

# Cómo crear una red de voz básica con Raspberry Pi

## Objetivo

Este documento proporciona instrucciones sobre cómo configurar una red de voz básica con Raspberry Pi como el servidor de comunicación mediante Asterisks. La red de área local virtual (VLAN) y la calidad de servicio (QoS) se utilizarán para ayudar a priorizar el tráfico mediante la separación del tráfico de voz y de datos. El objetivo de esta red es establecer pruebas internas. Estas pruebas le ayudarán a escalar la red de forma adecuada, ver si tiene suficiente ancho de banda para el volumen de voz que espera y encontrar cualquier otra posible contención entre los equipos. También puede ayudar a determinar si desea alojarlo localmente o en la nube. Una vez que una empresa ha alcanzado un determinado tamaño, es posible que prefiera tener su propio controlador de llamadas local, como PBX o PBX IP. Esto haría que las llamadas internas fueran más eficientes, ya que las llamadas entre teléfonos dentro de la empresa no tendrían que enrutarse fuera del edificio y luego volver a conectarse.

Nota importante: Raspberry Pi no es un producto compatible con Cisco. Este documento se ofrece solo como soporte y no es una solución.

## Introducción

Para que una empresa pueda desarrollar una actividad comercial eficaz, los empleados deben tener acceso a una red de voz. Esto facilita la comunicación entre los empleados y sus clientes, además de permitirles la posibilidad de comunicarse internamente. Se puede proporcionar a cada empleado un teléfono fijo y/o un teléfono celular, pero esto puede llegar a ser bastante caro. Las empresas suelen optar por configurar una red de voz que, en su lugar, utilice el protocolo de voz sobre IP (VoIP).

La tecnología VoIP le permite utilizar Internet para hacer y recibir llamadas telefónicas desde cualquier ubicación, a cualquier ubicación en el mundo con cargos mínimos, si los hay, de larga distancia. Esto se puede utilizar en cualquier dispositivo que utiliza Internet.

VoIP puede ahorrar dinero a la empresa a la vez que aumenta la productividad, la comunicación y la satisfacción del cliente. Los empleados pueden utilizar diferentes funciones, como enrutamiento de llamadas, música en espera y correo de voz integrado.

Una característica común de VoIP que utilizan muchas empresas es el enrutamiento de llamadas, también conocido como distribuidor automático de llamadas. El enrutamiento de llamadas distribuye las llamadas entrantes al siguiente agente disponible en lugar de enviarlas al buzón de voz. Esto garantiza que las llamadas de los clientes se responderán de la forma más eficaz posible. Después del horario laboral, las llamadas se pueden enviar directamente al correo de voz.

Agregar usuarios y actualizar funciones es un proceso sencillo, que resulta útil cuando su empresa está en expansión o sus necesidades cambian. A diferencia de un sistema telefónico tradicional, no es necesario realizar un cableado costoso.

Para configurar una red VoIP, tiene opciones que considerar. Puede alojar un servicio VoIP para su propio sistema telefónico mediante KSU, sin KSU, centralita privada (PBX) u otro sistema VoIP.

Debe tener en cuenta su presupuesto, el número de empleados y ubicaciones, los servicios disponibles en su zona y el crecimiento de la empresa. Es posible que sea necesario disponer también de formación y equipo adicional, como auriculares. VoIP puede aumentar el uso de datos y es posible que necesite aumentar el ancho de banda para dar cuenta del tráfico de red de voz.

También debe planificar una copia de seguridad, "Plan B", en caso de que la red se caiga alguna vez. Si pierde la alimentación, el sistema VoIP no se conectará. Esta redundancia debe implementarse para restaurar inmediatamente los servicios telefónicos y evitar la interrupción de la productividad empresarial.

En este artículo, implementaremos nuestro propio sistema telefónico con Asterisk, un PBX en un Raspberry Pi.

Nota: una vez completados estos pasos y si desea poder llamar desde su red interna, debe elegir un distribuidor de servicios de telefonía por Internet (ITSP).

## Definiciones

Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En situaciones en las que se pueden transmitir datos confidenciales en una red, se puede crear una VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Los usuarios en una VLAN específica son los únicos que pueden acceder y manipular los datos en esa VLAN. Las VLAN también pueden utilizarse para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusiones a destinos innecesarios.

Todos los puertos, de forma predeterminada, se asignan a la VLAN 1, por lo que una vez configuradas diferentes VLAN, debe asignar manualmente cada puerto a la VLAN adecuada.

Cada VLAN debe configurarse con un ID de VLAN (VID) único con un valor entre 1 y 4094. El dispositivo reserva VID 4095 como la VLAN de descarte. Todos los paquetes clasificados en la VLAN de descarte se descartan en el ingreso y no se reenvían a un puerto.

La calidad de servicio (QoS) permite dar prioridad al tráfico de las diferentes aplicaciones, usuarios o flujos de datos. También se puede utilizar para garantizar el rendimiento a un nivel especificado, lo que afecta a la QoS del cliente. QoS se ve generalmente afectada por los siguientes factores: fluctuación, latencia y pérdida de paquetes. En la mayoría de los casos, se da prioridad al vídeo o a la VoIP, ya que son los más afectados por QoS.

La centralita privada (PBX) es un sistema de conmutación telefónica que administra las llamadas entrantes y salientes de los usuarios internos de una empresa. Un PBX está conectado al sistema de telefonía pública y enruta automáticamente las llamadas entrantes a extensiones específicas. También comparte y gestiona varias líneas. Un sistema PBX típico para pequeñas empresas incluye líneas telefónicas externas e internas, un servidor informático que administra el switching y el enrutamiento de llamadas, y una consola para el control manual.

Una PBX IP puede hacer todo lo que una PBX tradicional para pequeñas empresas puede hacer y mucho más. Realiza la conmutación y la conexión de VoIP, así como las llamadas de línea fija. Un sistema PBX IP se ejecuta en una red de datos IP, lo que ahorra costes y minimiza la gestión de la red. Puede utilizar teléfonos IP, softphones (que no requieren ningún hardware telefónico más allá de un ordenador y auriculares de micrófono) y teléfonos fijos en un sistema telefónico PBX IP.

Un Raspberry Pi es un equipo pequeño, portátil y económico que funciona como un equipo de escritorio.

Asterisk es un marco de código abierto que puede convertir un equipo, como un Raspberry Pi, en un servidor de comunicaciones. Esto le permite crear su propio sistema telefónico PBX empresarial. En este artículo, Asterisk utiliza FreePBX como una interfaz gráfica de usuario (GUI) que controla y gestiona Asterisk donde puede configurar extensiones, usuarios, etc.

## Dispositivos aplicables

- Router

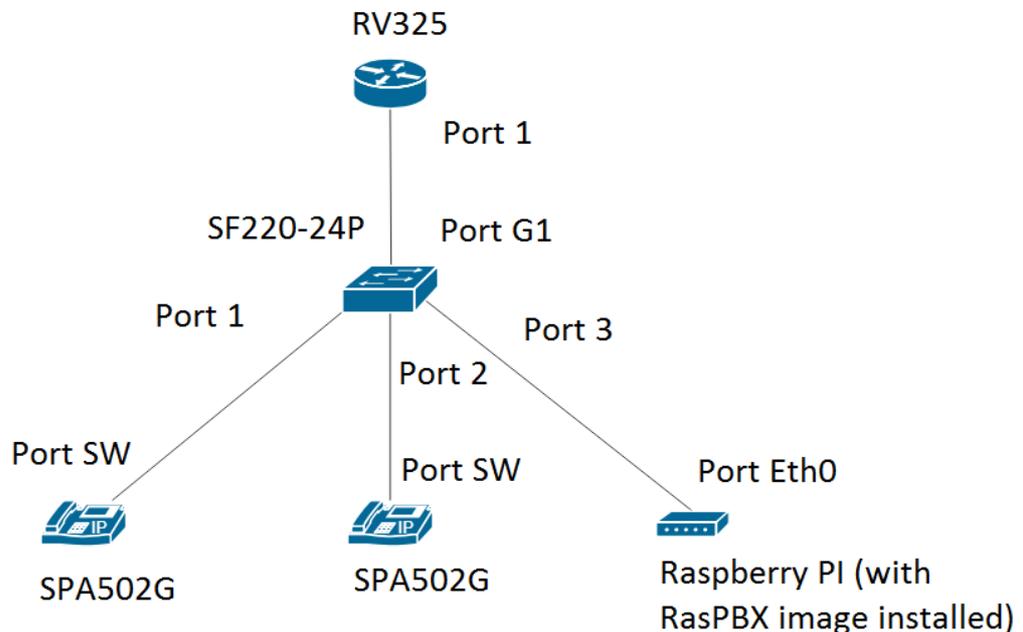
- Switch Power over Ethernet (PoE)
- Raspberry Pi (modelos Pi 3 B+, Pi 3, Pi 3, B+, B y A)
- 2 o más teléfonos Cisco SPA/MPP IP Phones

## Versión del software

- 14.0.1.20 (FreePBX)
- 13.20.0 (Asterisco)
- 1.1.1.06 (router RV325)
- 1.1.4.1 (SF220-24P)
- 7.1.3 (SPA502G)

Para configurar la red de voz básica con Raspberry Pi, siga estas instrucciones:

Topología:



La imagen para el RasPBX se puede encontrar [aquí](#). Esta imagen debe instalarse en el Raspberry Pi.

Nota: En este documento, el Raspberry Pi con la imagen RasPBX ya está configurado. Para

acceder a la GUI del Raspberry Pi, escriba <http://raspbx.local> o la dirección IP del Raspberry Pi en su navegador para configurar el PBX. El inicio de sesión predeterminado de FreePBX es user: admin password: admin. Además, Raspberry Pi estaba preconfigurado para tener una dirección IP estática.

## Table Of Contents

1. [Configuración de VLAN en el router](#)
2. [Configuración de teléfonos SPA/MPP](#)
3. [Configuración de VLAN en un Switch](#)
4. [Configuración de VLAN de voz en un switch](#)
5. [Configuración de los Parámetros de la Interfaz en un Switch](#)
6. [Configuración de la Pertenencia a VLAN de Puerto en un Switch](#)
7. [Cambiar la dirección IP de Raspberry Pi para que esté en una subred diferente](#)
8. [Conclusión](#)

## Configuración de VLAN en el router

Paso 1. Inicie sesión en la utilidad basada en web y navegue hasta Administración de puertos > Pertenencia a VLAN.

Nota: Esto puede variar en función del modelo. En este ejemplo, se utiliza RV325. Para obtener más información sobre cómo acceder a la página de configuración basada en Web, haga clic [aquí](#).

Small Business  
cisco RV325 Gigabit Dual WAN VPN Router

English Log Out About Help

Getting Started  
System Summary  
Setup  
DHCP  
System Management  
Port Management  
Port Setup  
Port Status  
Traffic Statistics  
VLAN Membership  
QoS:CoS/DSCP Setting  
DSCP Marking  
802.1X Configuration  
Firewall  
VPN  
Certificate Management  
Log  
SSL VPN  
User Management  
Wizard

### VLAN Membership

VLAN:  Enable  
Create VLANs and assign the Outgoing Frame Type.  
Up to fourteen new VLANs can be created. VLAN IDs must be in the range (4...4094)

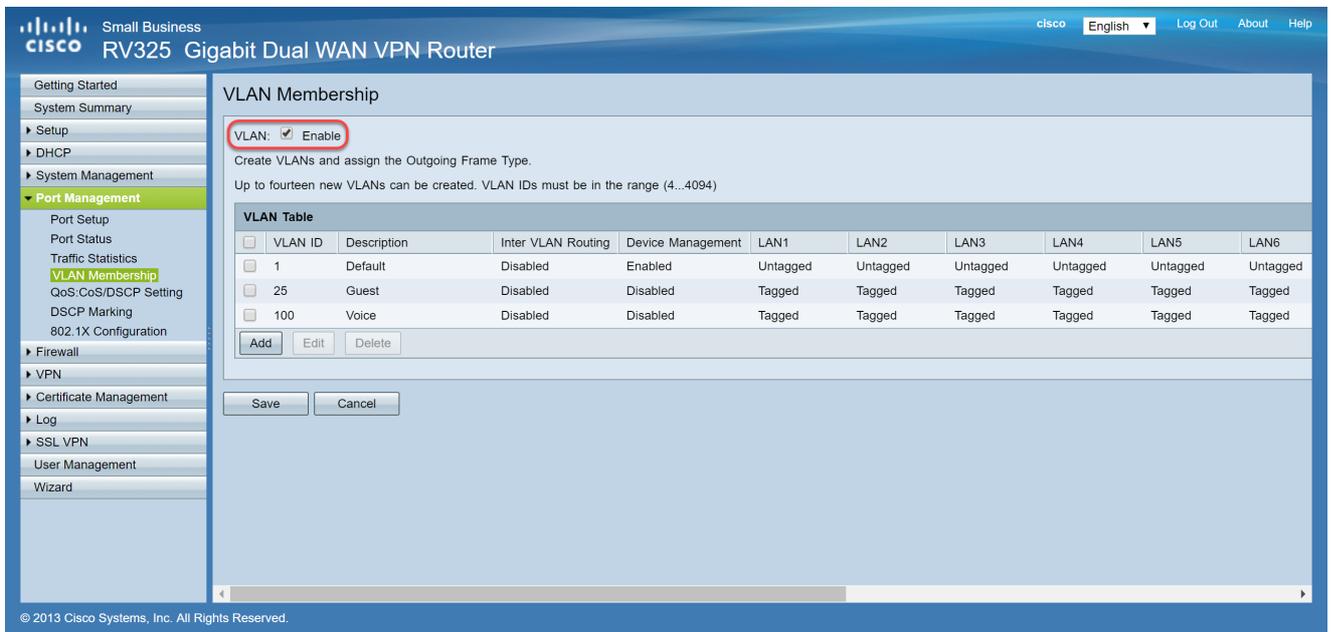
| VLAN ID                      | Description | Inter VLAN Routing | Device Management | LAN1     | LAN2     | LAN3     | LAN4     | LAN5     | LAN6     |
|------------------------------|-------------|--------------------|-------------------|----------|----------|----------|----------|----------|----------|
| <input type="checkbox"/> 1   | Default     | Disabled           | Enabled           | Untagged | Untagged | Untagged | Untagged | Untagged | Untagged |
| <input type="checkbox"/> 25  | Guest       | Disabled           | Disabled          | Tagged   | Tagged   | Tagged   | Tagged   | Tagged   | Tagged   |
| <input type="checkbox"/> 100 | Voice       | Disabled           | Disabled          | Tagged   | Tagged   | Tagged   | Tagged   | Tagged   | Tagged   |

