Ans Call Without Reg: no
 DNS SRV Auto Prefix: no
 Proxy Redundancy Method: Normal

Subscriber Information

Display Name: 1003
 Password: 12345
 Auth ID:
 Mini Certificate:
 SRTP Private Key:

User ID: 1003
 Use Auth ID: **yes**

Audio Configuration

Preferred Codec: G711u
 Second Preferred Codec: Unspecified
 G729a Enable: yes
 G726-16 Enable: yes
 G726-32 Enable: yes

Use Pref Codec Only: no
 Third Preferred Codec: Unspecified
 G722 Enable: yes
 G726-24 Enable: yes
 G726-40 Enable: yes

Undo All Changes Submit All Changes

© 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone

Passo 7. Digite o ramal que você está tentando configurar para este telefone no campo *ID de autenticação*. A ID de autenticação é para autenticação SIP.

Small Business Pro
cisco SPA502G Configuration Utility

User Login basic advanced

Voice Call History Personal Directory Attendant Console Status

Info System SIP Provisioning Regional Phone User Attendant Console

Ext 1

Register Expires: 3600
 Use DNS SRV: no
 Proxy Fallback Intvl: 3600

Ans Call Without Reg: no
 DNS SRV Auto Prefix: no
 Proxy Redundancy Method: Normal

Subscriber Information

Display Name: 1003
 Password: 12345
 Auth ID: **1003**
 Mini Certificate:
 SRTP Private Key:

User ID: 1003
 Use Auth ID: yes

Audio Configuration

Preferred Codec: G711u
 Second Preferred Codec: Unspecified
 G729a Enable: yes
 G726-16 Enable: yes

Use Pref Codec Only: no
 Third Preferred Codec: Unspecified
 G722 Enable: yes
 G726-24 Enable: yes

Undo All Changes Submit All Changes

© 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone

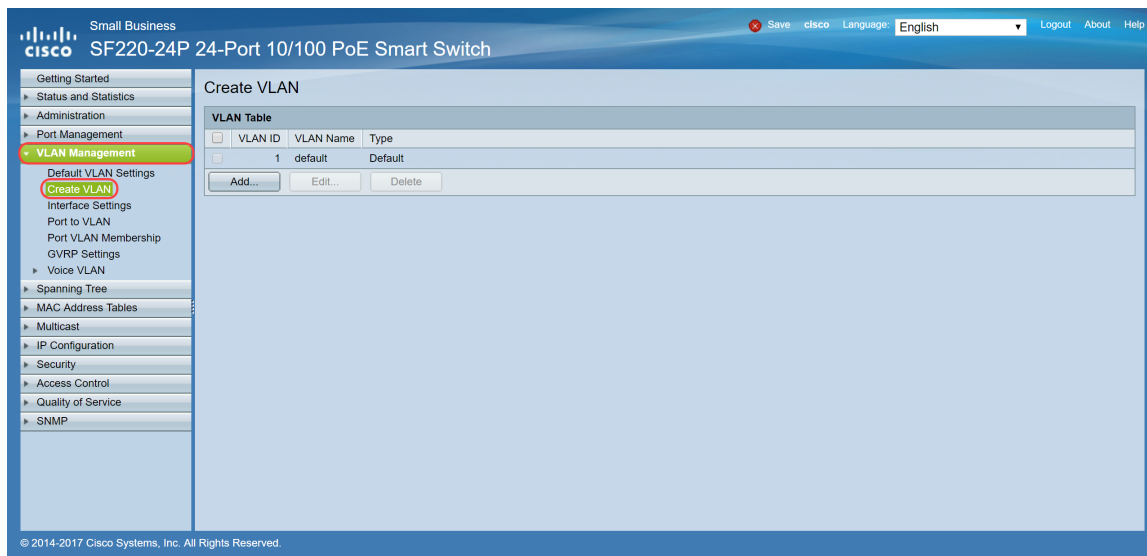
Etapa 8. Em seguida, clique em **Submit All Changes (Enviar todas as alterações)**.

Observação: Volte para a etapa 1 da seção Configuração de Telefones SPA/MPP se tiver mais telefones SPA/MPP para configurar.

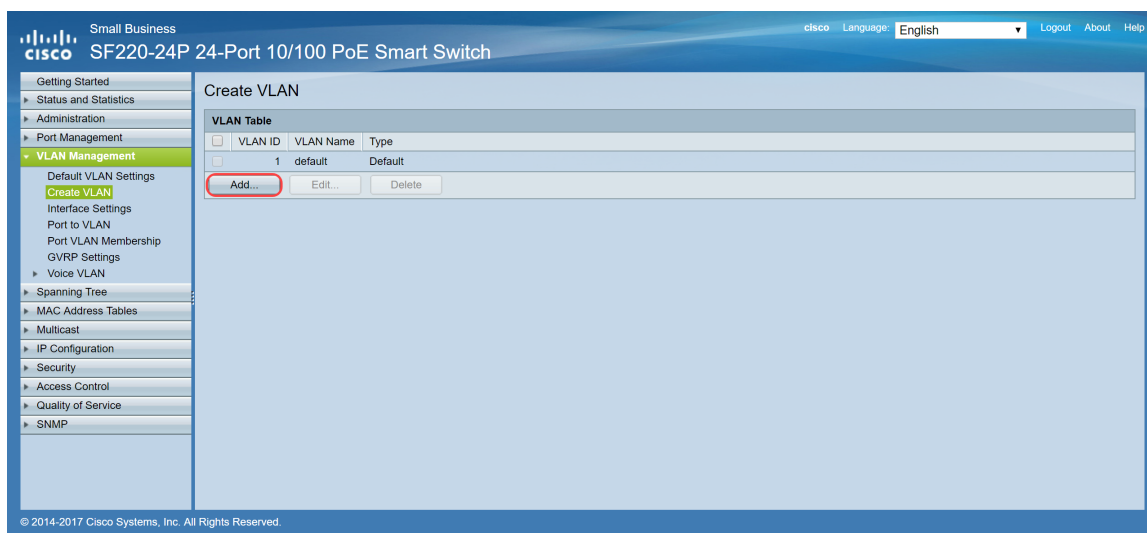
Configurando VLANs no Switch

Etapa 1. Faça login no utilitário baseado na Web e navegue até **VLAN Management > Create VLAN**.

Nota: A configuração pode variar dependendo do dispositivo. Neste exemplo, estamos usando o SF220-24P para configurar VLANs.

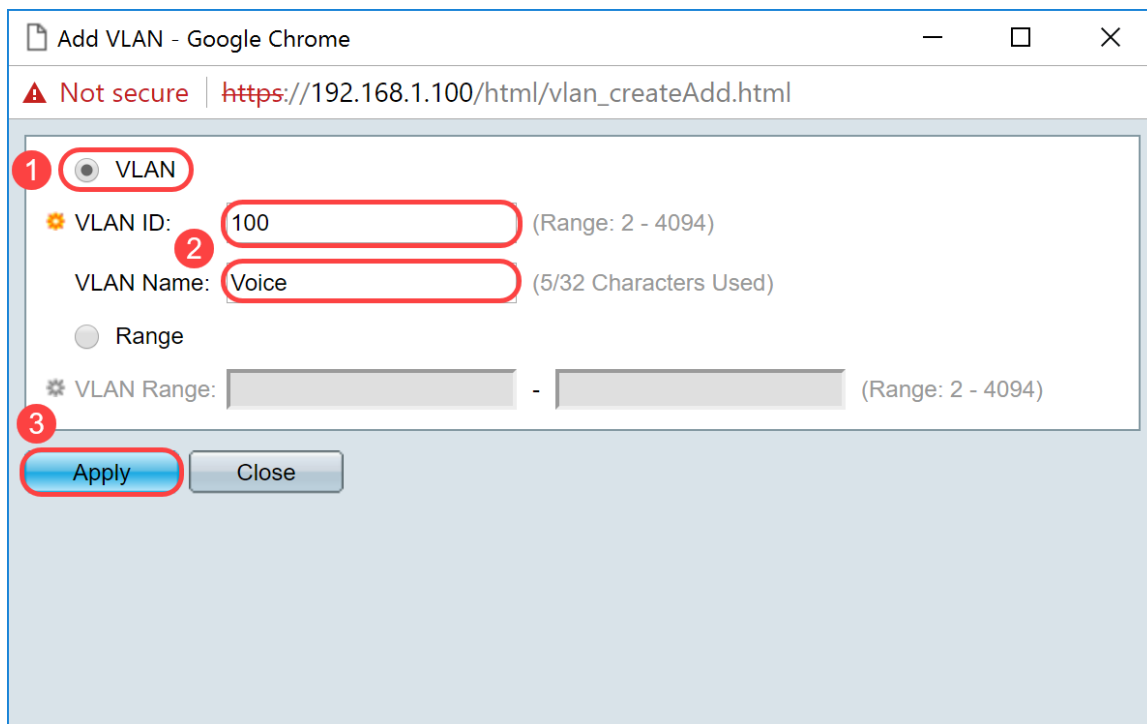


Etapa 2. Clique em **Add...** para criar uma nova VLAN.



Etapa 3. Para criar uma única VLAN, selecione o botão de opção **VLAN**. Insira o **VLAN ID** e o **VLAN Name**. Em seguida, clique em **Apply** para salvar a VLAN. Neste exemplo, criaremos a VLAN 100 para voz e 200 para dados.

Observação: algumas VLANs são exigidas pelo sistema para uso interno do sistema e, portanto, não podem ser criadas inserindo-se o VID inicial e o VID final, inclusive. Ao usar a função **Range**, o número máximo de VLANs que você pode criar de uma vez é 100.