Add Edit Delete

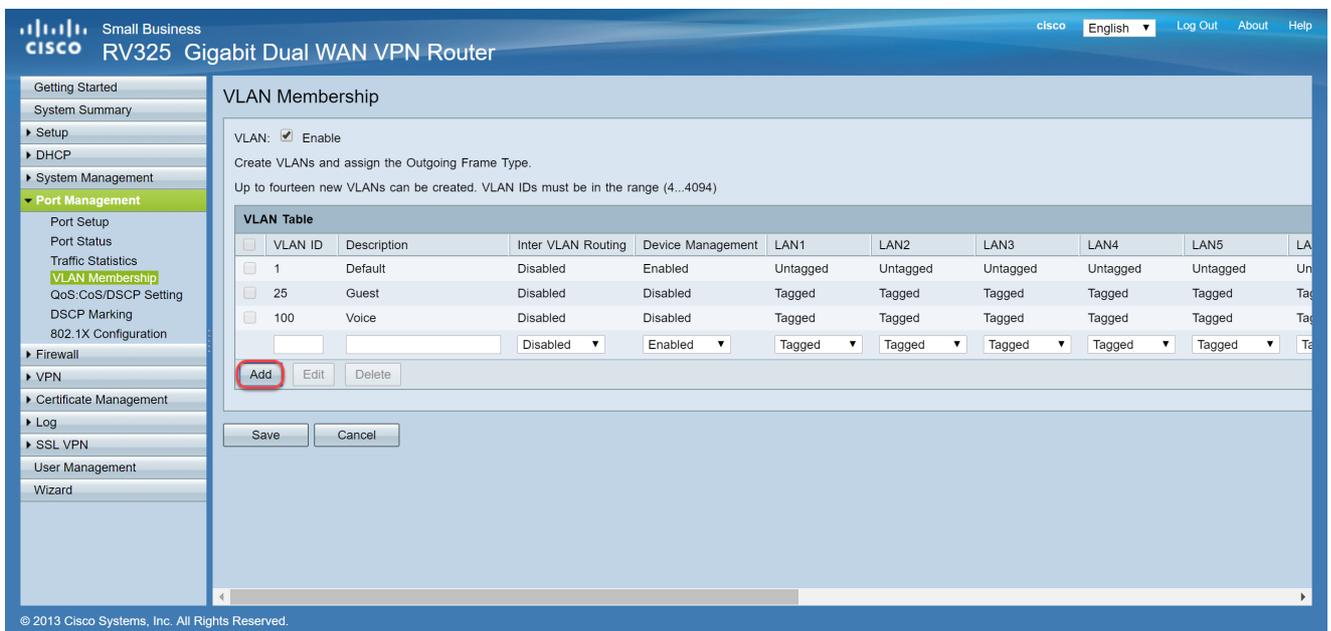
Save Cancel

© 2013 Cisco Systems, Inc. All Rights Reserved.

Paso 2. Marque la casilla de verificación Enable para habilitar la VLAN en el router.

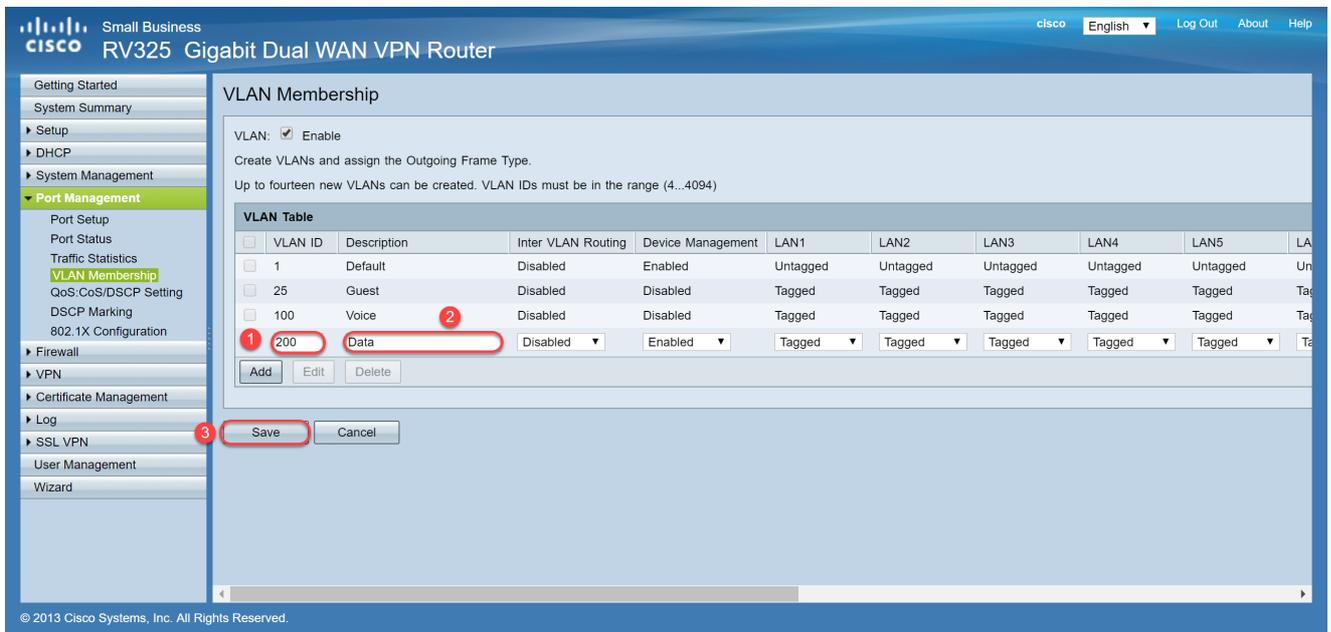


Paso 3. En la sección VLAN Table, haga clic en Add para crear un nuevo ID de VLAN.



Paso 4. Ingrese un número de VLAN en el campo VLAN ID. Los ID de VLAN deben estar en el rango de 4 a 4094. En este ejemplo, 200 se utiliza para datos como ID de VLAN. A continuación, introduzca una descripción para la VLAN en el campo Description. Los datos se introducen como ejemplo para la descripción. A continuación, haga clic en Guardar.

Nota: VLAN 100 para voz se creó de forma predeterminada en este router. Se pueden crear hasta catorce nuevas VLAN.



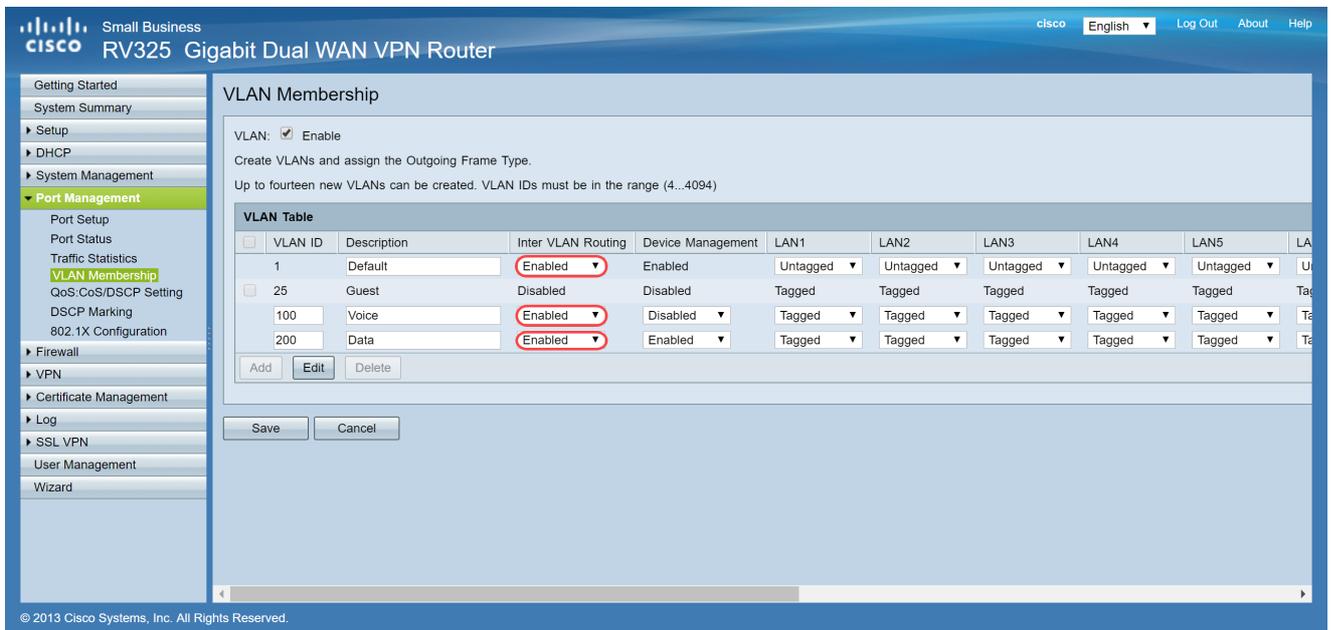
Paso 5. Para editar una VLAN, marque la casilla de verificación de la VLAN correspondiente. En este ejemplo, se editarán las VLAN 1, 100 y 200. A continuación, haga clic en Edit para editar las VLAN.



Paso 6. (Opcional) En la lista desplegable Inter VLAN Routing, elija Enabled o Disabled para rutear paquetes de una VLAN a otra VLAN. Esta opción es útil porque los administradores de red internos podrán acceder de forma remota a sus dispositivos para ayudar a solucionar sus problemas. Esto reducirá el tiempo de tener que cambiar constantemente las VLAN para acceder a los dispositivos.

- Deshabilitado: representa que el ruteo entre VLAN está inactivo
- Habilitado: representa que el ruteo entre VLAN está activo en esta VLAN. El ruteo entre VLAN enruta los paquetes solamente entre las VLAN que lo tienen habilitado.

Nota: En este ejemplo, habilitaremos el ruteo Inter VLAN para los ID de VLAN 1, 100 y 200.



Paso 7. Elija la opción que desee en la lista desplegable del puerto LAN al que está conectado y la configuración debe coincidir con el puerto conectado. Si está conectado con más de un puerto, debe seleccionar los mismos parámetros para cada puerto que esté conectado. El valor predeterminado es etiquetado, pero para la VLAN 1 no es etiquetado.

Nota: Si habilita el ruteo entre VLAN en el Paso 6, debe etiquetar la VLAN para distinguir el tráfico.

etiquetado

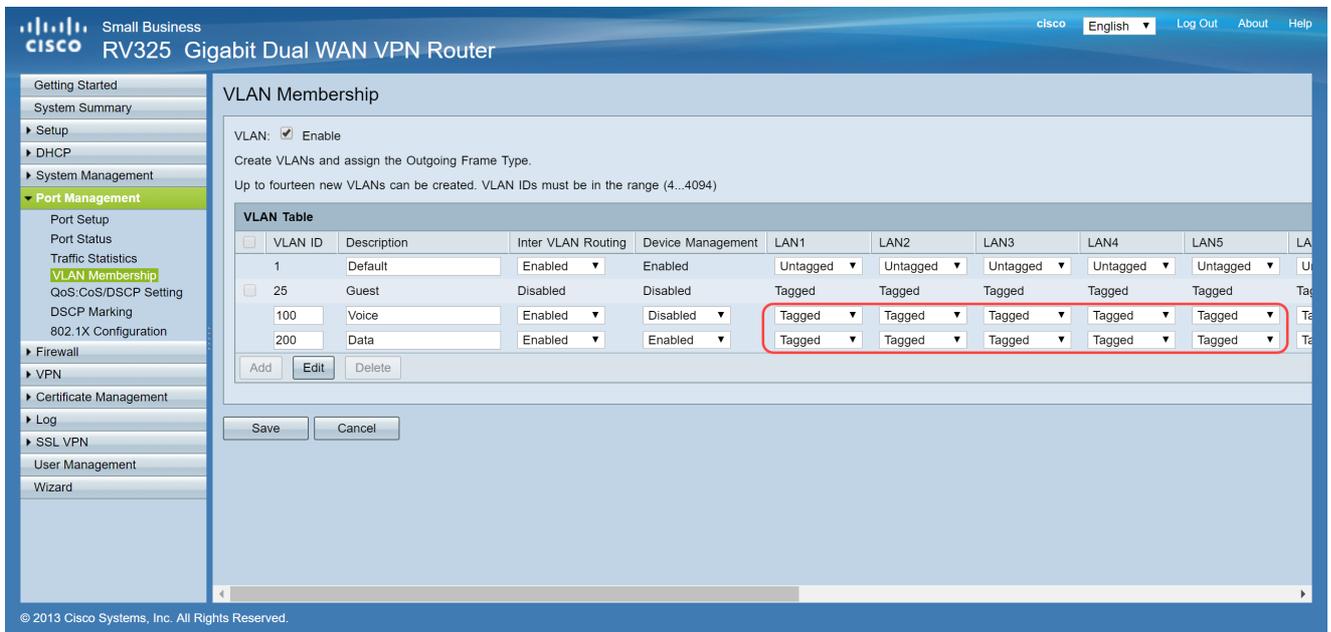
- Representa que la asociación entre el puerto y la VLAN está etiquetada.
- El etiquetado se utiliza para determinar a qué VLAN pertenece el tráfico a través del ID de VLAN único cuando se crean varias VLAN para el mismo puerto.

Sin etiquetas

- Representa que la asociación entre el puerto y la VLAN no está etiquetado.
- Se utiliza cuando sólo se crea una VLAN y el tráfico es consciente de la VLAN. Solo una VLAN se puede marcar como no etiquetada para cada puerto LAN.
- Si la VLAN predeterminada está en el puerto, siempre debe estar sin etiqueta incluso si el puerto tiene varias VLAN.

Excluido

- Representa que la interfaz no es un miembro de la VLAN.
- Si elige esta opción, el tráfico se inhabilita entre la VLAN y el puerto.



Paso 8. Haga clic en Guardar para guardar la configuración.

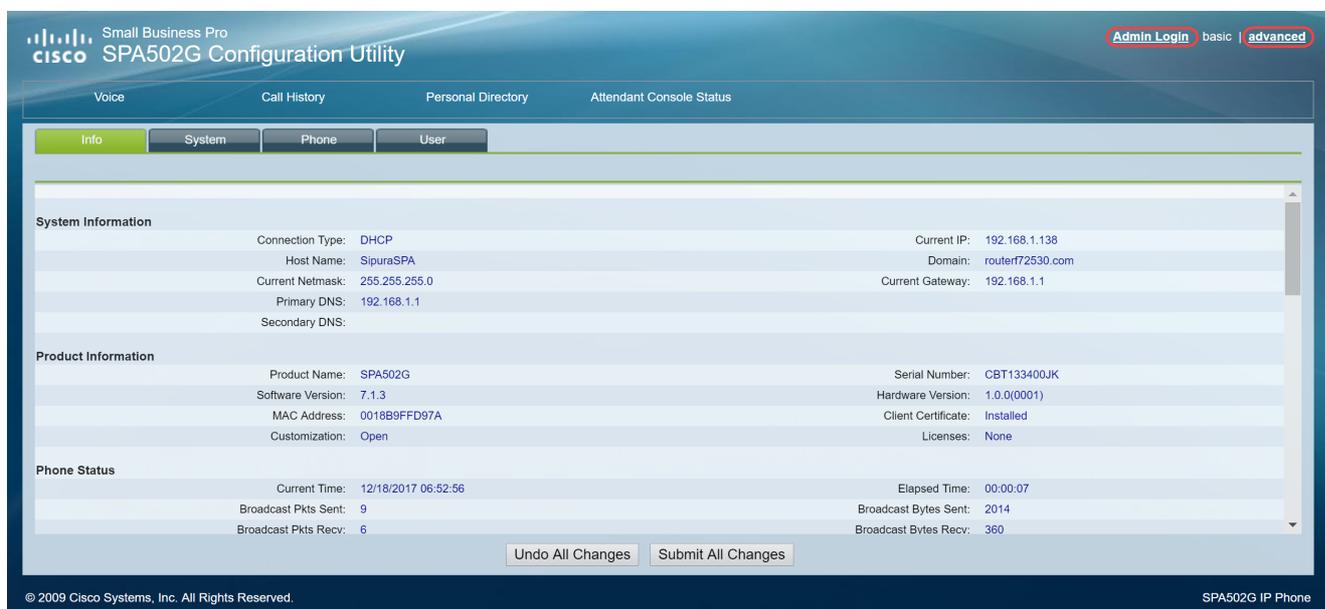
Nota: En el router, puede iniciar sesión en la utilidad basada en web y navegar hasta DHCP > DHCP Setup para configurar las VLAN en una subred específica que desee. De forma predeterminada, las VLAN están configuradas para estar en una subred diferente.

## Configuración de teléfonos SPA/MPP

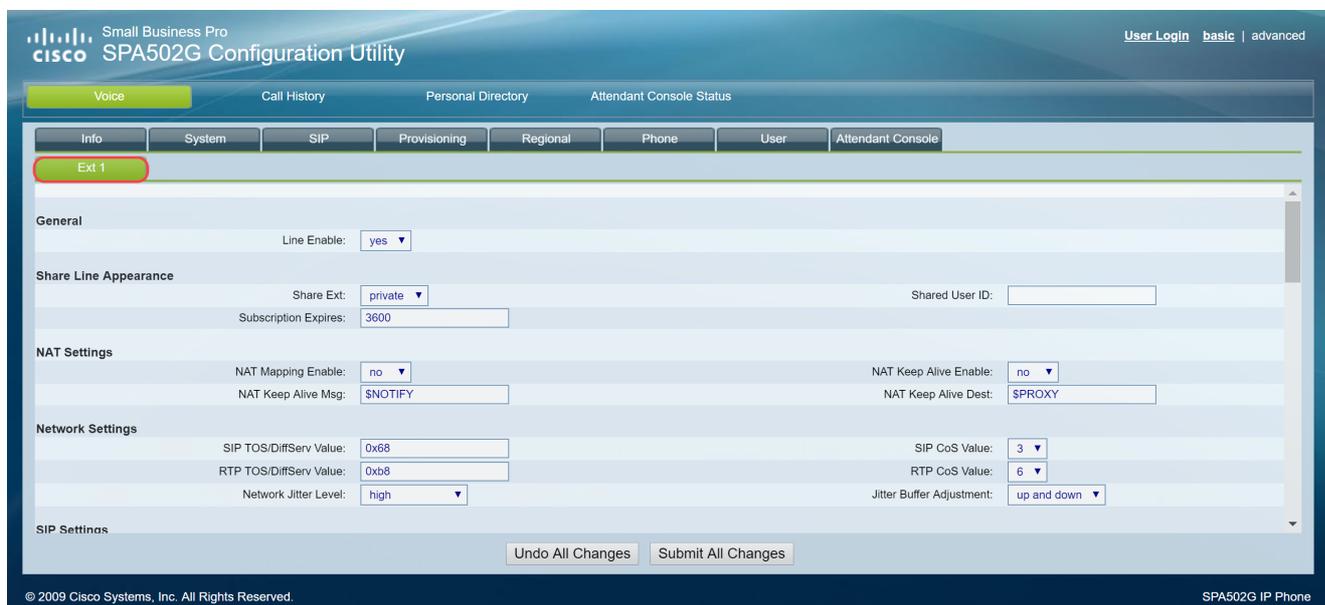
Los usuarios también pueden configurar los teléfonos para extraer un perfil desde una ubicación de perfil configurada manualmente, una ubicación encontrada mediante la opción DHCP 150 o desde un servidor EDOS de Cisco. A continuación se muestra un ejemplo de una configuración manual.

Paso 1. Introduzca la dirección IP del SPA/MPP en el navegador, vaya a Admin Login y, a continuación, a advanced.

Nota: La configuración del teléfono SPA/MPP puede variar en función del modelo. En este ejemplo, estamos utilizando el SPA502G. Para buscar la dirección IP del teléfono IP, vaya a DHCP > DHCP Status en el router (puede variar según el modelo). Otra forma consiste en pulsar el botón Setup y navegar hasta Network en el teléfono Cisco (los menús y las opciones pueden variar según el modelo de teléfono).



Paso 2. Navegue hasta Voz > Extensión 1, se abre la página de extensión.



Paso 3. En la sección Proxy y Registro, escriba el servidor proxy en el campo Proxy. En este ejemplo, se utilizará la dirección de Raspberry Pi (192.168.3.10) como servidor proxy. VLAN 100 está en la subred con 192.168.3.x.

Nota: Configuraré la dirección IP del Raspberry Pi más adelante en este artículo, si desea obtener más información, haga clic en el enlace que se redirigirá a esa sección: [Cambiar la dirección del Raspberry Pi para que esté en una subred diferente.](#)

The screenshot shows the Cisco SPA502G Configuration Utility interface. The 'Proxy and Registration' section is active, and the 'Proxy' field is highlighted with a red box, containing the value '192.168.3.10'. Other fields in this section include 'Outbound Proxy', 'Register' (set to 'yes'), 'Register Expires' (3600), 'Use DNS SRV' (set to 'no'), 'Proxy Fallback Intvl' (3600), 'Use Outbound Proxy' (set to 'no'), 'Use OB Proxy In Dialog' (set to 'yes'), 'Make Call Without Reg.' (set to 'no'), 'Ans Call Without Reg.' (set to 'no'), 'DNS SRV Auto Prefix' (set to 'no'), and 'Proxy Redundancy Method' (set to 'Normal'). The 'Subscriber Information' section is also visible, with fields for 'Display Name', 'Password', 'Auth ID', 'Mini Certificate', 'SRTP Private Key', 'User ID', and 'Use Auth ID' (set to 'no'). At the bottom, there are buttons for 'Undo All Changes' and 'Submit All Changes'.

Paso 4. En Subscriber Information, introduzca el nombre para mostrar y el ID de usuario (número de extensión) de la extensión compartida. En este ejemplo, utilizaremos la extensión 1003.

Nota: La extensión 1003 ya se ha creado y configurado en Raspberry Pi.

The screenshot shows the Cisco SPA502G Configuration Utility interface. The 'Subscriber Information' section is active, and the 'Display Name' and 'User ID' fields are highlighted with red boxes, both containing the value '1003'. Other fields in this section include 'Password', 'Auth ID', 'Mini Certificate', 'SRTP Private Key', and 'Use Auth ID' (set to 'no'). The 'Audio Configuration' section is also visible, with fields for 'Preferred Codec' (set to 'G711u'), 'Second Preferred Codec' (set to 'Unspecified'), 'Third Preferred Codec' (set to 'Unspecified'), and several 'G72x' enable options (G729a, G726-16, G726-32, G722, G726-24, G726-40) all set to 'yes'. At the bottom, there are buttons for 'Undo All Changes' and 'Submit All Changes'.

Paso 5. Introduzca la contraseña de la extensión que ha configurado en la sección Extensión de Raspberry Pi. Esto también se conoce como Secreto en la sección Editar extensión en el Raspberry Pi. En este ejemplo, se utilizó la contraseña 12345.

Nota: La contraseña 12345 sólo se utilizó como ejemplo; se recomienda una contraseña más compleja.

The screenshot shows the Cisco SPA502G Configuration Utility interface. The 'User' tab is selected, and the configuration is for 'Ext 1'. The 'Subscriber Information' section contains the following fields:

|                   |       |              |      |
|-------------------|-------|--------------|------|
| Display Name:     | 1003  | User ID:     | 1003 |
| Password:         | 12345 | Use Auth ID: | no   |
| Auth ID:          |       |              |      |
| Mini Certificate: |       |              |      |
| SRTP Private Key: |       |              |      |

The 'Audio Configuration' section includes:

|                         |             |                        |             |
|-------------------------|-------------|------------------------|-------------|
| Preferred Codec:        | G711u       | Use Pref Codec Only:   | no          |
| Second Preferred Codec: | Unspecified | Third Preferred Codec: | Unspecified |
| G729a Enable:           | yes         | G722 Enable:           | yes         |
| G726-16 Enable:         | yes         | G726-24 Enable:        | yes         |
| G726-32 Enable:         | yes         | G726-40 Enable:        | yes         |

Buttons at the bottom: 'Undo All Changes' and 'Submit All Changes'. Copyright: © 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone.

Paso 6. Elija la opción deseada de la lista desplegable Use Auth ID. Las opciones son Yes y No. Para habilitar la autenticación del protocolo de inicio de sesión (SIP), donde los mensajes SIP se pueden desafiar para determinar si están autorizados antes de que puedan transmitir, elija Yes en la lista desplegable Auth ID. En este ejemplo, elegimos Yes.

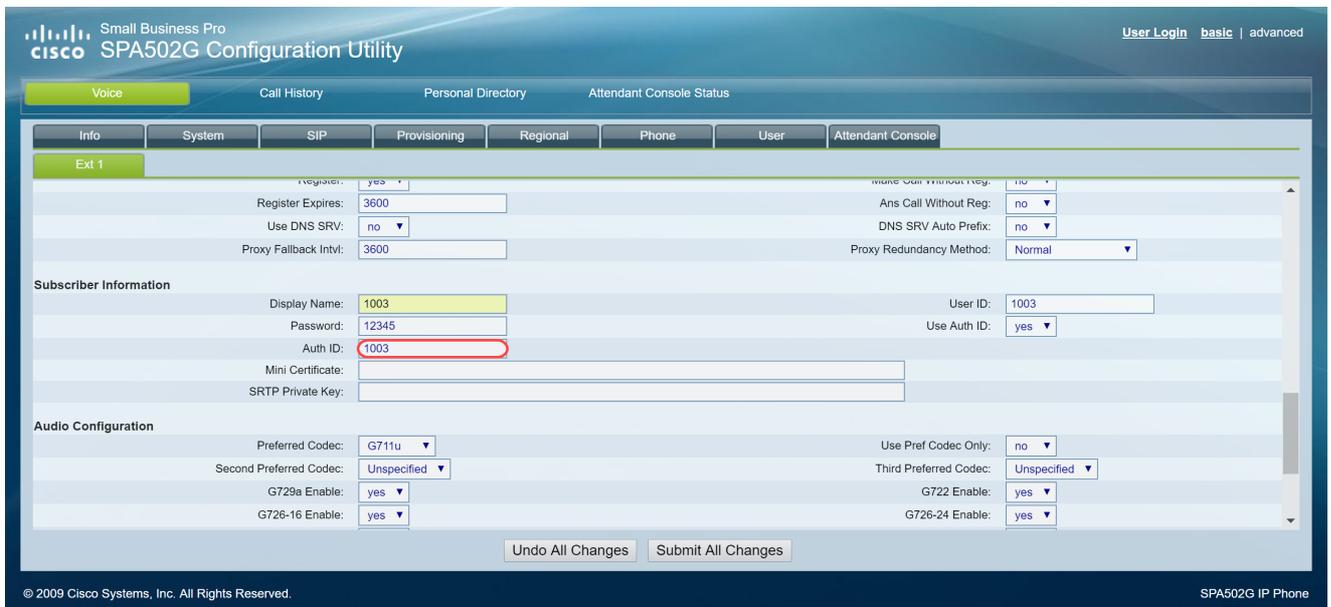
The screenshot shows the same Cisco SPA502G Configuration Utility interface as the previous one. In the 'Subscriber Information' section, the 'Use Auth ID' dropdown menu is now set to 'yes' and is highlighted with a red circle.

|                   |       |              |      |
|-------------------|-------|--------------|------|
| Display Name:     | 1003  | User ID:     | 1003 |
| Password:         | 12345 | Use Auth ID: | yes  |
| Auth ID:          |       |              |      |
| Mini Certificate: |       |              |      |
| SRTP Private Key: |       |              |      |

The 'Audio Configuration' section remains the same as in the previous screenshot.

Buttons at the bottom: 'Undo All Changes' and 'Submit All Changes'. Copyright: © 2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone.

Paso 7. Ingrese la extensión que intenta configurar para este teléfono en el campo Auth ID. El ID de autenticación es para la autenticación SIP.