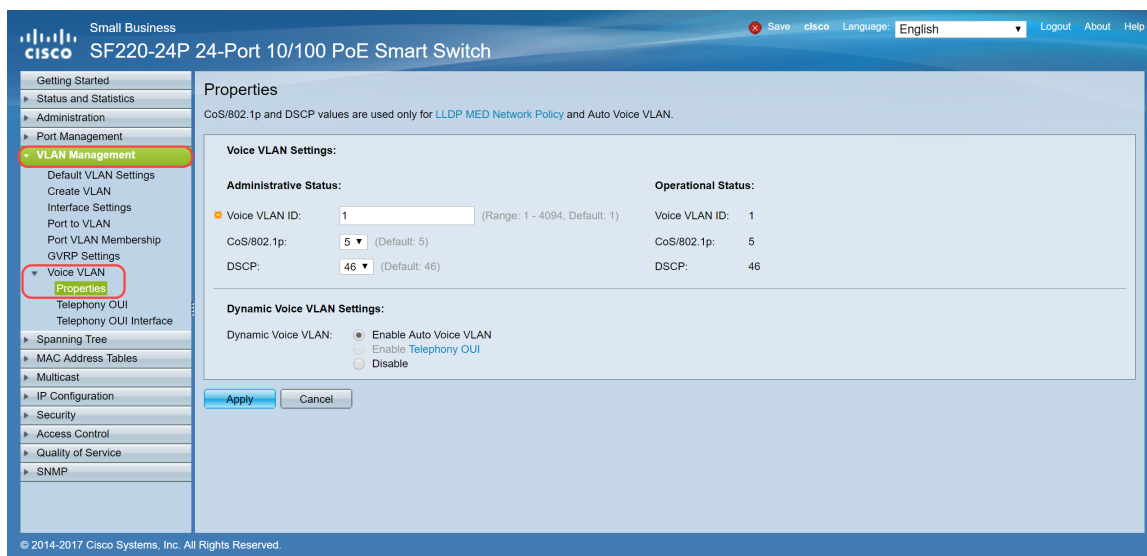


Nota: Repita a Etapa 2 se precisar criar outra VLAN única.

Configurando a VLAN de voz no Switch

Etapa 1. Faça login na configuração da Web e navegue até **VLAN Management > Voice VLAN > Properties**.

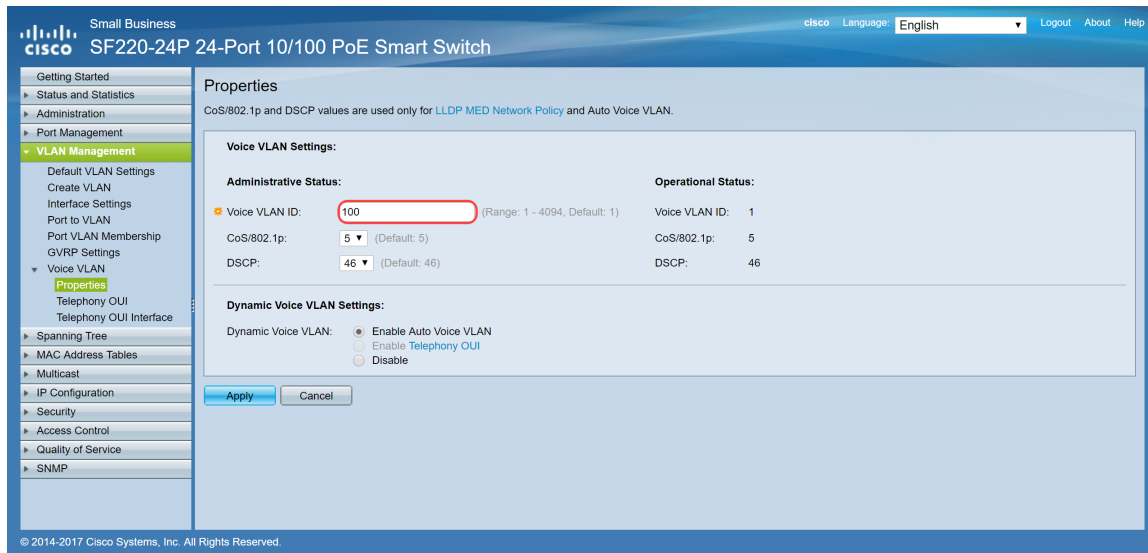
Nota: Configurar VLAN de voz automática aplicará automaticamente as configurações de QoS para VLAN de voz e priorizará o tráfego de voz.



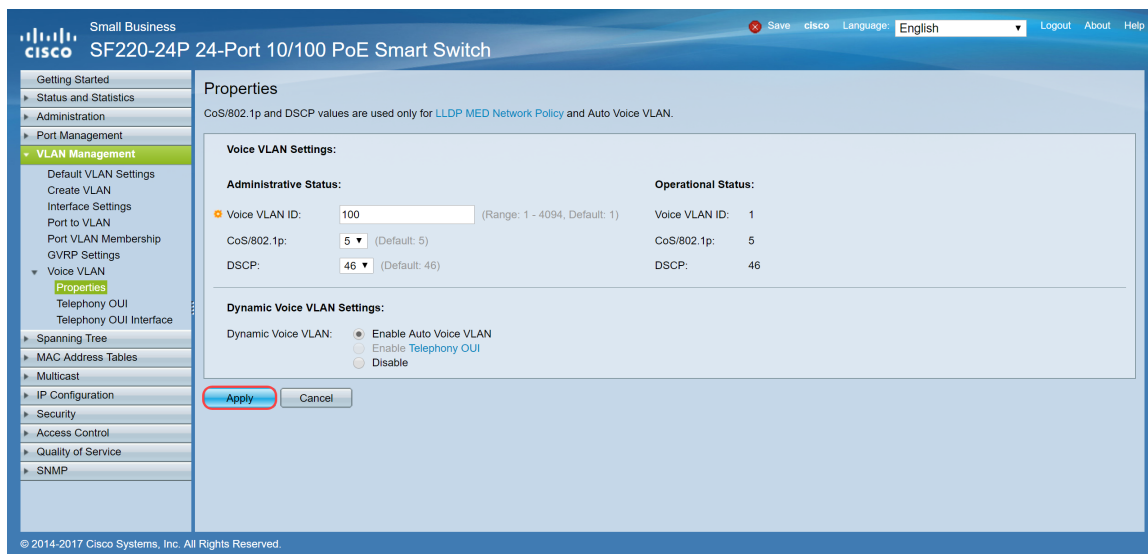
Etapa 2. Em *Administrative Status*, insira a VLAN que deve ser a VLAN de voz no campo *Voice VLAN ID*. Neste exemplo, a VLAN 100 é inserida para ser a VLAN de voz.

Nota: As alterações na VLAN ID de voz, Classe de Serviço (CoS)/802.1p e/ou Ponto de Código de Serviço Diferenciado (DSCP) fazem com que o dispositivo anuncie a VLAN de voz administrativa como uma VLAN de voz estática. Se a opção *Ativação automática de VLAN de voz* disparada por VLAN de voz externa for selecionada, os valores padrão precisarão ser mantidos. Neste exemplo,

CoS/802.1p é deixado como padrão de 5 e DSCP é deixado como padrão de 46.



Etapa 3. Clique em **Apply** para salvar suas configurações.



Definindo as configurações de interface no switch

As interfaces, as portas físicas no switch, podem ser atribuídas a uma das seguintes configurações:

- Geral: a porta pode suportar todas as funções definidas na especificação IEEE 802.1q. A interface pode ser um membro marcado ou não marcado de uma ou mais VLANs.
- Acesso: Só pode ter uma VLAN configurada na interface e só pode transportar uma VLAN.
- Tronco: pode transportar o tráfego de várias VLANs em um único link e permitir que você estenda as VLANs pela rede.
- Dot1p-Tunnel: coloca a interface no modo QinQ. Isso permite que o usuário use suas próprias disposições de VLAN (PVID) na rede do provedor. O switch estará no modo QinQ quando tiver uma ou mais portas de túnel dot1p.

Etapa 1. Faça login na configuração da Web e navegue até **VLAN Management > Interface Settings**.

Small Business SF220-24P 24-Port 10/100 PoE Smart Switch

Language: English

Getting Started
 Status and Statistics
 Administration
 Port Management
 VLAN Management
 Default VLAN Settings
 Create VLAN
 Interface Settings
 Port to VLAN
 Port VLAN Membership
 GVRP Settings
 Voice VLAN
 Properties
 Telephony OUI
 Telephony OUI Interface
 Spanning Tree
 MAC Address Tables
 Multicast
 IP Configuration
 Security
 Access Control
 Quality of Service
 SNMP

Interface Settings

Interface Settings Table

Filter: Interface Type equals to Port Go

Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Uplink
1	FE1	Trunk	1	Admit All	Enabled	Disabled
2	FE2	Trunk	1	Admit All	Enabled	Disabled
3	FE3	Trunk	1	Admit All	Enabled	Disabled
4	FE4	Trunk	1	Admit All	Enabled	Disabled
5	FE5	Trunk	1	Admit All	Enabled	Disabled
6	FE6	Trunk	1	Admit All	Enabled	Disabled
7	FE7	Trunk	1	Admit All	Enabled	Disabled
8	FE8	Trunk	1	Admit All	Enabled	Disabled
9	FE9	Trunk	1	Admit All	Enabled	Disabled
10	FE10	Trunk	1	Admit All	Enabled	Disabled
11	FE11	Trunk	1	Admit All	Enabled	Disabled
12	FE12	Trunk	1	Admit All	Enabled	Disabled
13	FE13	Trunk	1	Admit All	Enabled	Disabled
14	FE14	Trunk	1	Admit All	Enabled	Disabled
15	FE15	Trunk	1	Admit All	Enabled	Disabled
16	FE16	Trunk	1	Admit All	Enabled	Disabled
17	FE17	Trunk	1	Admit All	Enabled	Disabled
18	FE18	Trunk	1	Admit All	Enabled	Disabled

Showing 1-26 of 26 All per page

© 2014-2017 Cisco Systems, Inc. All Rights Reserved.

Etapa 2. Seleção o modo de interface para a VLAN. Neste exemplo, configuraremos o Raspberry Pi (porta: FE3) como uma porta de acesso.

Small Business SF220-24P 24-Port 10/100 PoE Smart Switch

Language: English

Getting Started
 Status and Statistics
 Administration
 Port Management
 VLAN Management
 Default VLAN Settings
 Create VLAN
 Interface Settings
 Port to VLAN
 Port VLAN Membership
 GVRP Settings
 Voice VLAN
 Spanning Tree
 MAC Address Tables
 Multicast
 IP Configuration
 Security
 Access Control
 Quality of Service
 SNMP

Interface Settings

Interface Settings Table

Filter: Interface Type equals to Port Go

Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Uplink
1	FE1	Trunk	1	Admit All	Enabled	Disabled
2	FE2	Trunk	1	Admit All	Enabled	Disabled
3	FE3	Trunk	1	Admit All	Enabled	Disabled
4	FE4	Trunk	1	Admit All	Enabled	Disabled
5	FE5	Trunk	1	Admit All	Enabled	Disabled
6	FE6	Trunk	1	Admit All	Enabled	Disabled
7	FE7	Trunk	1	Admit All	Enabled	Disabled
8	FE8	Trunk	1	Admit All	Enabled	Disabled
9	FE9	Trunk	1	Admit All	Enabled	Disabled
10	FE10	Trunk	1	Admit All	Enabled	Disabled
11	FE11	Trunk	1	Admit All	Enabled	Disabled
12	FE12	Trunk	1	Admit All	Enabled	Disabled
13	FE13	Trunk	1	Admit All	Enabled	Disabled
14	FE14	Trunk	1	Admit All	Enabled	Disabled
15	FE15	Trunk	1	Admit All	Enabled	Disabled
16	FE16	Trunk	1	Admit All	Enabled	Disabled
17	FE17	Trunk	1	Admit All	Enabled	Disabled

Showing 1-26 of 26 All per page

© 2014-2017 Cisco Systems, Inc. All Rights Reserved.

Etapa 3. Em seguida, clique em **Editar...** para editar a interface.

Small Business SF220-24P 24-Port 10/100 PoE Smart Switch

Language: English

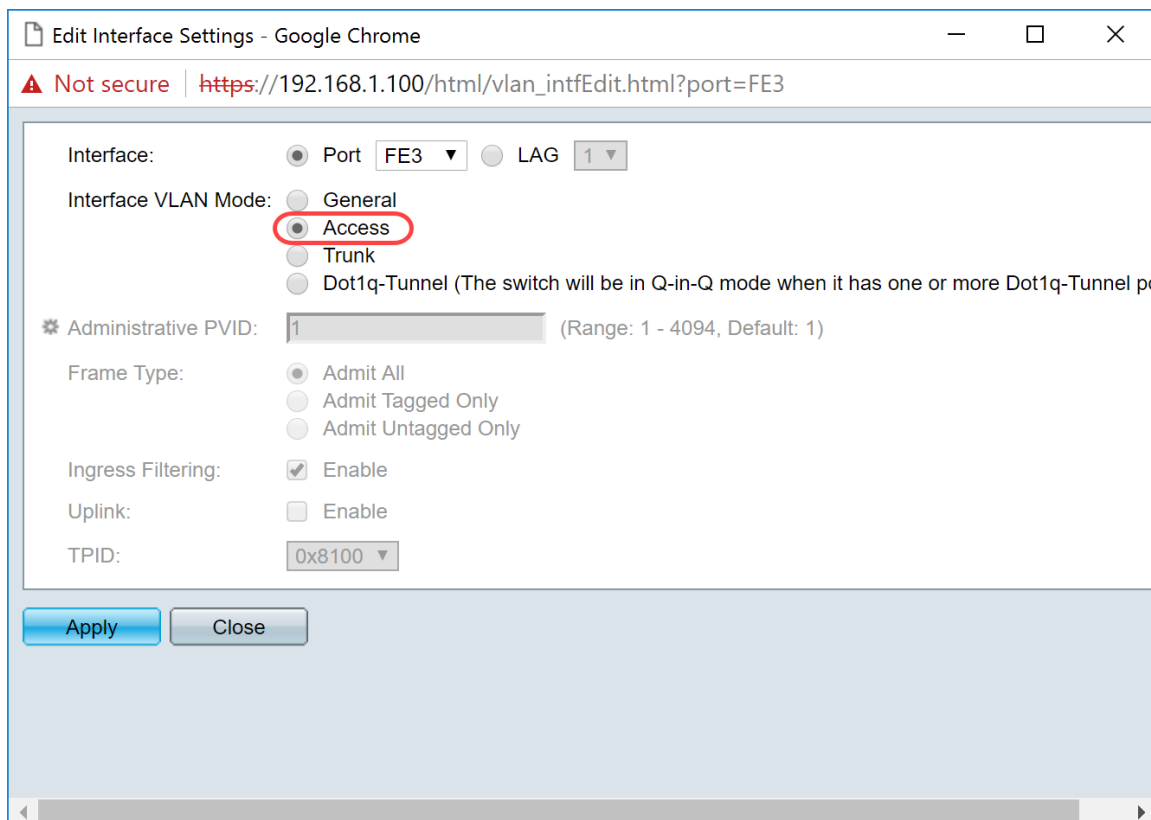
Getting Started
 Status and Statistics
 Administration
 Port Management
 VLAN Management
 Default VLAN Settings
 Create VLAN
 Interface Settings
 Port to VLAN
 Port VLAN Membership
 GVRP Settings
 Voice VLAN
 Spanning Tree
 MAC Address Tables
 Multicast
 IP Configuration
 Security
 Access Control
 Quality of Service
 SNMP

7	FE7	Trunk	1	Admit All	Enabled	Disabled
8	FE8	Trunk	1	Admit All	Enabled	Disabled
9	FE9	Trunk	1	Admit All	Enabled	Disabled
10	FE10	Trunk	1	Admit All	Enabled	Disabled
11	FE11	Trunk	1	Admit All	Enabled	Disabled
12	FE12	Trunk	1	Admit All	Enabled	Disabled
13	FE13	Trunk	1	Admit All	Enabled	Disabled
14	FE14	Trunk	1	Admit All	Enabled	Disabled
15	FE15	Trunk	1	Admit All	Enabled	Disabled
16	FE16	Trunk	1	Admit All	Enabled	Disabled
17	FE17	Trunk	1	Admit All	Enabled	Disabled
18	FE18	Trunk	1	Admit All	Enabled	Disabled
19	FE19	Trunk	1	Admit All	Enabled	Disabled
20	FE20	Trunk	1	Admit All	Enabled	Disabled
21	FE21	Trunk	1	Admit All	Enabled	Disabled
22	FE22	Trunk	1	Admit All	Enabled	Disabled
23	FE23	Trunk	1	Admit All	Enabled	Disabled
24	FE24	Trunk	1	Admit All	Enabled	Disabled
25	GE1	Trunk	1	Admit All	Enabled	Disabled
26	GE2	Trunk	1	Admit All	Enabled	Disabled

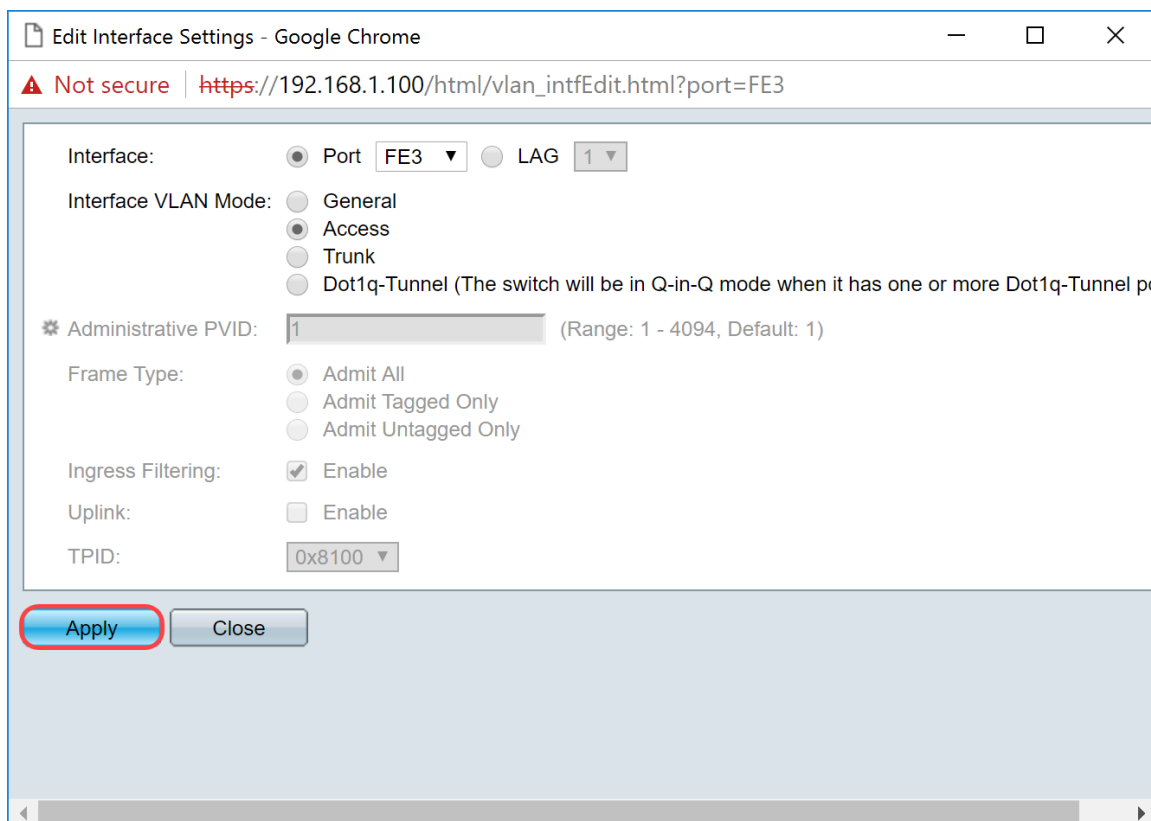
Copy Settings... Edit...

© 2014-2017 Cisco Systems, Inc. All Rights Reserved.

Etapa 4. No campo *Interface VLAN Mode*, escolha **Access** para configurar a interface como um membro não marcado de uma única VLAN.



Etapa 5. Clique em **Apply** para salvar suas configurações.



Configurando a participação de VLAN de porta no switch

Depois que as VLANs são criadas, você precisa atribuir VLANs às portas que deseja conectar.

Etapa 1. Faça login na configuração da Web e navegue até **VLAN Management > Port VLAN**

Membership.

The screenshot shows the Cisco configuration interface for a Small Business SF220-24P 24-Port 10/100 PoE Smart Switch. The 'Port VLAN Membership' page is displayed, showing a table of interface configurations. The table has columns for Interface, Mode, Administrative VLANs, Operational VLANs, and LAG. The row for FE3 is highlighted in green, indicating it is selected for configuration.