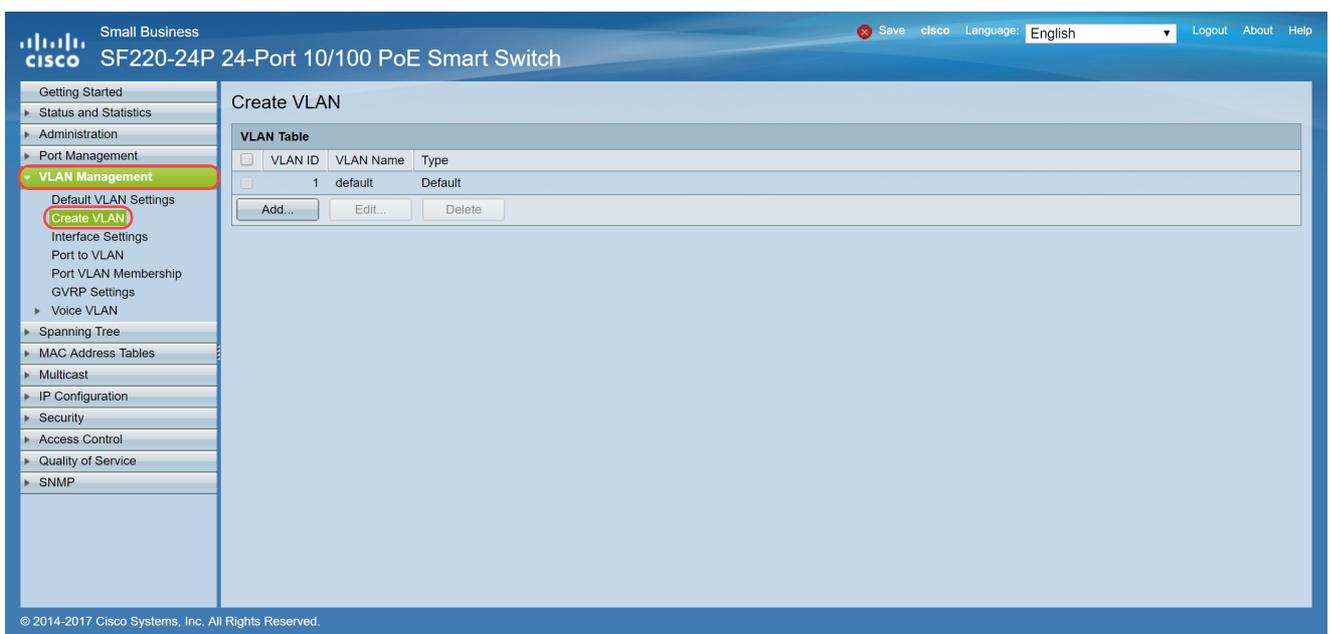
Paso 8. A continuación, haga clic en Enviar todos los cambios.

Nota: Vuelva al paso 1 de la sección Configuración de teléfonos SPA/MPP si tiene más teléfonos SPA/MPP que configurar.

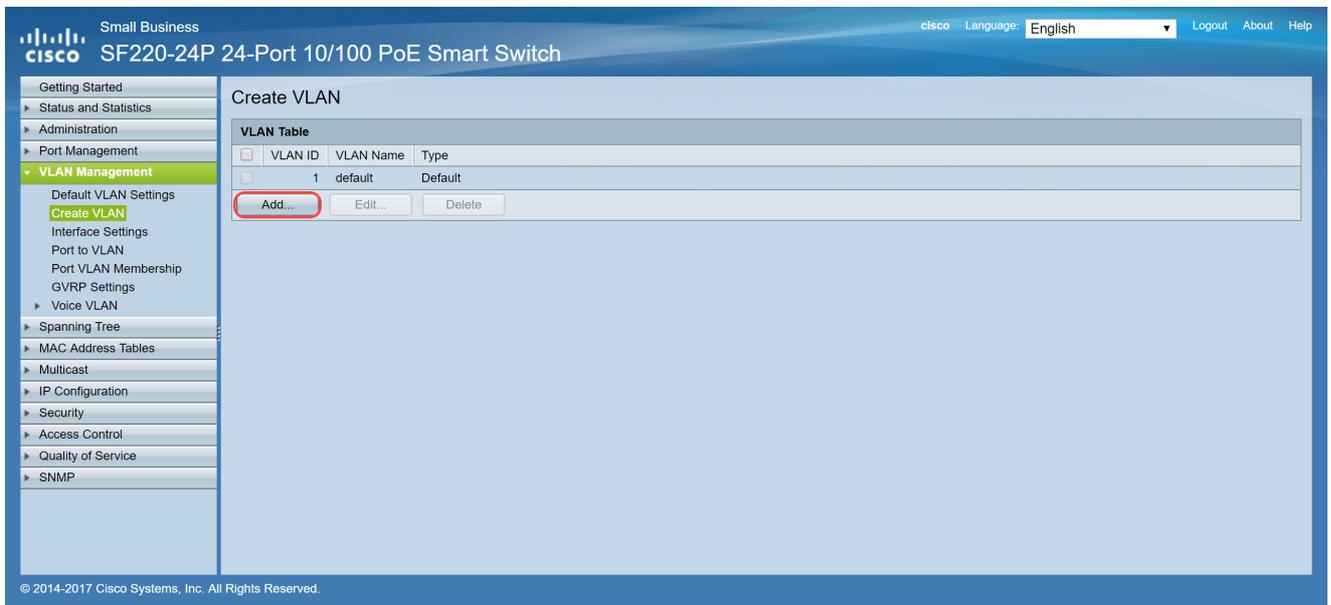
## Configuración de VLAN en el switch

Paso 1. Inicie sesión en la utilidad basada en web y navegue hasta VLAN Management > Create VLAN.

Nota: La configuración puede variar en función del dispositivo. En este ejemplo, estamos utilizando el SF220-24P para configurar las VLAN.

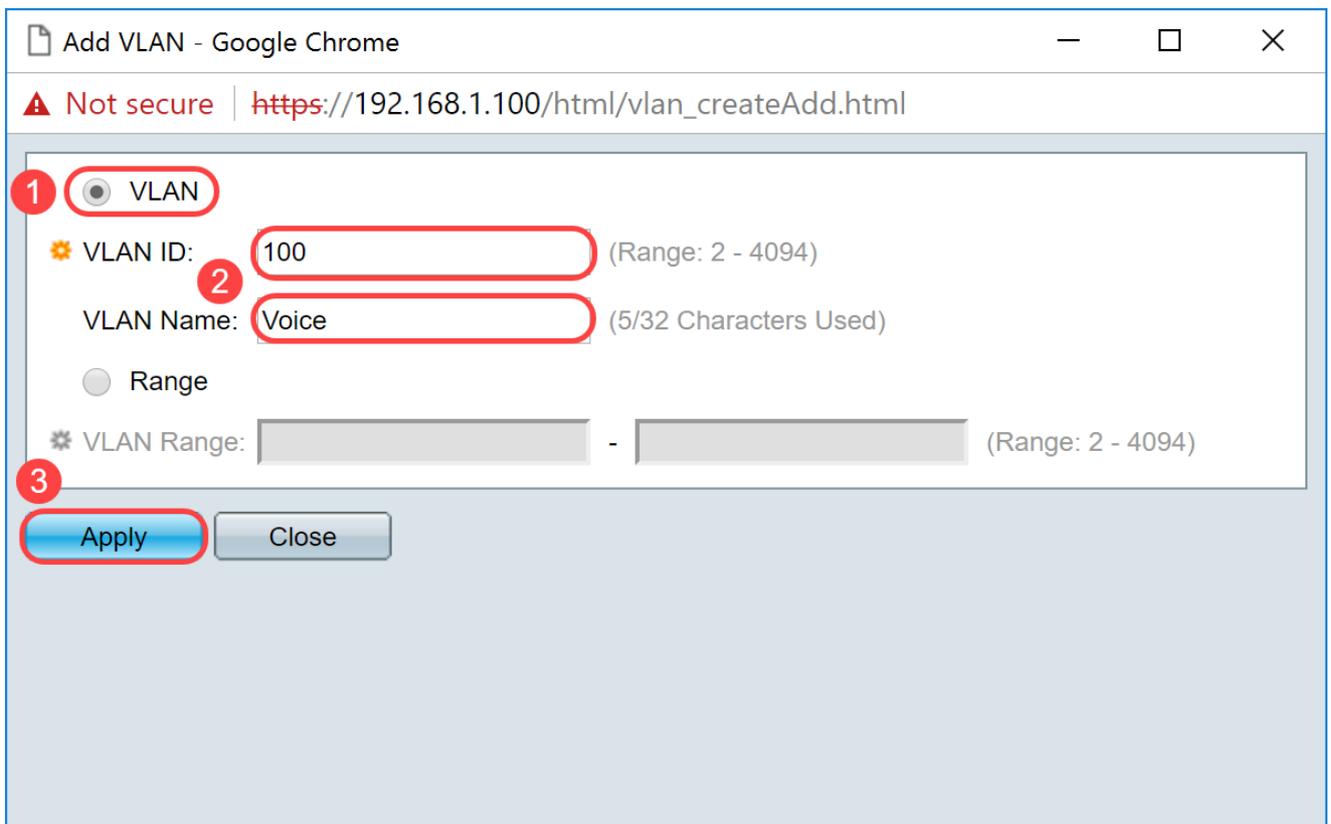


Paso 2. Haga clic en Add... para crear una nueva VLAN.



Paso 3. Para crear una única VLAN, seleccione el botón de opción VLAN. Ingrese el ID de VLAN y el nombre de VLAN. A continuación, haga clic en Apply para guardar la VLAN. En este ejemplo, crearemos VLAN 100 para voz y 200 para datos.

Nota: El sistema requiere algunas VLAN para el uso interno del sistema y, por lo tanto, no se pueden crear introduciendo el VID inicial y el VID final, ambos incluidos. Al utilizar la función Range, el número máximo de VLAN que puede crear a la vez es 100.

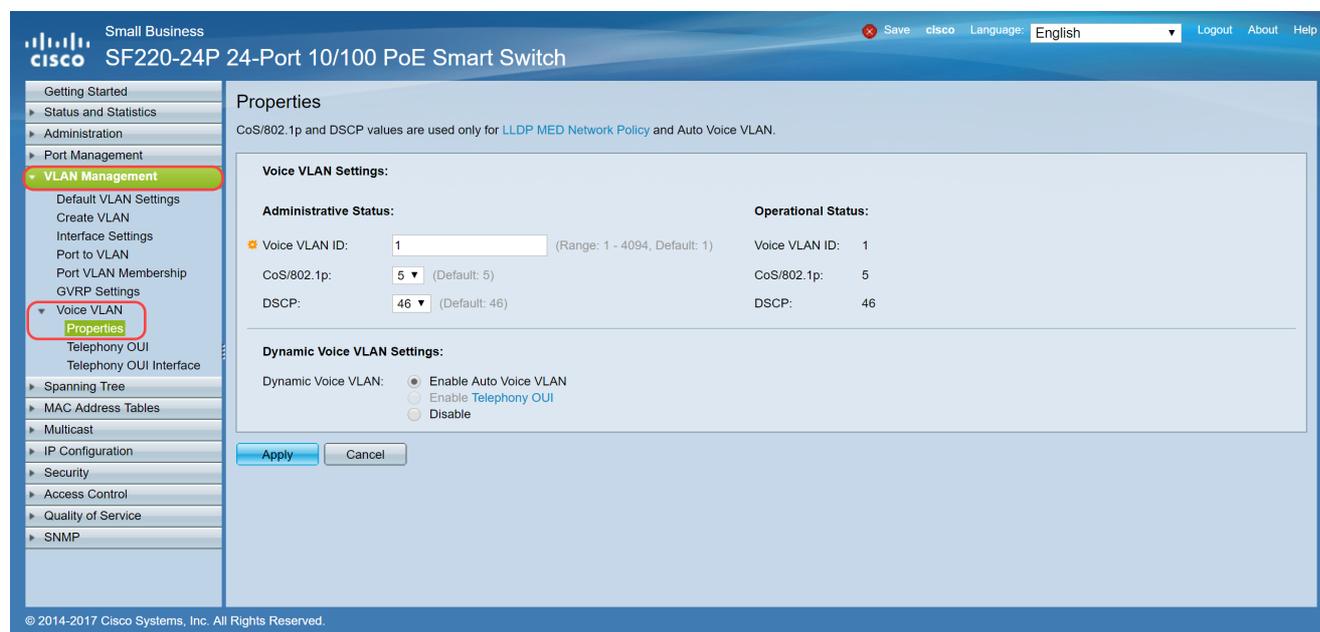


Nota: Repita el paso 2 si necesita crear otra VLAN única.

## Configuración de la VLAN de voz en el switch

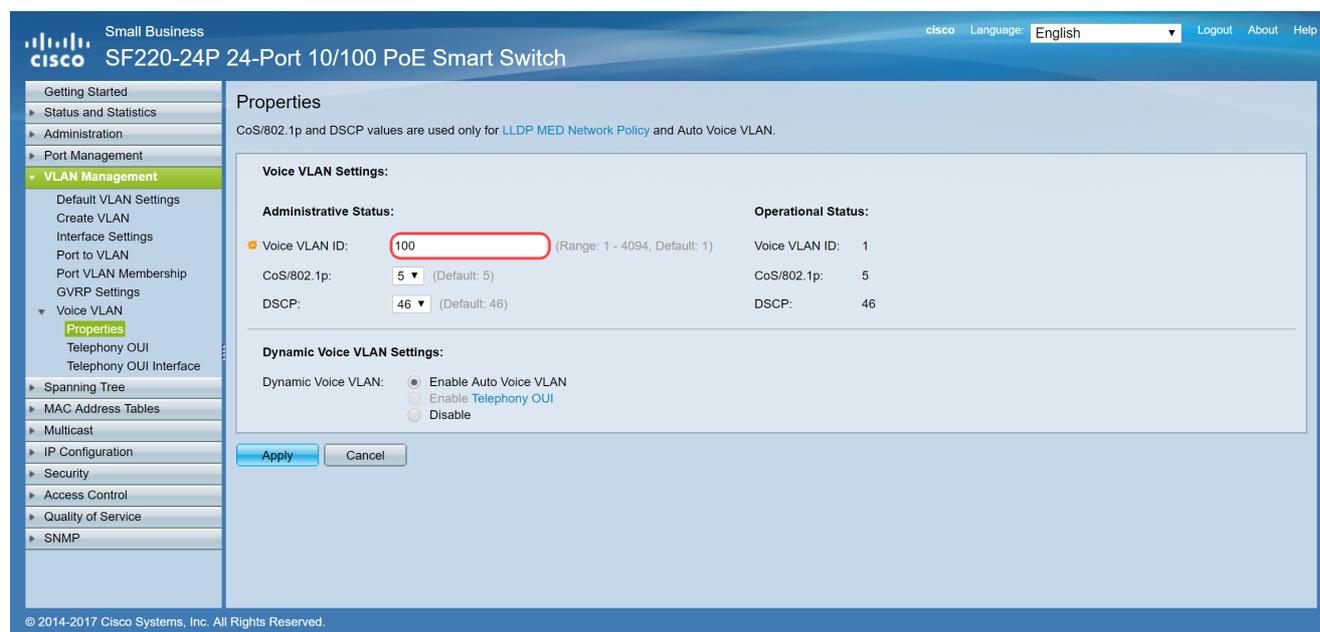
Paso 1. Inicie sesión en la configuración web y navegue hasta VLAN Management > Voice VLAN > Properties.

Nota: La configuración de la VLAN de voz automática aplicará automáticamente la configuración de QoS para la VLAN de voz y dará prioridad al tráfico de voz.