Interface	Mode	Administrative VLANs	Operational VLANs	LAG
FE1	Trunk	1UP	1UP, 100T	
FE2	Trunk	1UP	1UP, 100T	
FE3	Access	1UP	1UP	
FE4	Trunk	1UP	1UP	
FE5	Trunk	1UP	1UP	
FE6	Trunk	1UP	1UP	
FE7	Trunk	1UP	1UP	
FE8	Trunk	1UP	1UP	
FE9	Trunk	1UP	1UP	
FE10	Trunk	1UP	1UP	
FE11	Trunk	1UP	1UP	
FE12	Trunk	1UP	1UP	
FE13	Trunk	1UP	1UP	
FE14	Trunk	1UP	1UP	
FE15	Trunk	1UP	1UP	
FE16	Trunk	1UP	1UP	

Etapa 2. Na *Tabela de participação de VLAN de porta*, selecione a interface que você deseja configurar para a participação de VLAN. Neste exemplo, configuraremos o Raspberry Pi (Porta: FE3) para estar na VLAN 100.

Nota: Todos os dispositivos de voz já serão configurados para a VLAN de voz que você selecionou na seção [Configurando VLAN de voz no Switch](#).

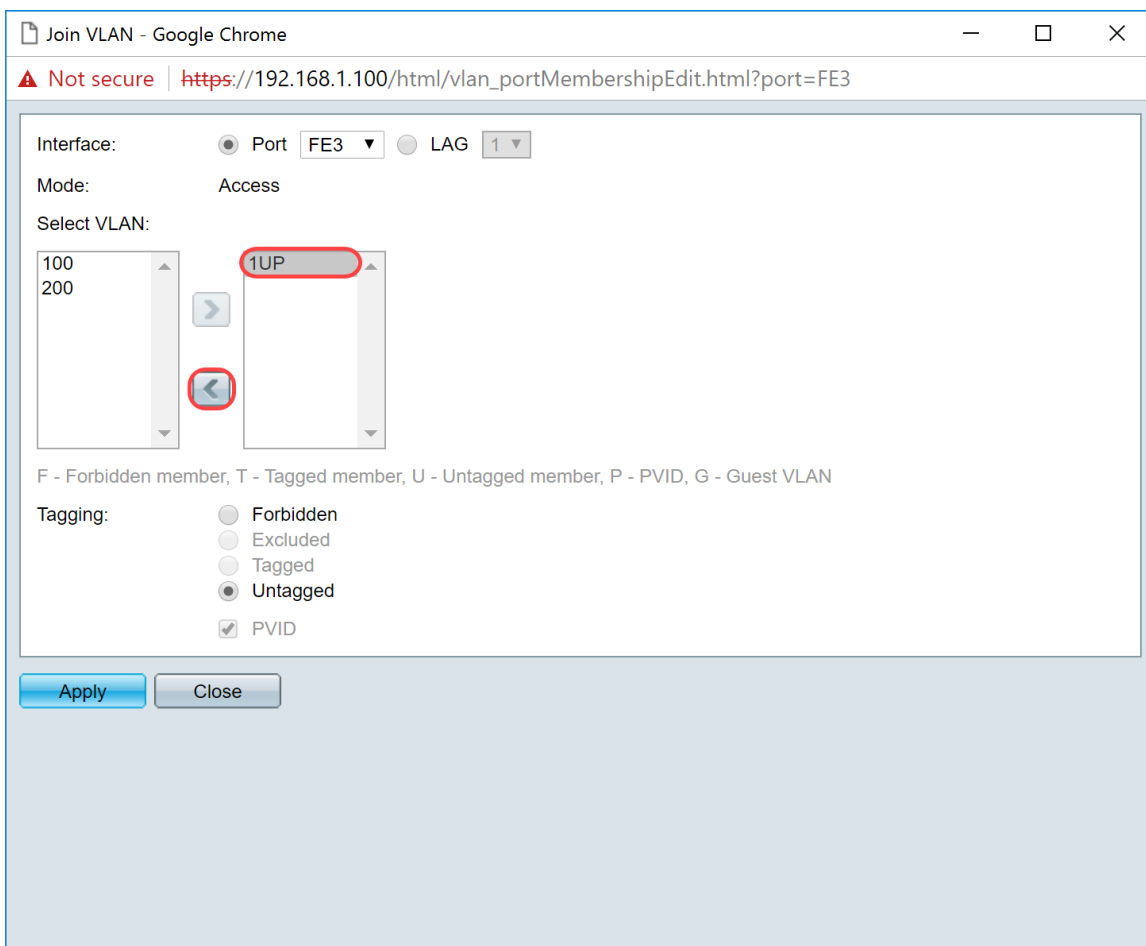
The screenshot shows the same Cisco configuration interface as above, but now the row for FE3 is highlighted in green, indicating it is selected for configuration.

Interface	Mode	Administrative VLANs	Operational VLANs	LAG
FE1	Trunk	1UP	1UP, 100T	
FE2	Trunk	1UP	1UP, 100T	
FE3	Access	1UP	1UP	
FE4	Trunk	1UP	1UP	
FE5	Trunk	1UP	1UP	
FE6	Trunk	1UP	1UP	
FE7	Trunk	1UP	1UP	
FE8	Trunk	1UP	1UP	
FE9	Trunk	1UP	1UP	
FE10	Trunk	1UP	1UP	
FE11	Trunk	1UP	1UP	
FE12	Trunk	1UP	1UP	
FE13	Trunk	1UP	1UP	
FE14	Trunk	1UP	1UP	
FE15	Trunk	1UP	1UP	
FE16	Trunk	1UP	1UP	

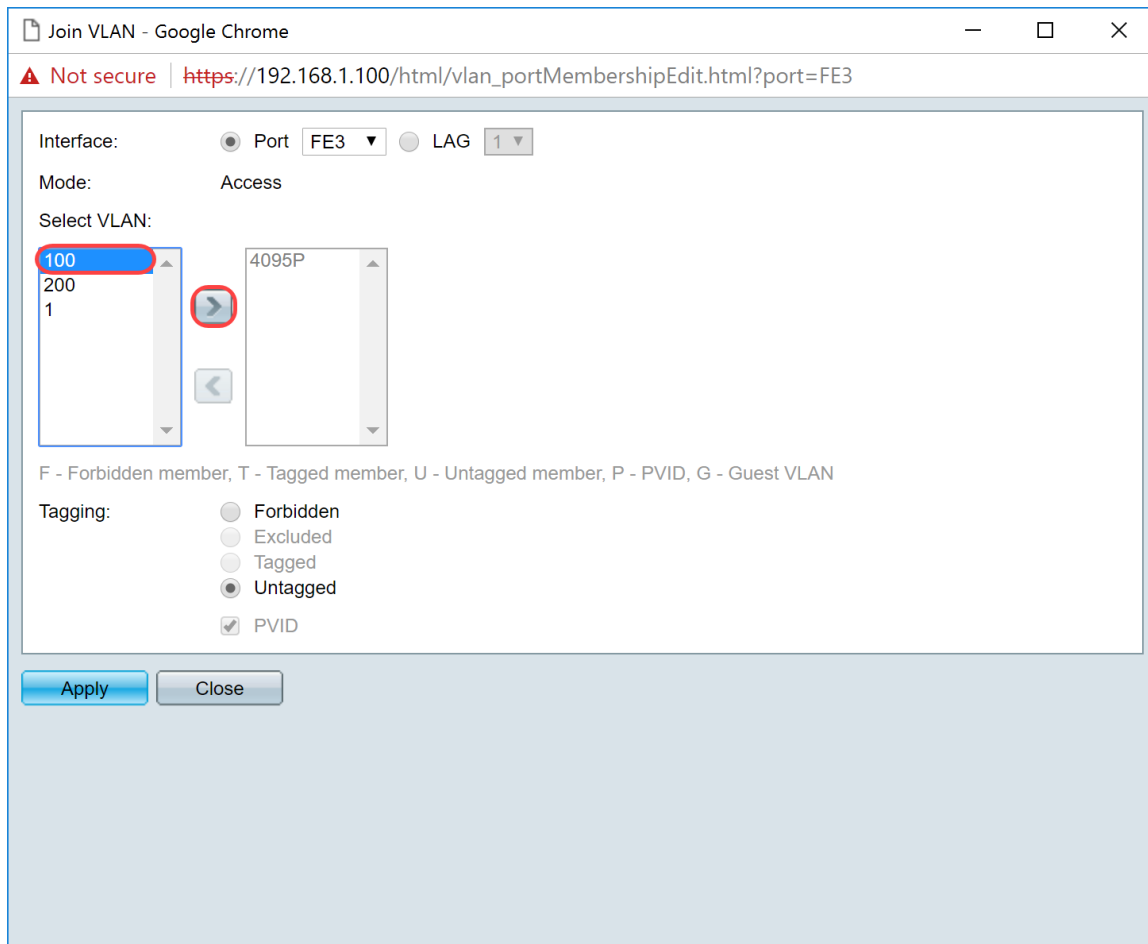
Etapa 3. Clique em **Join VLAN...** para modificar a porta na qual você deseja configurar VLANs.