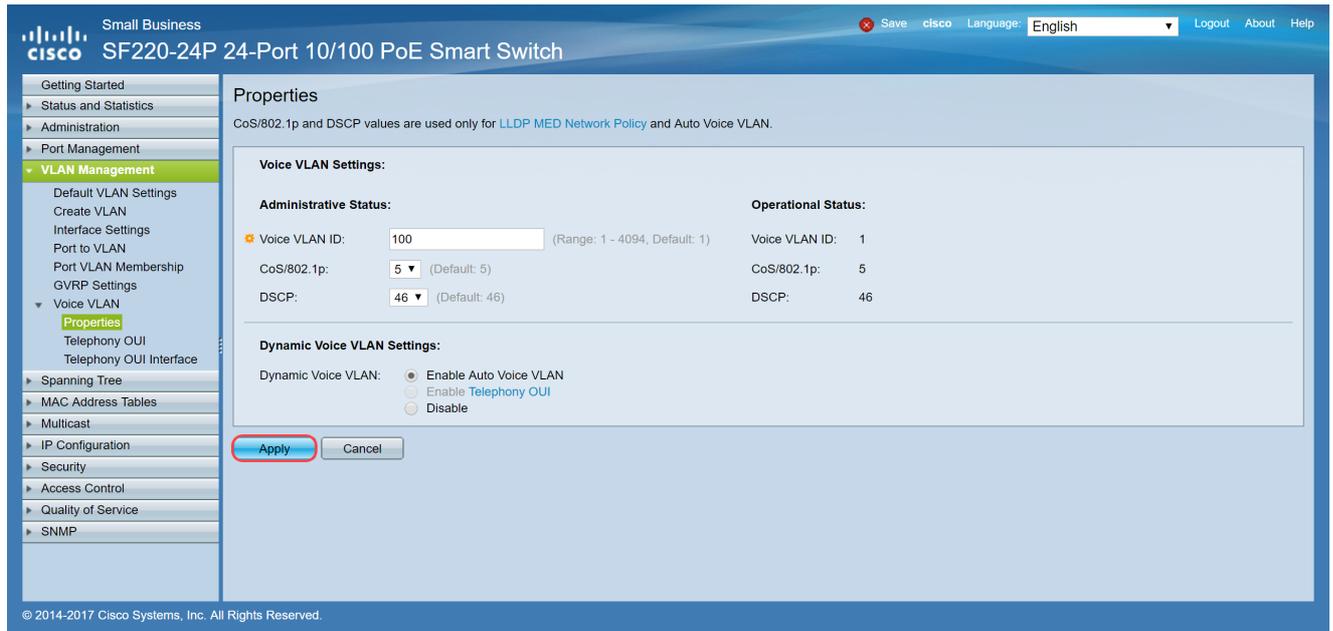


Paso 2. En Estado administrativo, ingrese la VLAN que debe ser la VLAN de voz en el campo ID de VLAN de voz. En este ejemplo, se ingresa la VLAN 100 como la VLAN de voz.

Nota: Los cambios en el ID de VLAN de voz, la clase de servicio (CoS)/802.1p y/o el punto de código de servicio diferenciado (DSCP) hacen que el dispositivo anuncie la VLAN de voz administrativa como una VLAN de voz estática. Si se selecciona la opción Activación automática de VLAN de voz activada por VLAN de voz externa, se deben mantener los valores predeterminados. En este ejemplo, CoS/802.1p se deja como valor predeterminado de 5 y DSCP se deja como valor predeterminado de 46.



Paso 3. Haga clic en Apply para guardar la configuración.



## Configuración de los parámetros de la interfaz en el switch

Las interfaces, los puertos físicos en el switch, se pueden asignar a una de las siguientes configuraciones:

- **General:** el puerto admite todas las funciones definidas en la especificación IEEE 802.1q. La interfaz puede ser un miembro etiquetado o no etiquetado de una o más VLAN.
- **Acceso:** solo puede tener una VLAN configurada en la interfaz y solo puede llevar una VLAN.
- **Troncal:** puede transportar el tráfico de varias VLAN a través de un único enlace y le permite extender las VLAN a través de la red.
- **Dot1p-Tunnel:** pone la interfaz en modo QinQ. Esto permite al usuario utilizar sus propias disposiciones de VLAN (PVID) en la red del proveedor. El switch estará en modo QinQ cuando tenga uno o más puertos de túnel dot1p.

Paso 1. Inicie sesión en la configuración web y navegue hasta 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 Showing 1-26 of 26 All per page

Filter: Interface Type equals to Port Go

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

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

Paso 2. Seleccione el modo de interfaz para la VLAN. En este ejemplo, configuraremos el Raspberry Pi (puerto: FE3) como puerto de acceso.

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

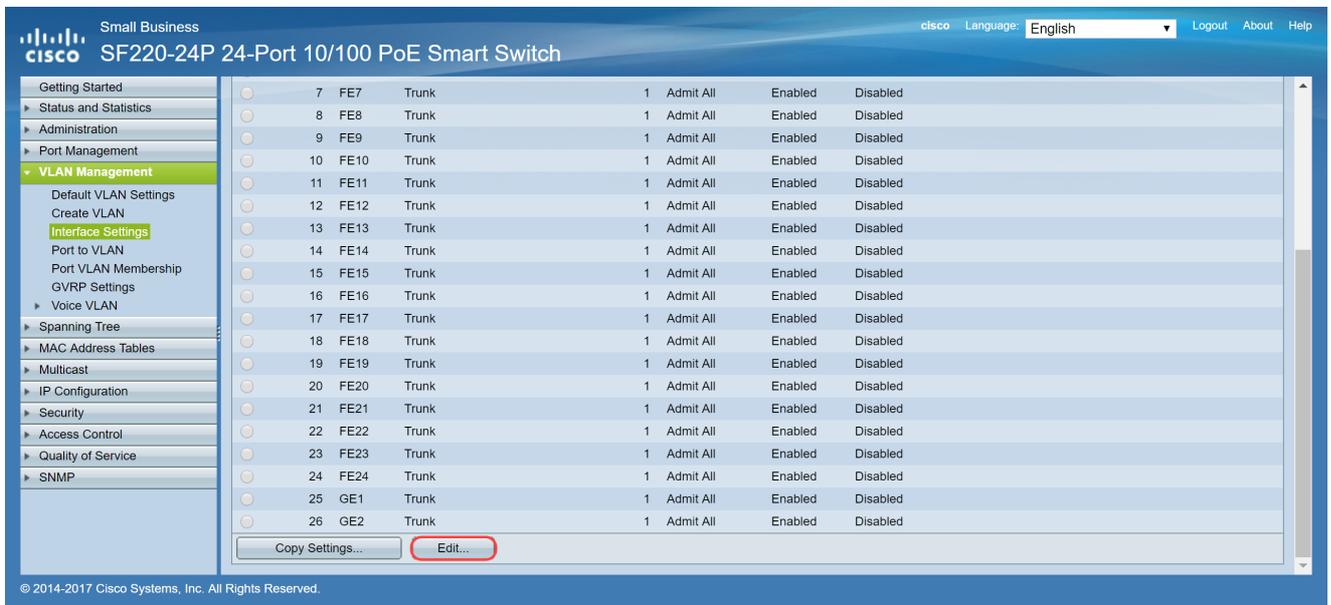
Interface Settings Table Showing 1-26 of 26 All per page

Filter: Interface Type equals to Port Go

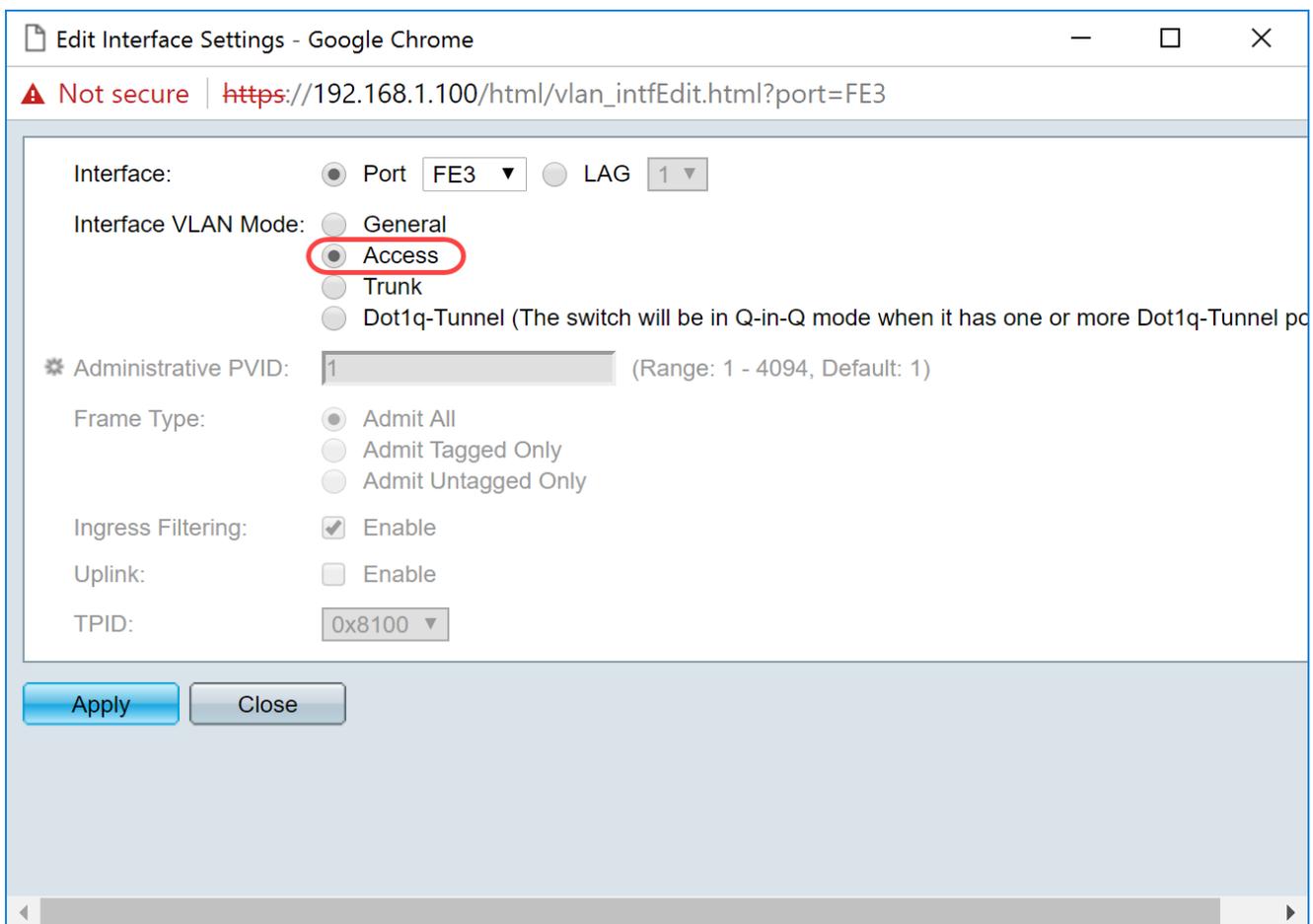
| Entry No.                        | Interface | Interface VLAN Mode | Administrative PVID | Frame Type | Ingress Filtering | Uplink   |
|----------------------------------|-----------|---------------------|---------------------|------------|-------------------|----------|
| <input type="radio"/>   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

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

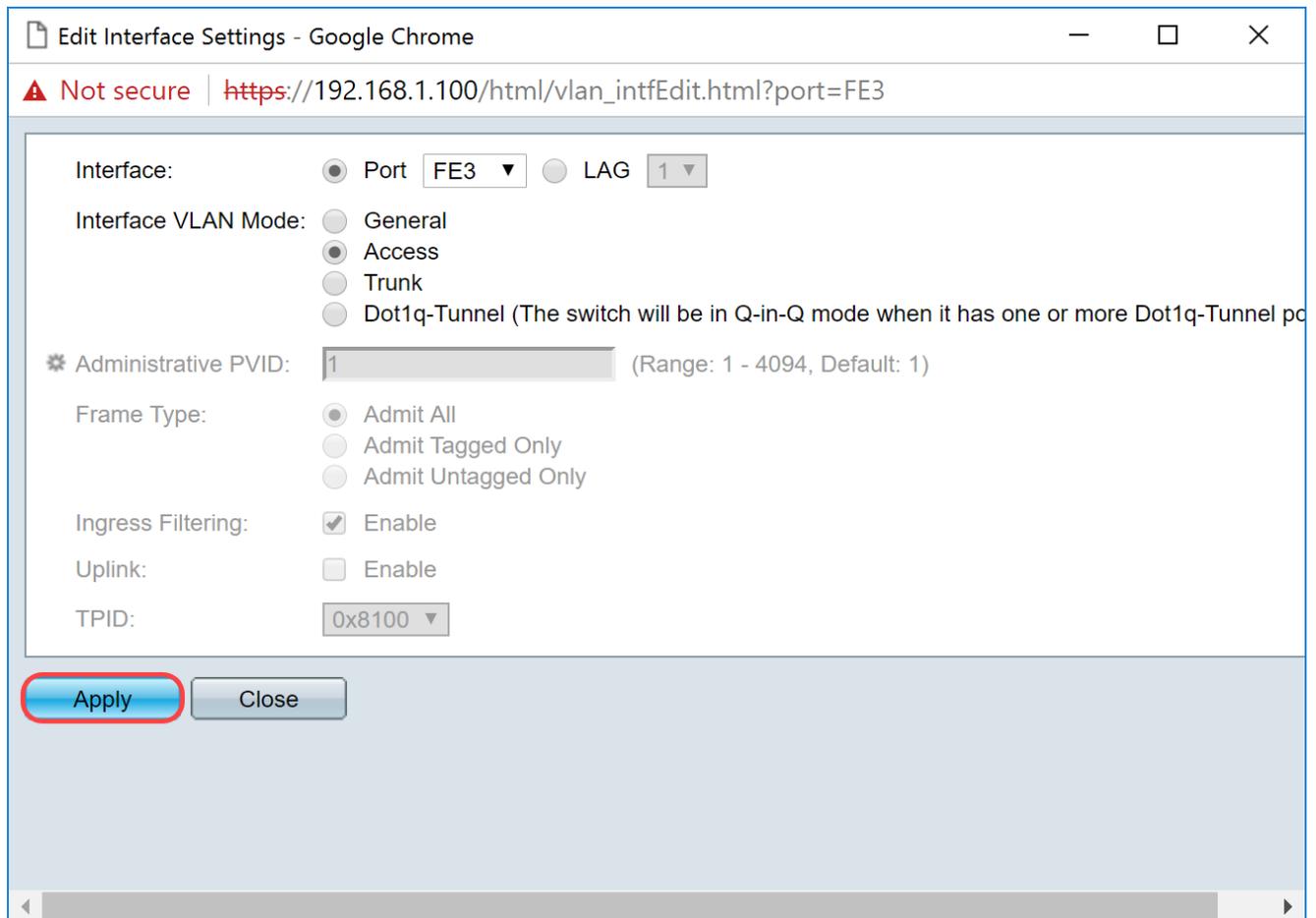
Paso 3. A continuación, haga clic en Edit... para editar la interfaz.



Paso 4. En el campo Interface VLAN Mode, elija Access para configurar la interfaz como un miembro sin etiqueta de una sola VLAN.



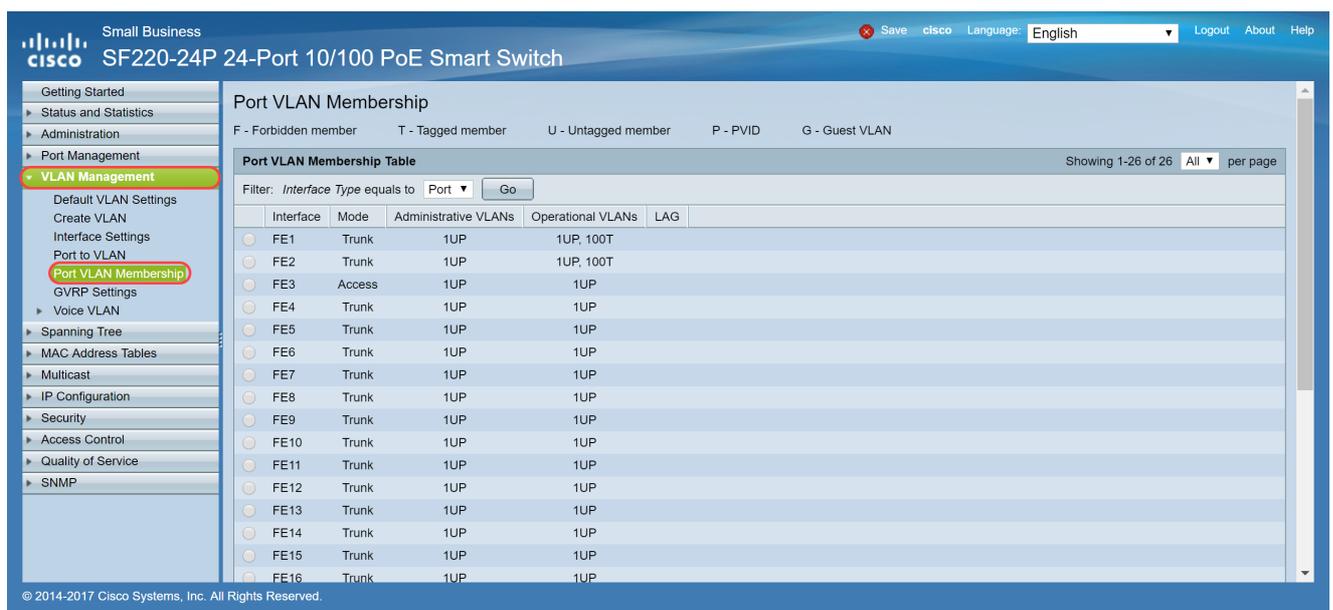
Paso 5. Haga clic en Apply para guardar la configuración.



## Configuración de la Pertenencia a VLAN de Puerto en el Switch

Una vez creadas las VLAN, debe asignar las VLAN a los puertos que desea conectar.

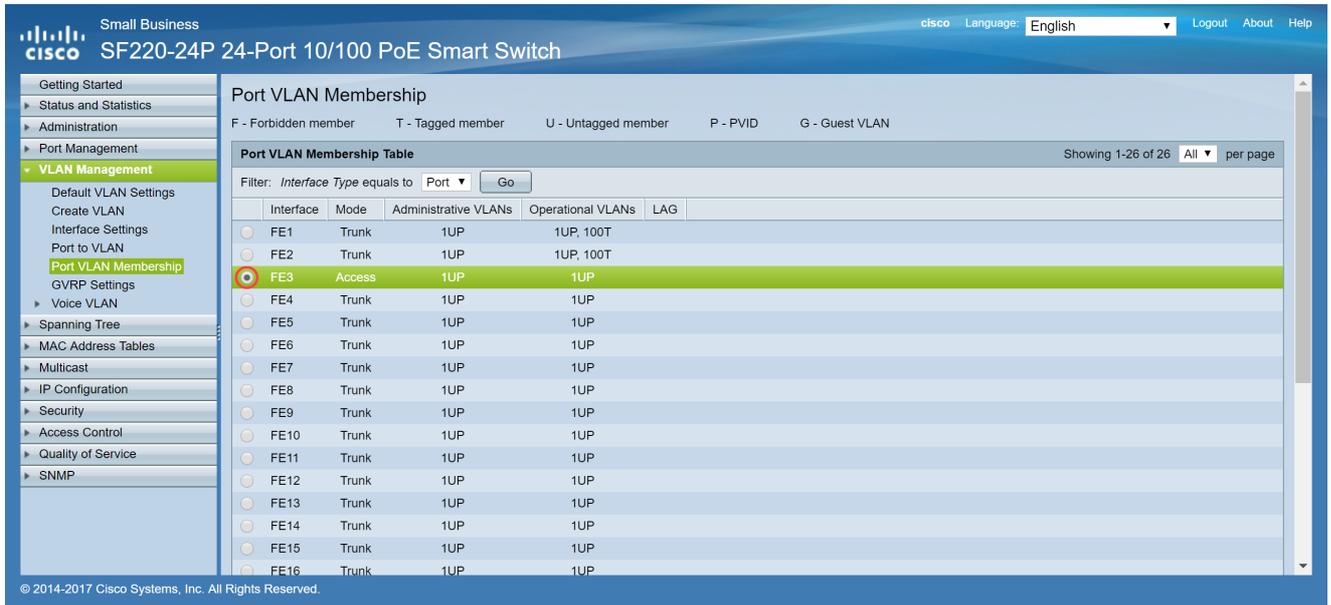
Paso 1. Inicie sesión en la configuración web y navegue hasta VLAN Management > Port VLAN Membership.



Paso 2. En Port VLAN Membership Table, seleccione la interfaz en la que desea configurar la pertenencia a VLAN. En este ejemplo, configuraremos Raspberry Pi (Puerto: FE3) para

que esté en VLAN 100.

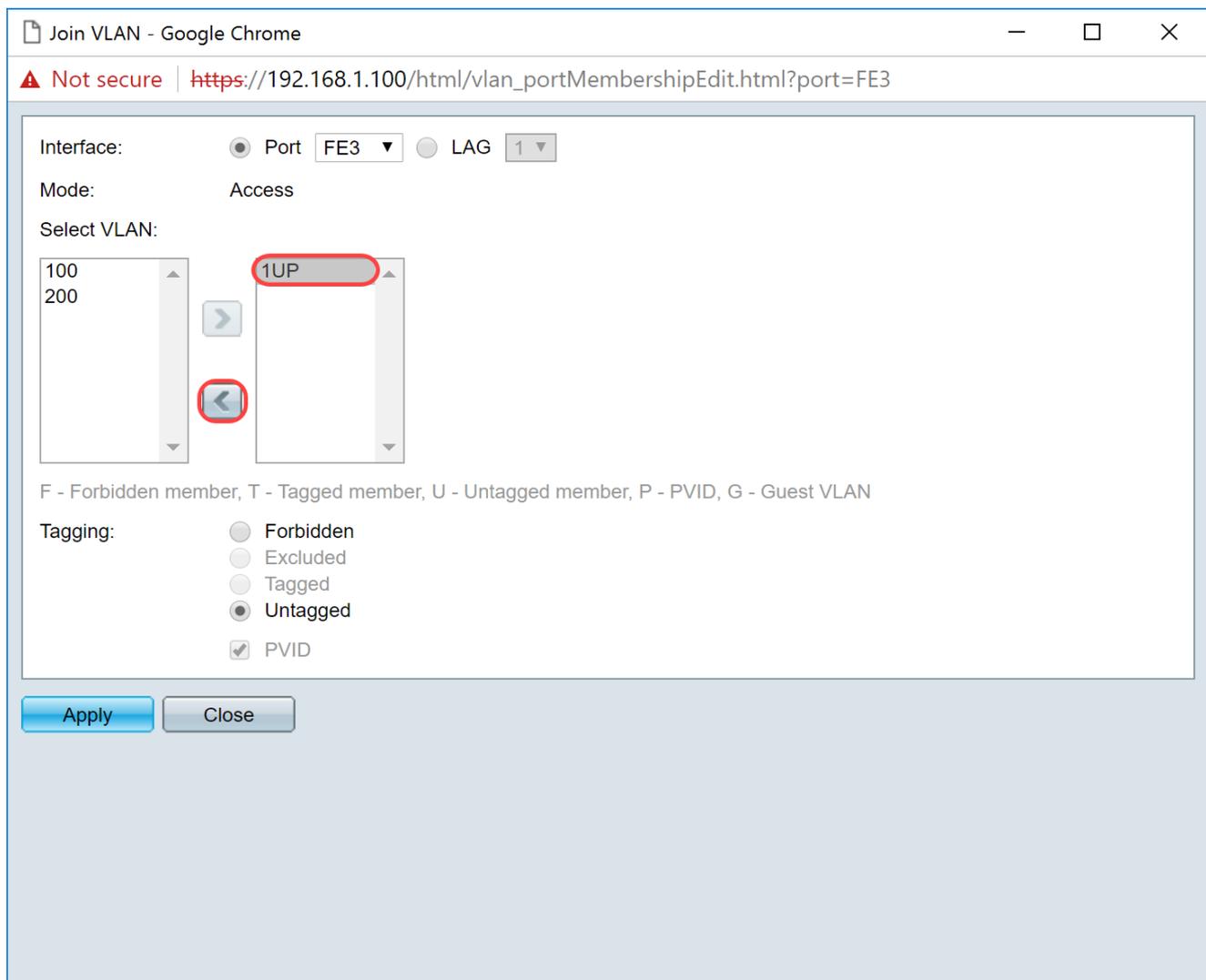
Nota: Cualquier dispositivo de voz ya se configurará en la VLAN de voz que haya seleccionado en la sección [Configuración de VLAN de voz en el switch](#).



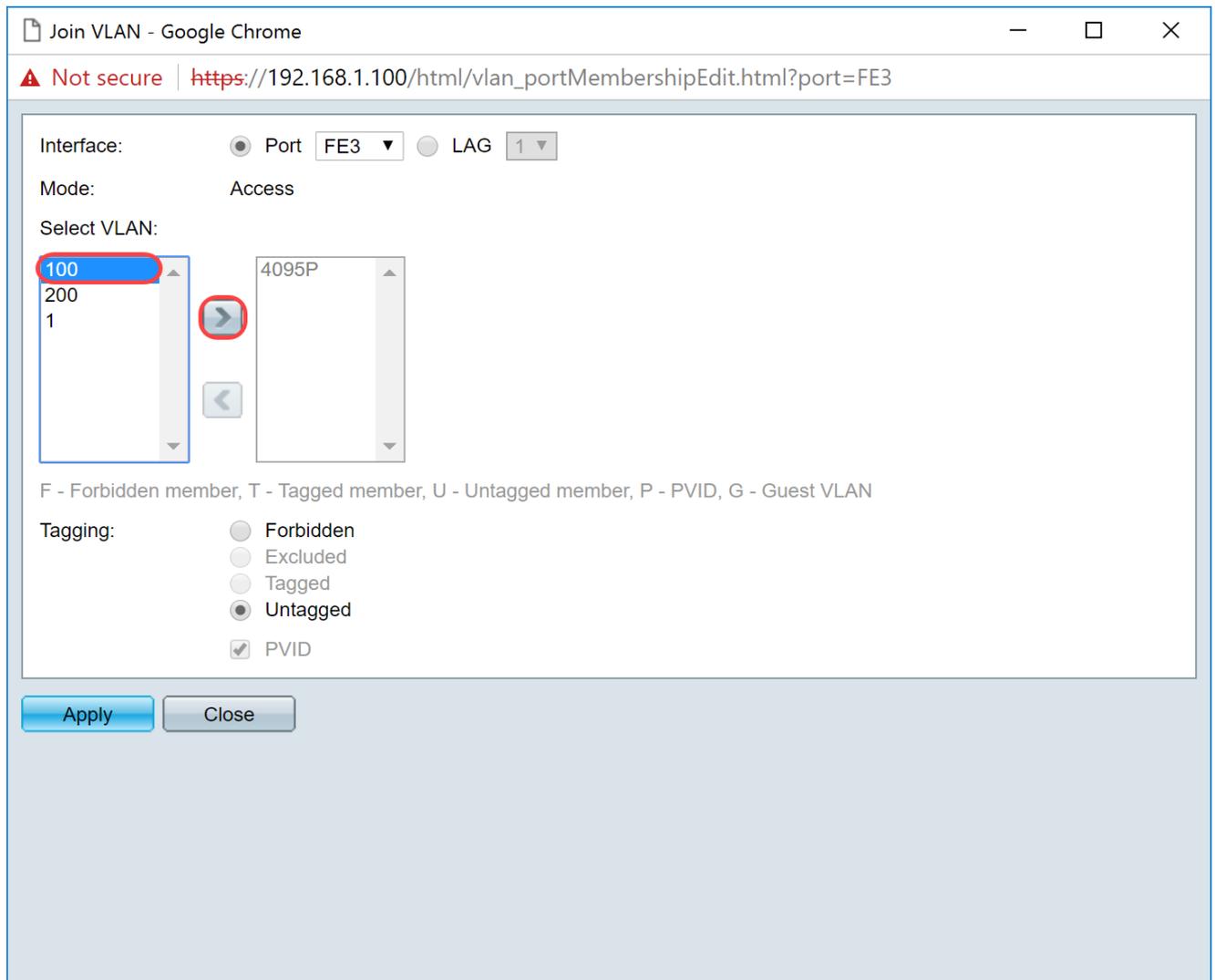
Paso 3. Haga clic en Join VLAN... para modificar el puerto que desea configurar las VLAN.