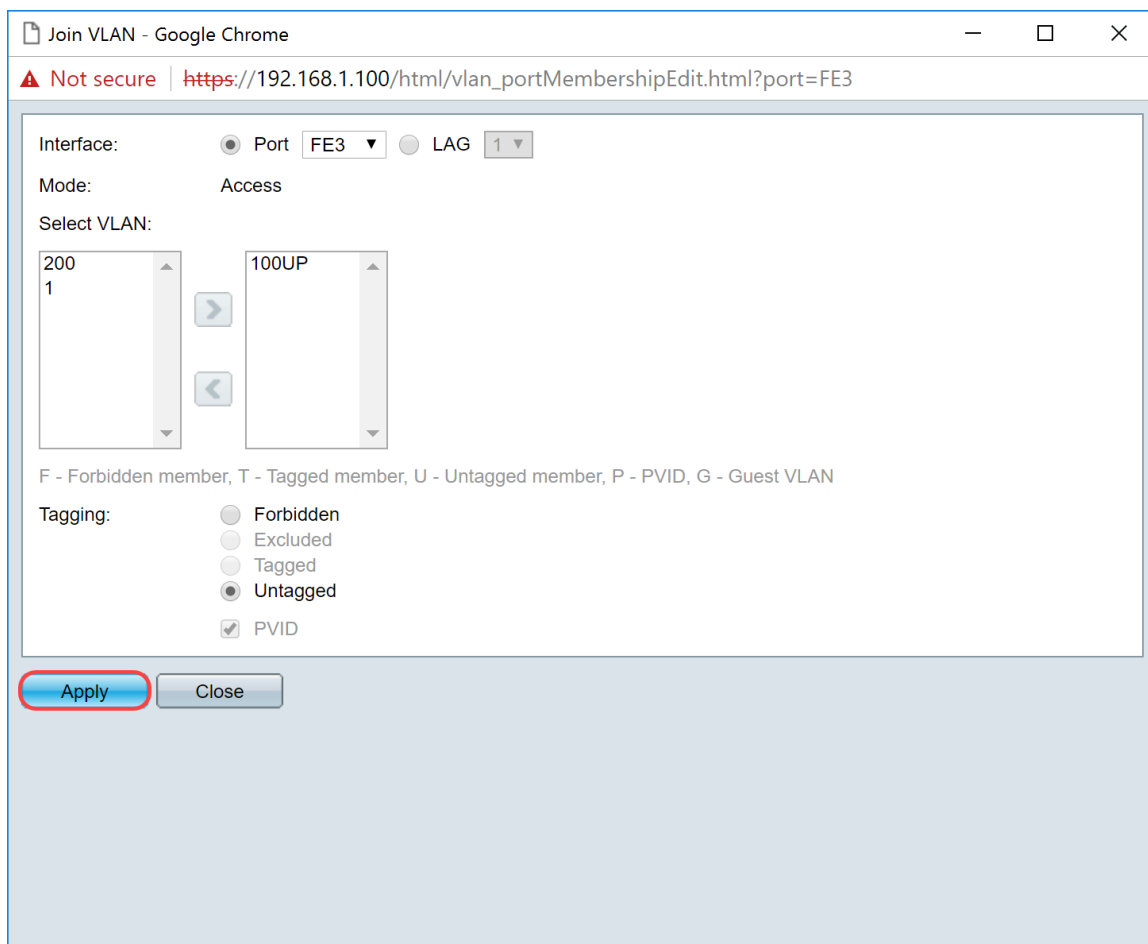
Etapa 4. Selecione **1UP** e clique em < para remover a VLAN 1 da interface na seção *Selecionar VLAN*. Apenas 1 VLAN sem rótulo pode ser adicionada à interface quando for uma porta de acesso.



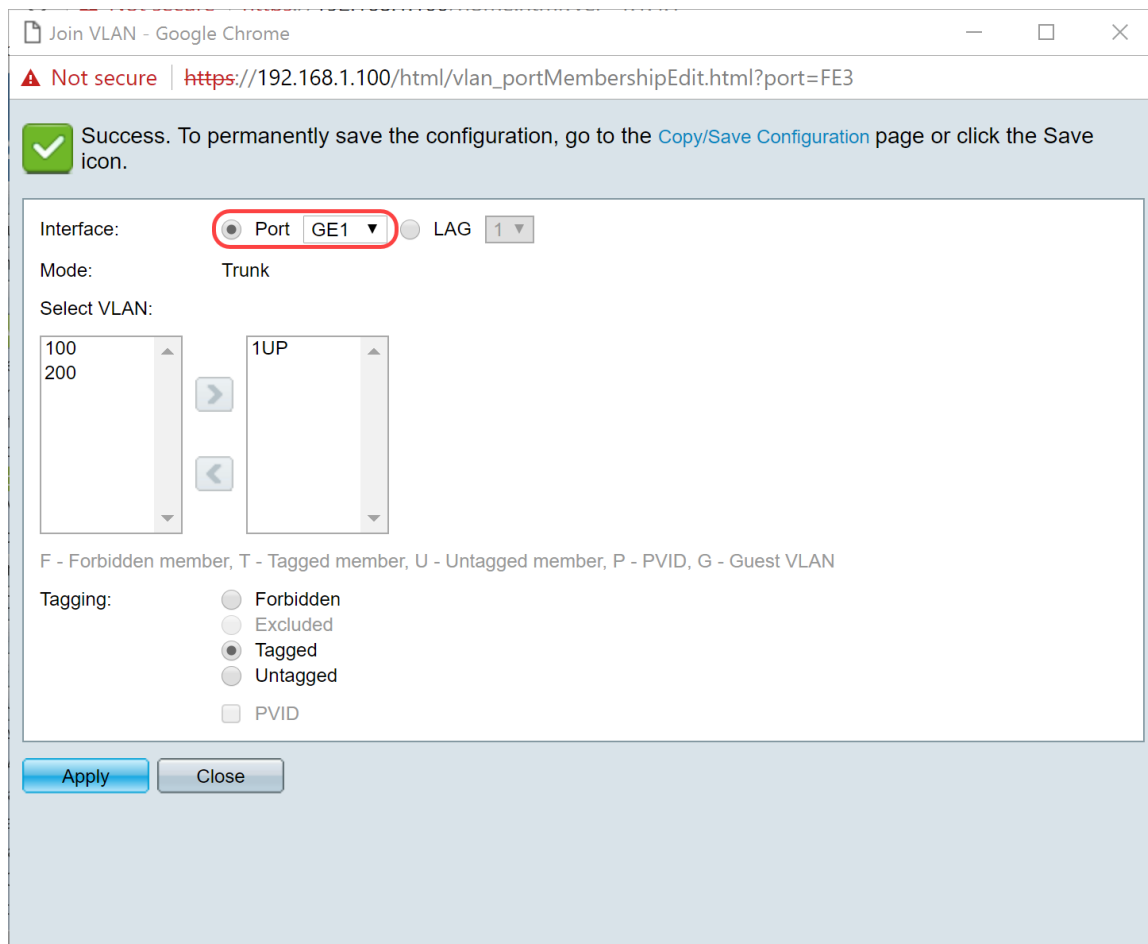
Etapa 5. Selecione **100** e clique em > para adicionar a VLAN não marcada à interface.



Etapa 6. Clique em **Apply** para salvar suas configurações.



Passo 7. Selecione a porta da interface conectada ao roteador no campo *Interface*. Neste exemplo, a porta GE1 está selecionada.



Join VLAN - Google Chrome
Not secure | https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3

Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

Interface: Port GE1 LAG 1

Mode: Trunk

Select VLAN:

100
200

1UP

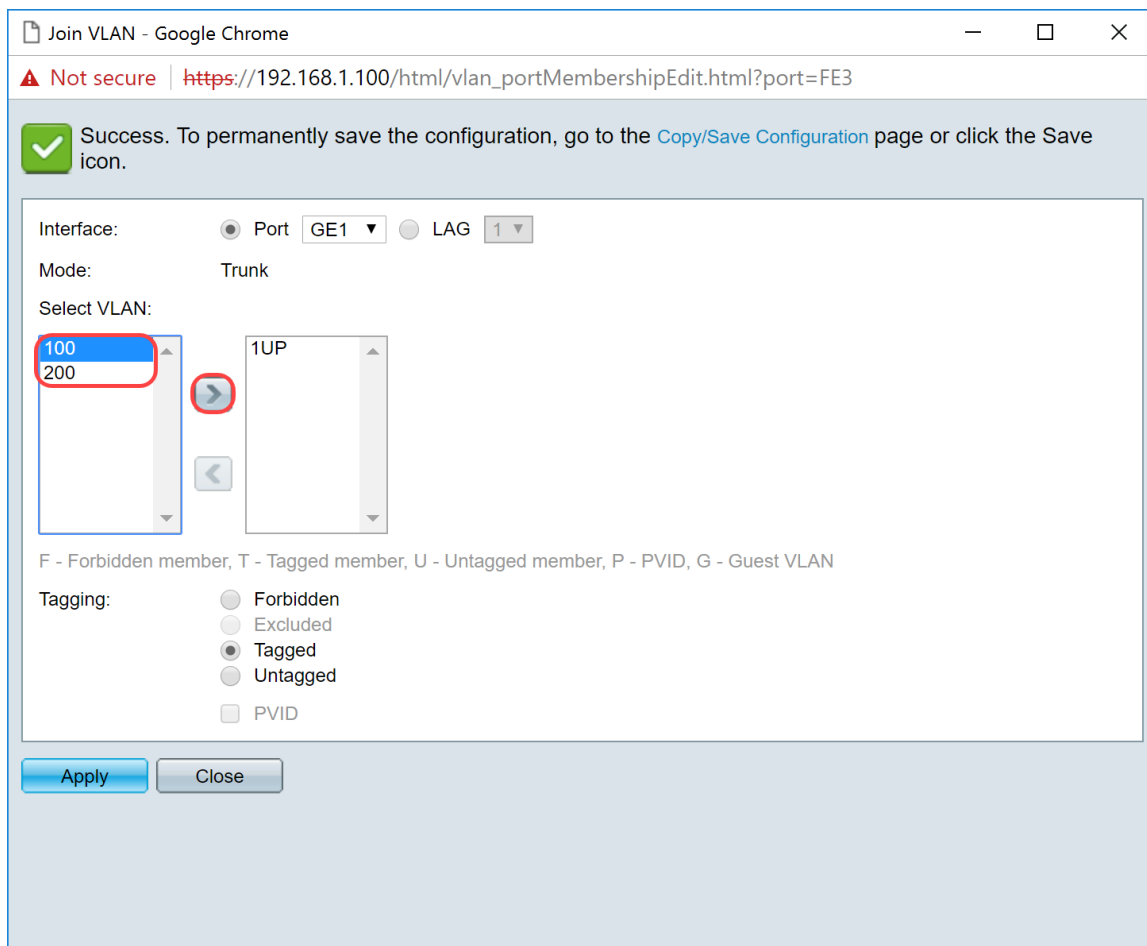
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN

Tagging:

Forbidden
 Excluded
 Tagged
 Untagged
 PVID

Apply Close

Etapa 8. Escolha a VLAN que será adicionada à interface selecionada e clique em > para adicioná-la na seção *Selecionar VLAN*. Neste exemplo, selecionaremos a VLAN **100** e **200**.