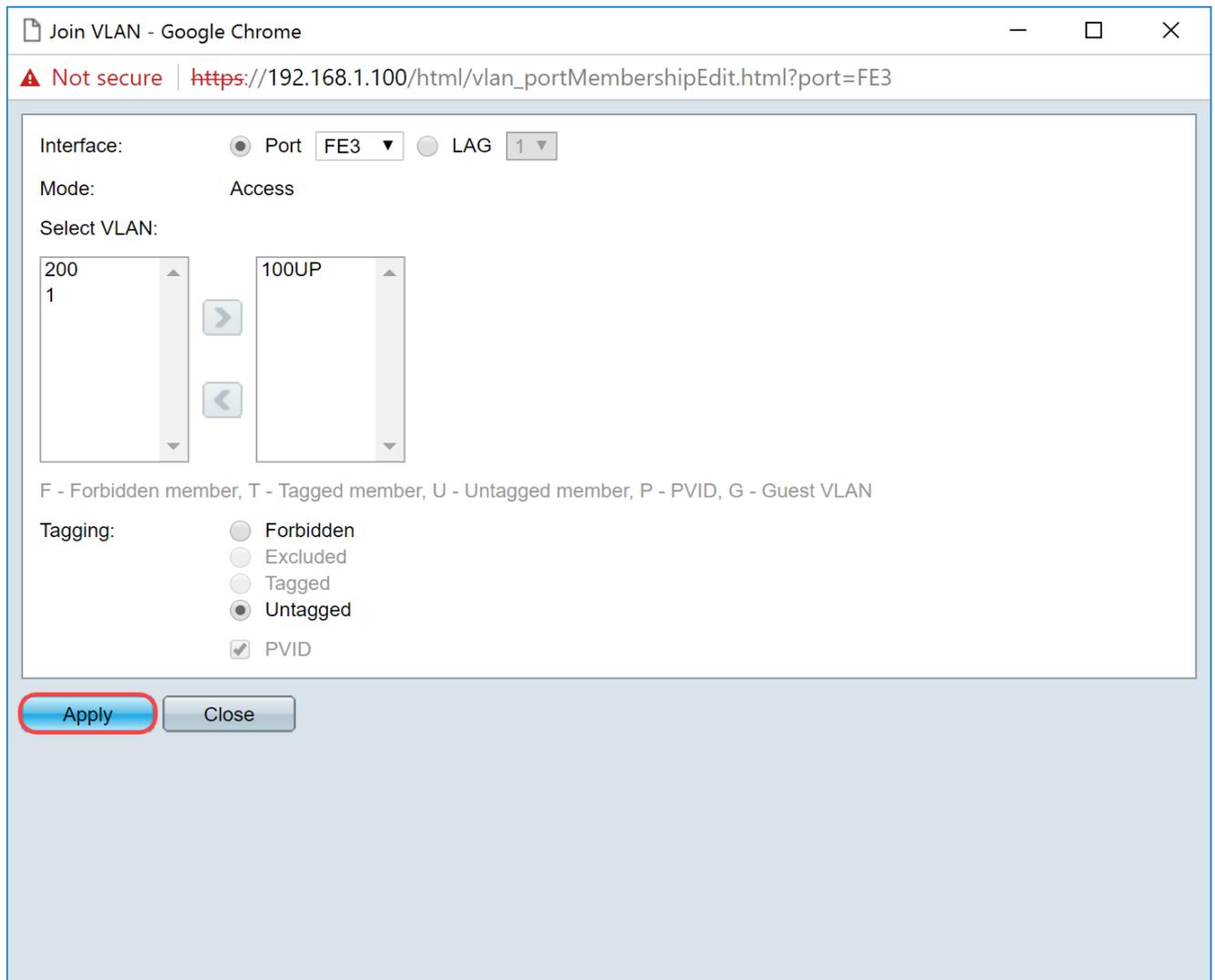
Paso 4. Seleccione 1UP y haga clic en < para quitar la VLAN 1 de la interfaz en la sección Select VLAN. Sólo se puede agregar 1 VLAN sin etiqueta a la interfaz cuando es un puerto de acceso.



Paso 5. Seleccione 100 y haga clic en > para agregar la VLAN sin etiqueta a la interfaz.



Paso 6. Haga clic en Apply para guardar la configuración.



Paso 7. Seleccione el puerto de interfaz que está conectado al router en el campo Interface. En este ejemplo, el puerto GE1 está seleccionado.

Join VLAN - Google Chrome

Not secure | [https://192.168.1.100/html/vlan\\_portMembershipEdit.html?port=FE3](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

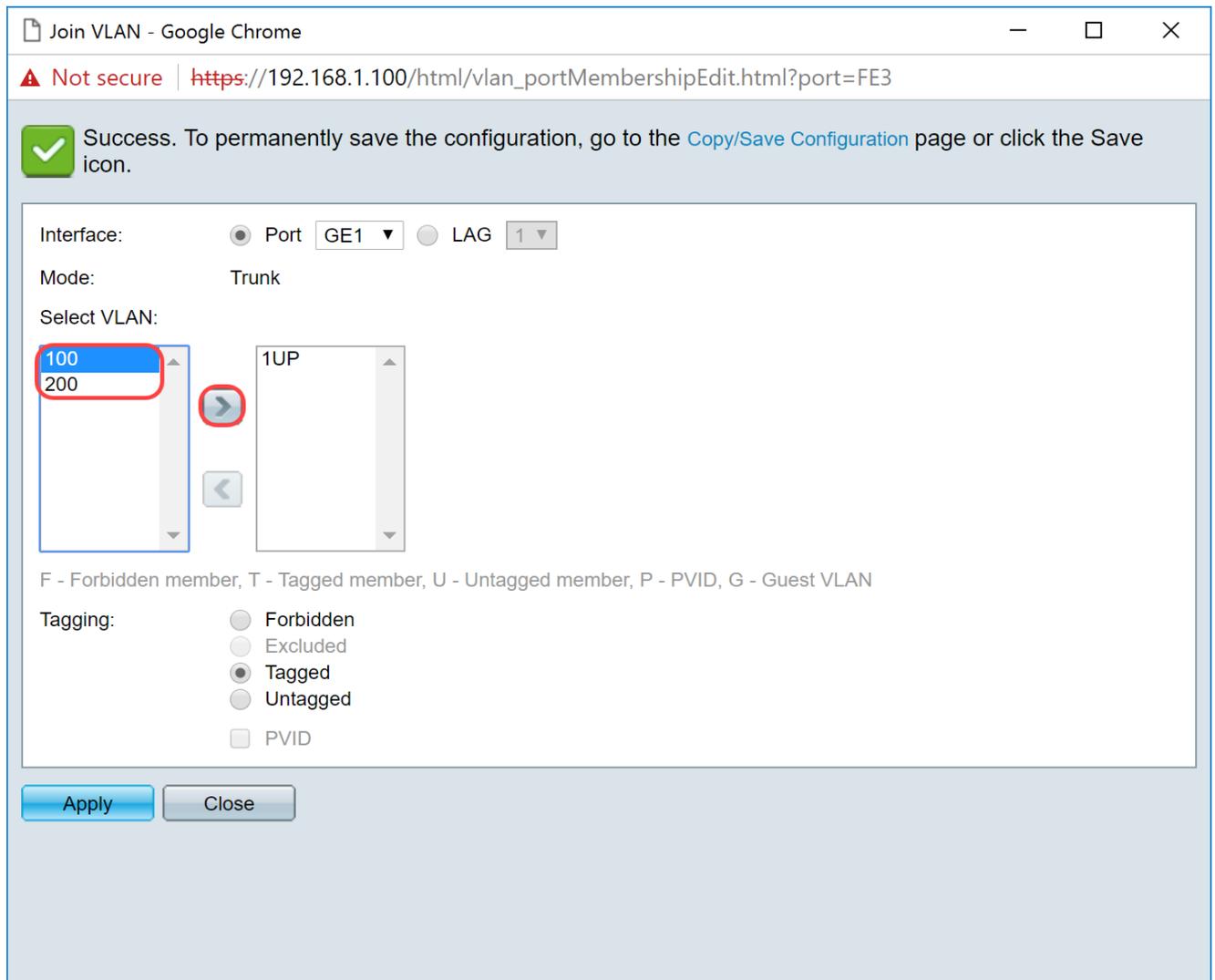
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN

Tagging:

Forbidden  
 Excluded  
 Tagged  
 Untagged  
 PVID

[Apply](#) [Close](#)

Paso 8. Elija la VLAN que se agregará a la interfaz seleccionada y luego haga clic en > para agregarla en la sección Select VLAN. En este ejemplo, seleccionaremos VLAN 100 y 200.



Paso 9. Haga clic en Apply para guardar la configuración.

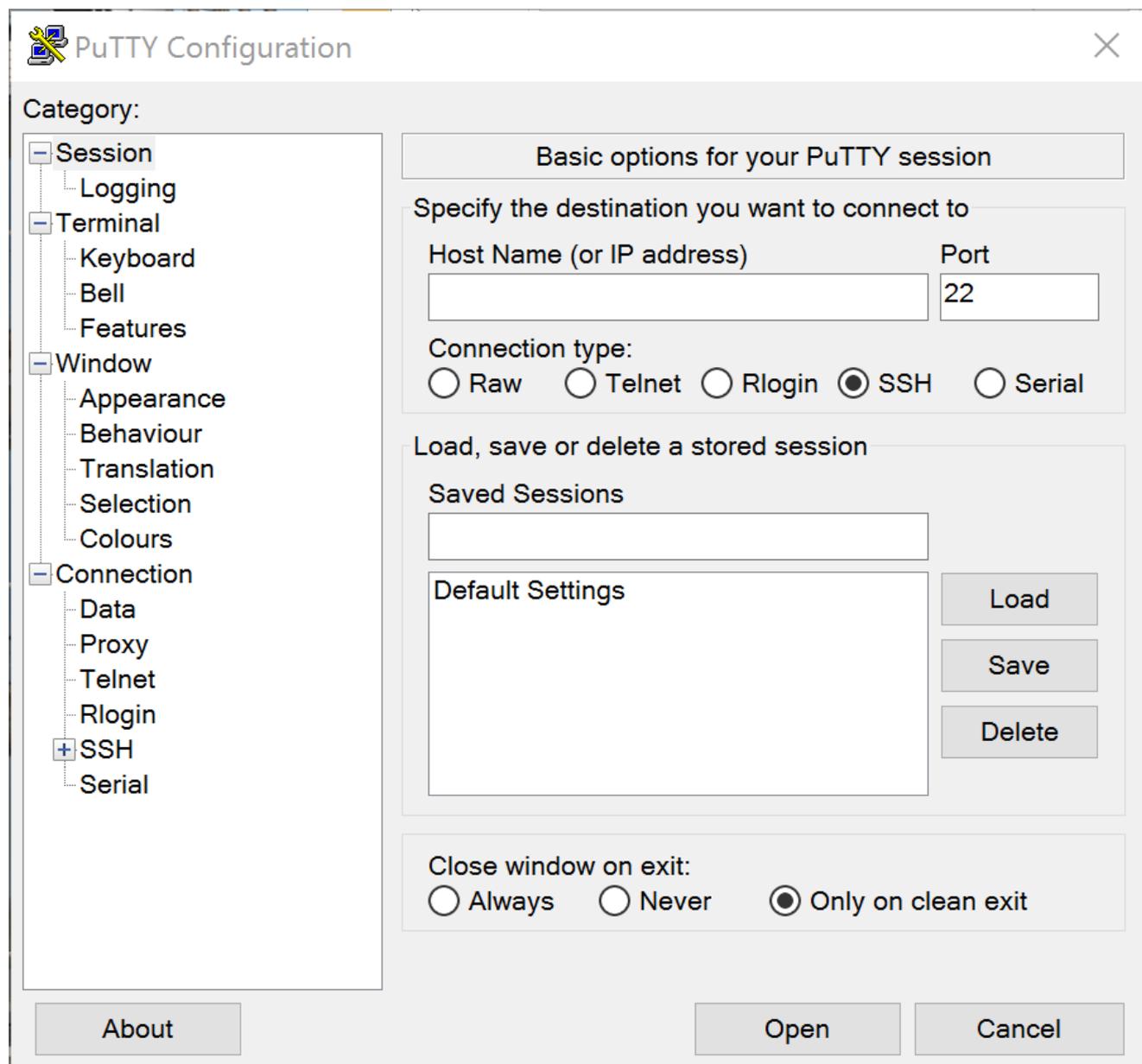
Nota: Es posible que sea necesario reiniciar los teléfonos IP para que la dirección IP cambie a la subred correcta.

## Cambiar la dirección IP de Raspberry Pi para que esté en una subred diferente

Paso 1. Conéctate a tu Raspberry Pi mediante Secure Shell (SSH) o conecta tu Raspberry Pi a un monitor de computadora. En este ejemplo, utilizaremos SSH para configurar el Raspberry Pi.