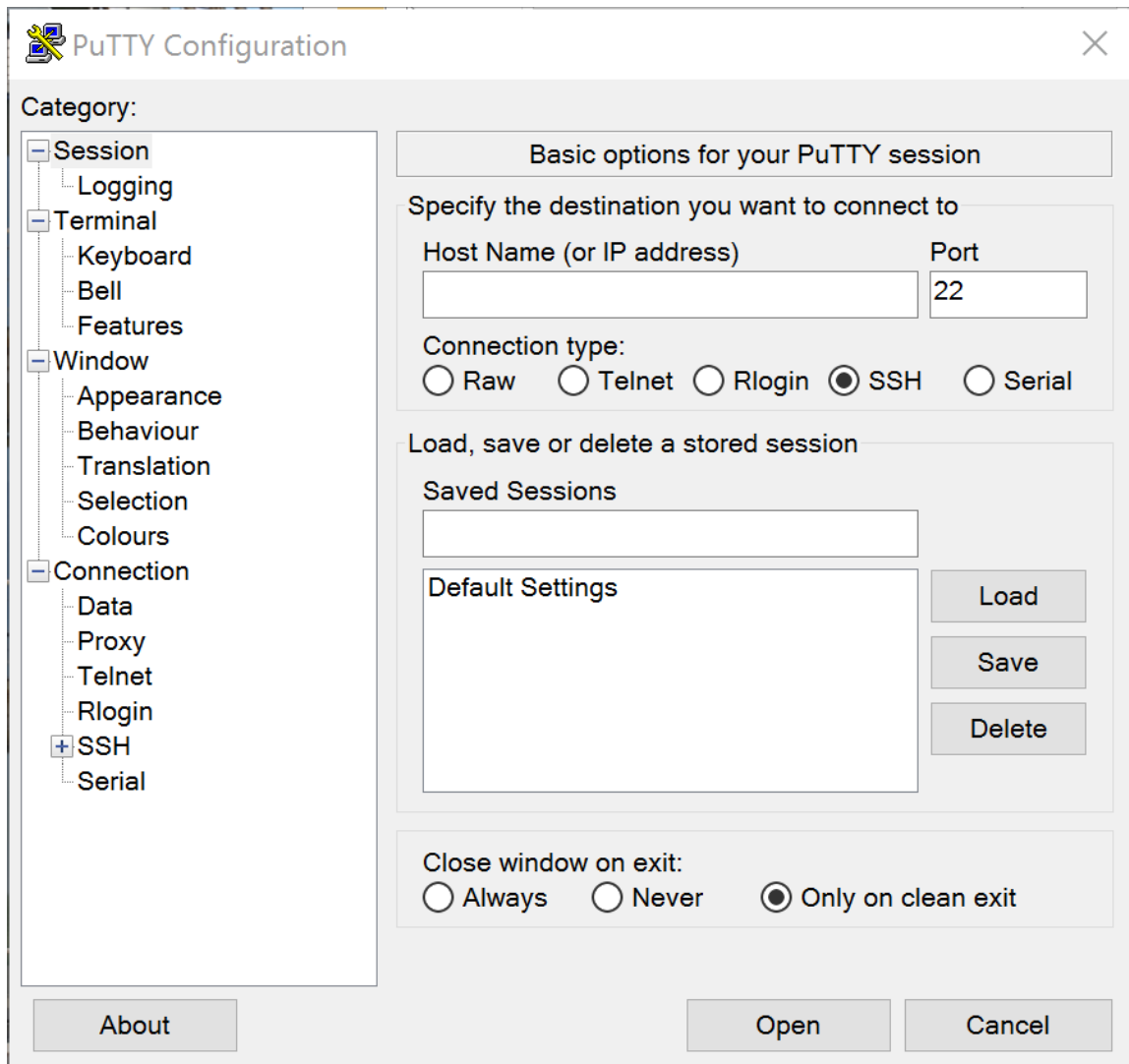
Etapa 9. Clique em **Apply** para salvar suas configurações.

Nota: Uma reinicialização nos telefones IP pode ser necessária para que o endereço IP mude para a sub-rede correta.

Como alterar o endereço IP do Raspberry Pi para uma sub-rede diferente

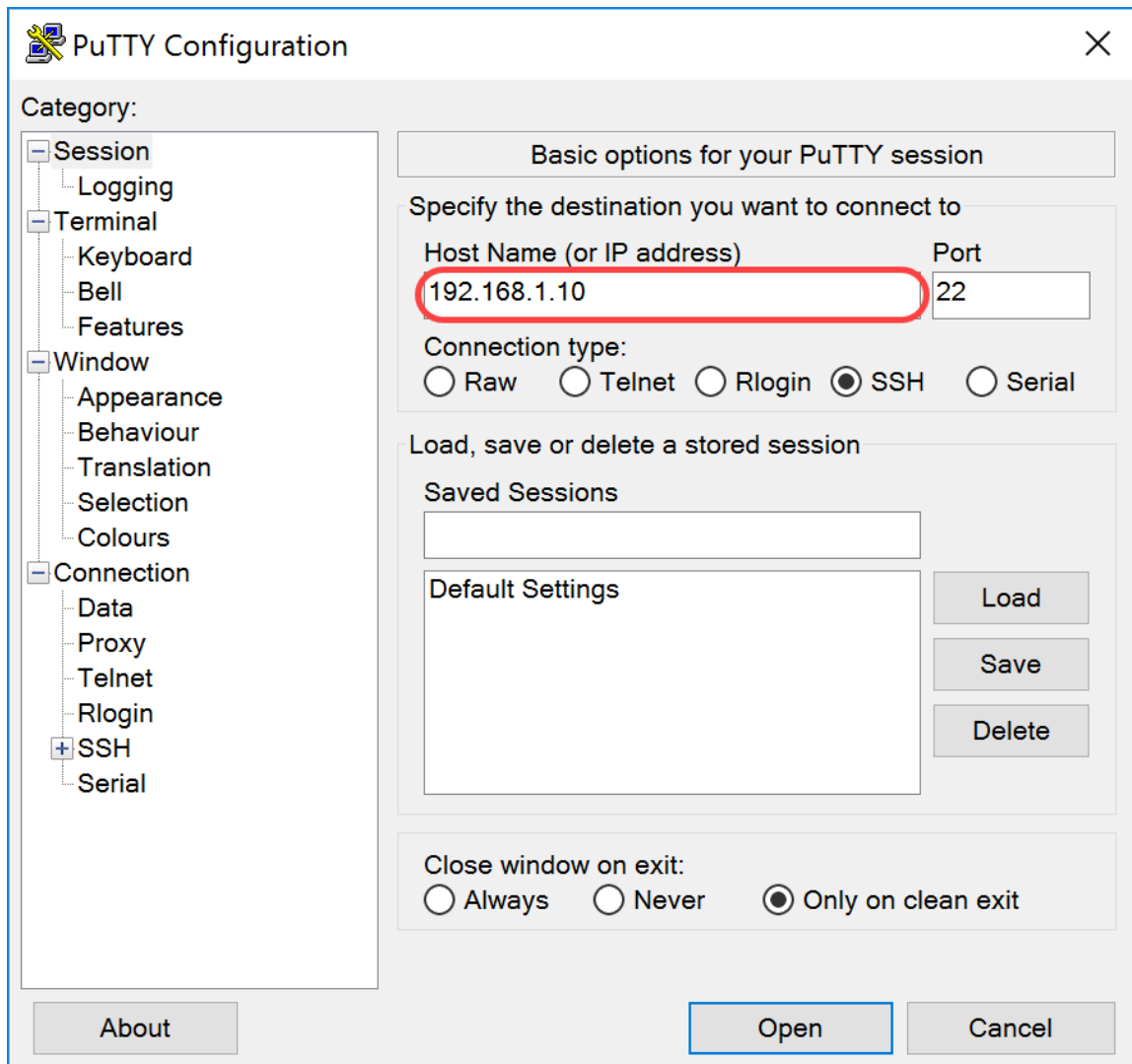
Etapa 1. Conecte-se ao Raspberry Pi pelo Secure Shell (SSH) ou conecte o Raspberry Pi a um monitor de computador. Neste exemplo, usaremos SSH para configurar o Raspberry Pi.

Nota: A porta do switch do computador/laptop precisará estar na mesma VLAN que o Raspberry Pi e configurada como uma porta de acesso ao definir as configurações da interface. Consulte a seção [Definição de Configurações de Interface em um Switch](#) e [Configuração de Associação de VLAN de Porta no Switch](#) deste artigo para revisar. Certifique-se de que seu endereço IP está na mesma rede que seu Raspberry Pi para fazer SSH nele. Se o seu dispositivo não estiver na mesma rede que o Raspberry Pi, use um endereço IP estático e altere manualmente o seu endereço IP para estar na mesma rede ou você pode digitar os comandos **ipconfig /release** e **ipconfig /renew** no prompt de comando para obter um novo endereço IP. Os clientes SSH podem variar dependendo do seu sistema operacional. Neste exemplo, o PuTTY foi usado para SSH no Raspberry Pi. Para obter mais detalhes sobre SSH, clique [aqui](#).

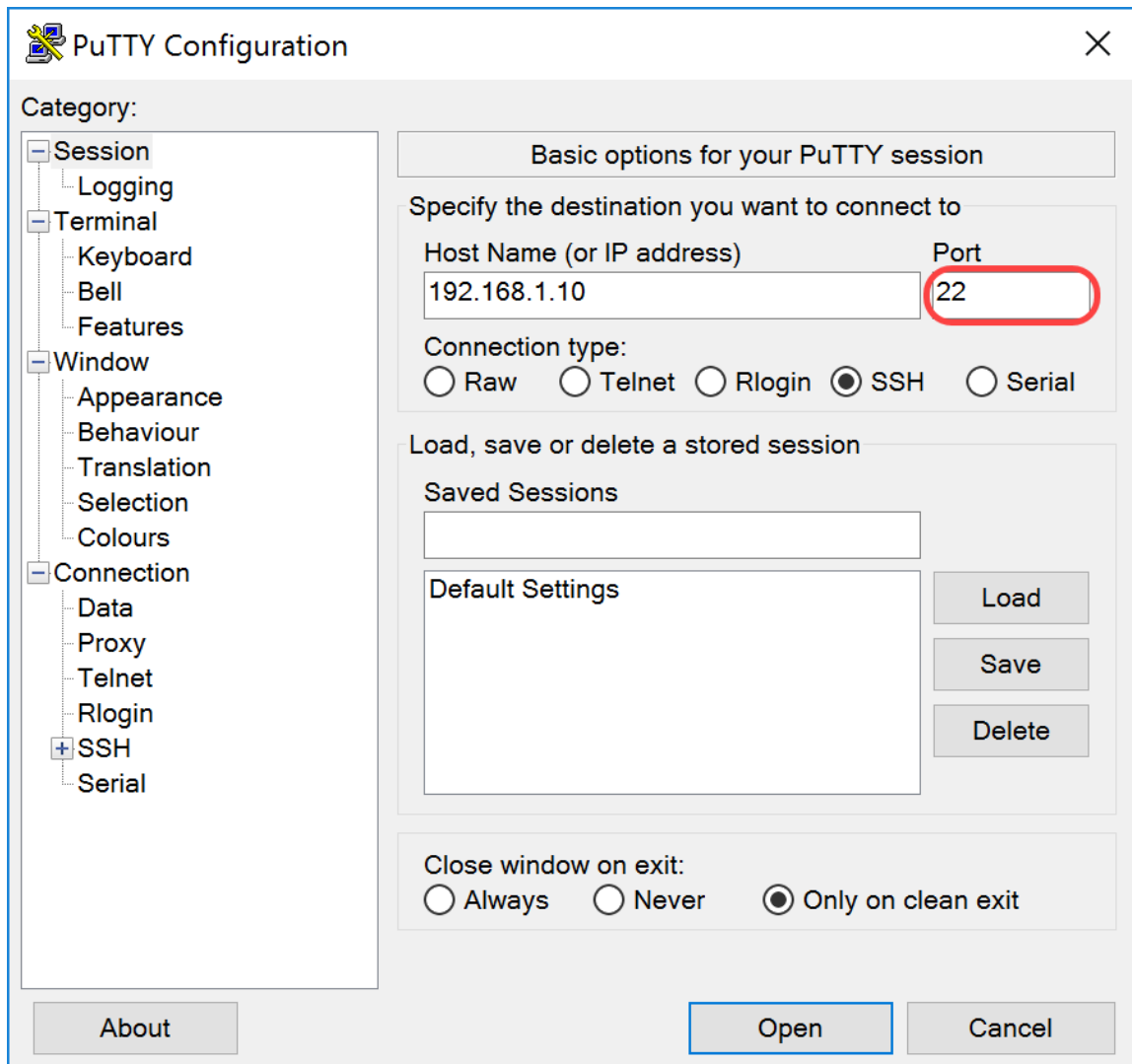


Etapa 2. Digite o endereço IP do seu Raspberry Pi no campo *Nome do host (ou endereço IP)*. Neste exemplo, 192.168.1.10 é inserido.

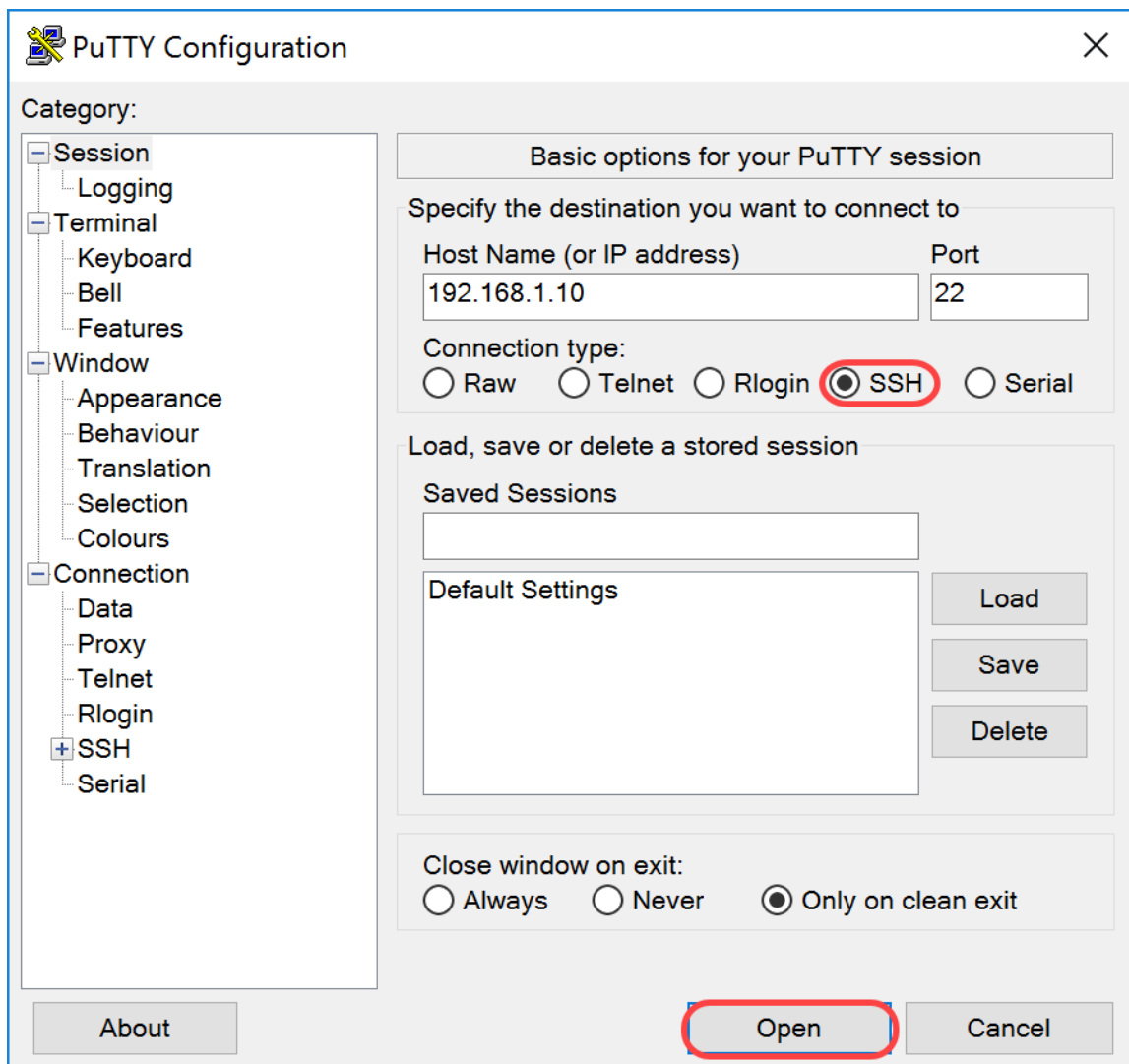
Observação: você pode usar a tabela DHCP no roteador para encontrar o endereço do Raspberry Pi. Neste documento, este Raspberry Pi foi pré-configurado para ter um endereço IP estático.



Etapa 3. Insira **22** como o número da porta no campo *Port*. A porta 22 é a porta padrão para o protocolo SSH.

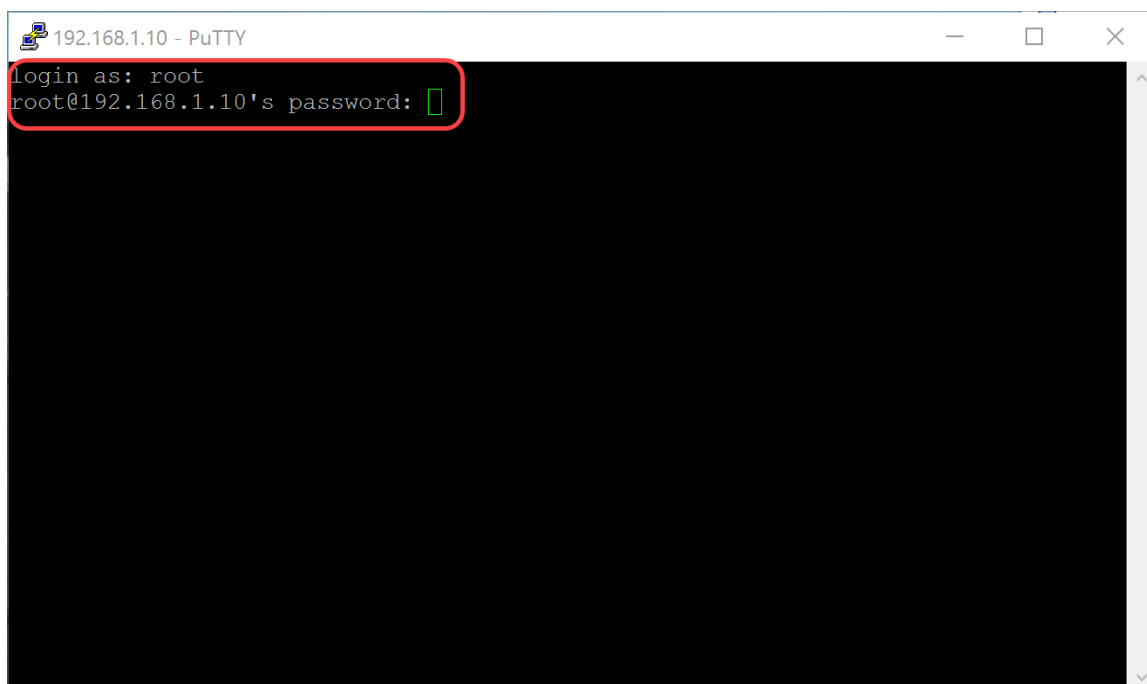


Etapa 4. Na seção *Tipo de conexão:* , clique no botão de opção **SSH** para escolher SSH como seu método de conexão com o switch. Em seguida, clique em **Abrir** para iniciar a sessão.



Etapa 5. Insira o nome de usuário e a senha do RasPBX no campo *login as e password*.

Nota: O usuário padrão: **root** e a senha padrão: **ramboesa**

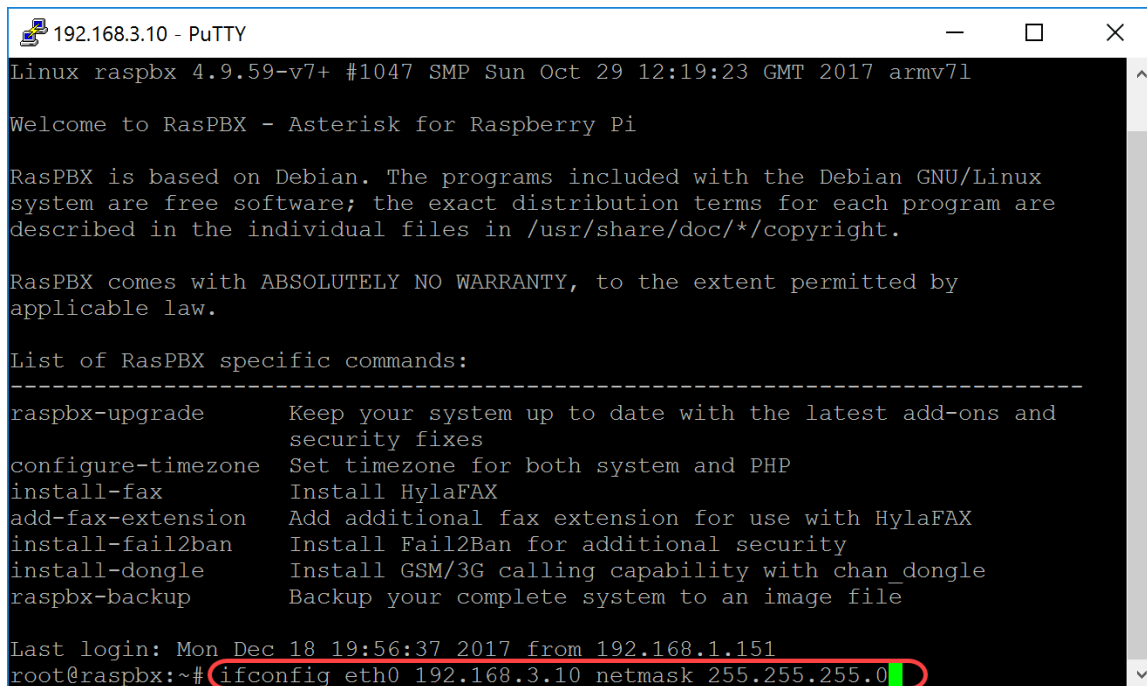


Etapa 6. Para alterar o endereço IP de sua Ethernet para ser um endereço IP estático, digite `ifconfig`

eth0 [endereço IP] netmask [máscara de rede]. Neste exemplo, usaremos 192.168.3.10 e a máscara de rede 255.255.255.0

```
ifconfig eth0 192.168.3.10 máscara de rede 255.255.255.0
```

Observação: você será desconectado da sessão quando alterar o endereço IP. Para se conectar novamente ao Raspberry Pi, seu computador/laptop precisa estar na mesma sub-rede que o Raspberry Pi (192.168.3.x).



```
192.168.3.10 - PuTTY
Linux raspbx 4.9.59-v7+ #1047 SMP Sun Oct 29 12:19:23 GMT 2017 armv7l
Welcome to RaspPBX - Asterisk for Raspberry Pi

RaspPBX is based on Debian. The programs included with the Debian GNU/Linux
system are free software; the exact distribution terms for each program are
described in the individual files in /usr/share/doc/*/copyright.

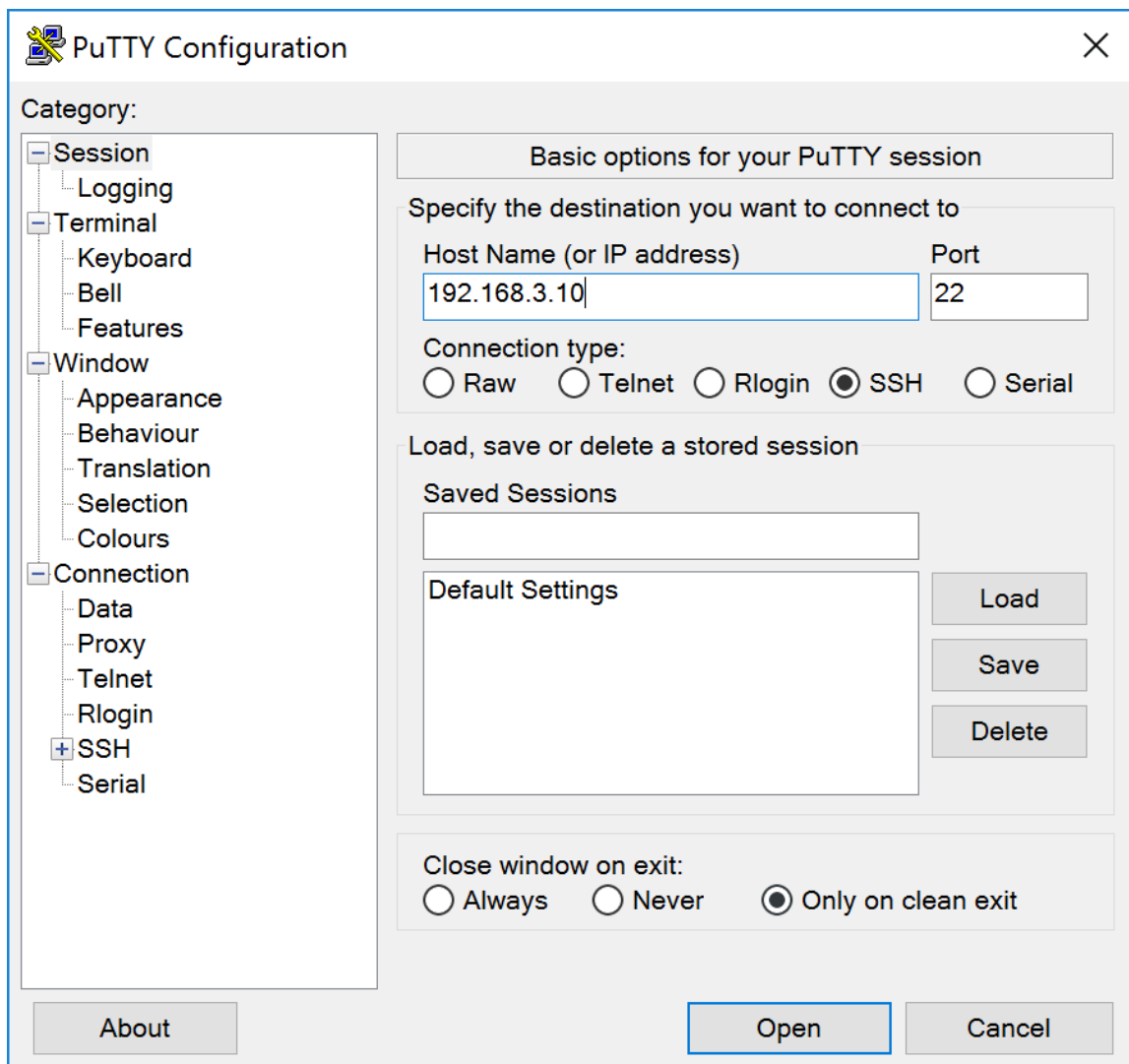
RaspPBX comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

List of RaspPBX specific commands:
-----
raspbx-upgrade      Keep your system up to date with the latest add-ons and
                    security fixes
configure-timezone  Set timezone for both system and PHP
install-fax         Install HylaFAX
add-fax-extension   Add additional fax extension for use with HylaFAX
install-fail2ban    Install Fail2Ban for additional security
install-dongle      Install GSM/3G calling capability with chan_dongle
raspbx-backup       Backup your complete system to an image file

Last login: Mon Dec 18 19:56:37 2017 from 192.168.1.151
root@raspbx:~# ifconfig eth0 192.168.3.10 netmask 255.255.255.0
```

Passo 7. Conecte-se novamente ao Raspberry Pi usando o endereço IP estático configurado na etapa 6. Neste exemplo, usamos 192.168.3.10 para conectar novamente.

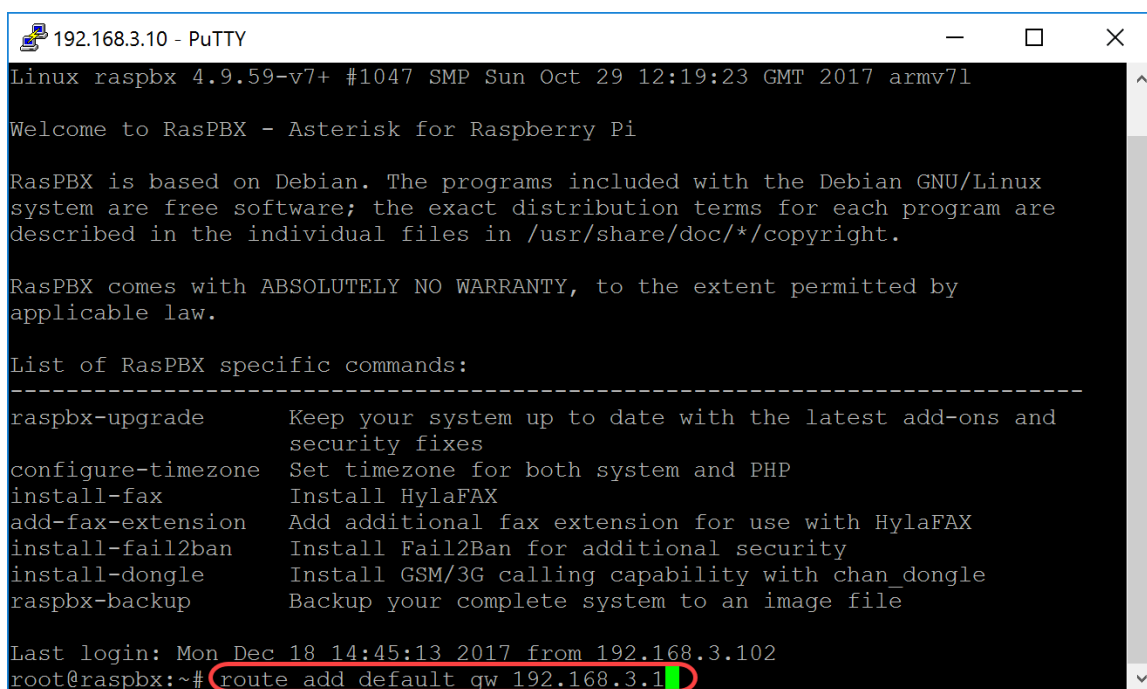
Nota: Certifique-se de que seu computador/laptop esteja na mesma sub-rede que o Raspberry Pi e também a VLAN. Se o seu computador/laptop estiver na mesma VLAN que o Raspberry Pi e você não tiver o endereço IP correto, você pode ir para o prompt de comando e digitar **ipconfig /release** e, em seguida, **ipconfig /renew** para solicitar um novo endereço IP ou você pode configurar seu dispositivo para ter um endereço IP estático nas propriedades Ethernet.



Etapa 8. Na linha de comando, digite `route add default gw [Router IP address of subnet]` para adicionar um gateway padrão.

Observação: você pode usar o comando `route` para ver a tabela de roteamento.

```
route add default gw 192.168.3.1
```



Conclusão

Agora você deve ter configurado com êxito uma rede de voz básica. Para verificar isso, pegue um dos telefones SPA/MPP e você deverá ouvir um tom de discagem. Neste documento, um dos telefones SPA/MPP tem o ramal 1002 e o outro tem o 1003. Você deve conseguir chamar o ramal 1003 ao usar o ramal 1002 do telefone SPA/MPP.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.