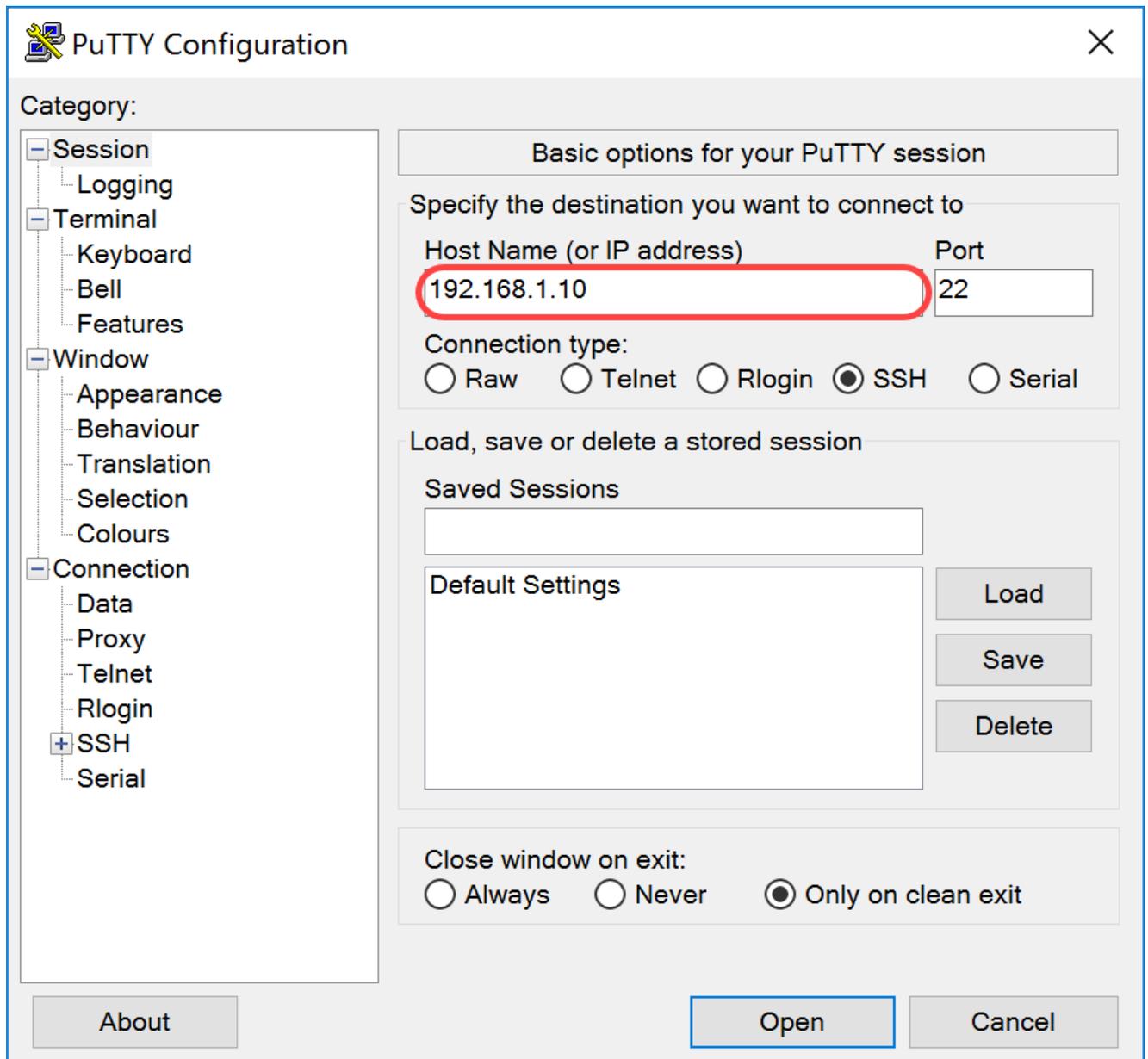
Nota: el puerto del switch para el ordenador/portátil deberá estar en la misma VLAN que el Raspberry Pi y configurado como puerto de acceso al configurar los parámetros de la interfaz. Consulte [Configuración de los parámetros de interfaz en un switch](#) y [Configuración de la pertenencia a VLAN de puerto en la sección Switch](#) de este artículo para revisar. Asegúrese de que su dirección IP está en la misma red que su Raspberry Pi para SSH en ella. Si su dispositivo no está en la misma red que el Raspberry Pi, utilice una dirección IP estática y cambie manualmente su dirección IP para que esté en la misma red o puede escribir el comando `ipconfig /release` e `ipconfig/renew` en el símbolo del sistema para

obtener una nueva dirección IP. Los clientes SSH pueden variar dependiendo de su sistema operativo. En este ejemplo, PuTTY se utilizó para introducir SSH en el Raspberry Pi. Para obtener más información sobre SSH, haga clic [aquí](#).

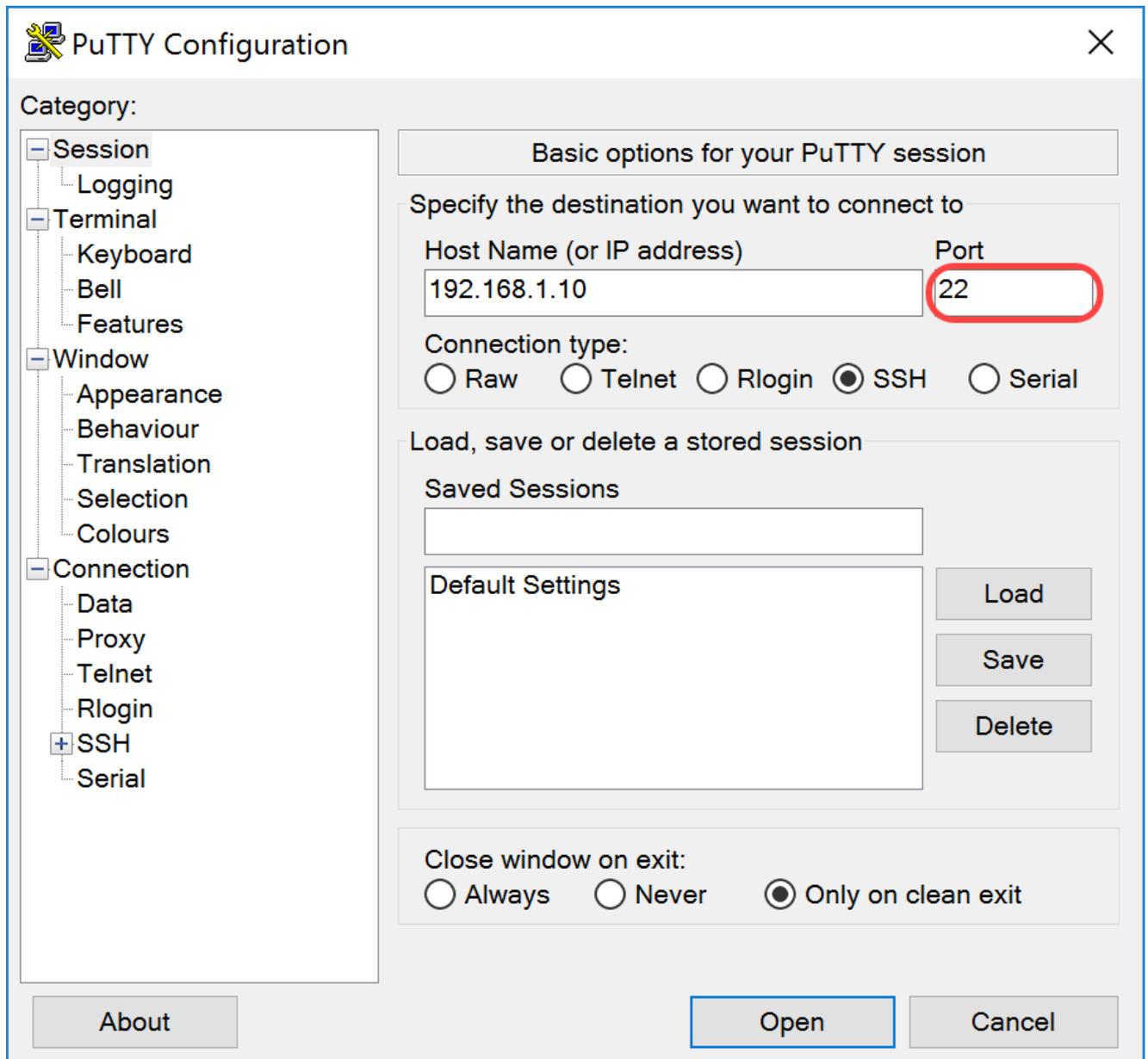


Paso 2. Escriba la dirección IP de su Raspberry Pi en el campo Nombre de host (o dirección IP). En este ejemplo, se introduce 192.168.1.10.

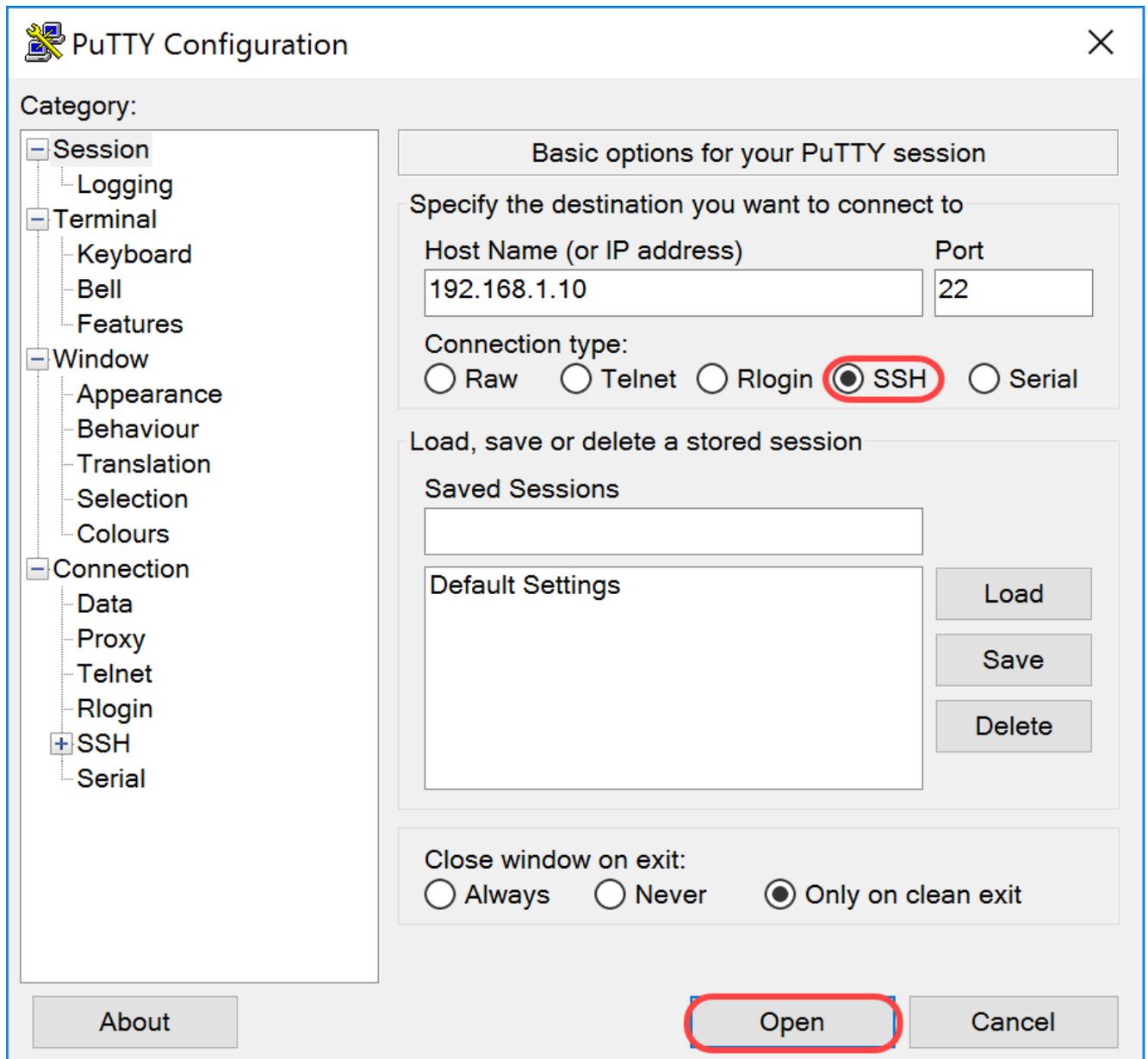
Nota: Puede utilizar la tabla DHCP en el router para encontrar la dirección del Raspberry Pi. En este documento, esta Raspberry Pi estaba preconfigurada para tener una dirección IP estática.



Paso 3. Ingrese 22 como el número de puerto en el campo Puerto. El puerto 22 es el puerto estándar para el protocolo SSH.

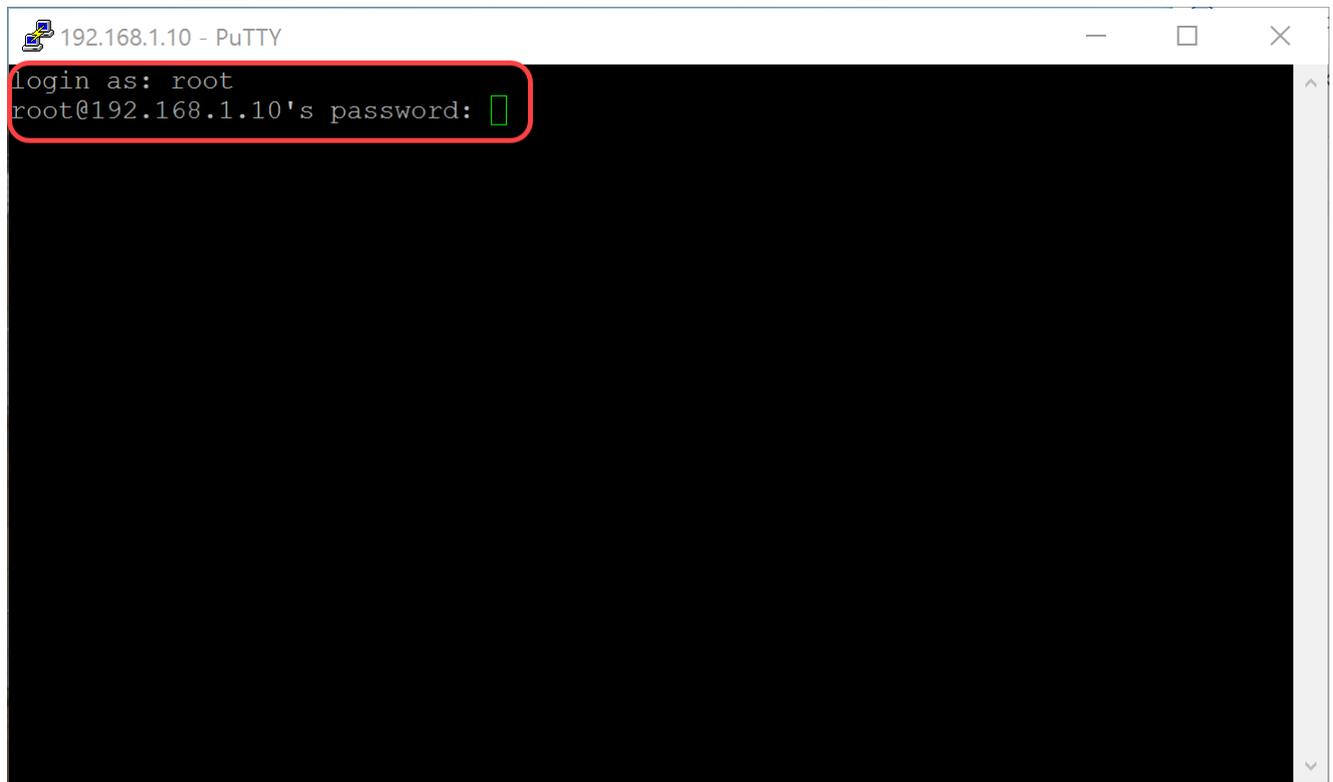


Paso 4. En la sección Tipo de conexión: , haga clic en el botón de opción SSH para elegir SSH como método de conexión con el switch. A continuación, haga clic en Abrir para iniciar la sesión.



Paso 5. Ingrese el nombre de usuario y la contraseña del RasPBX en el campo login as y password.

Nota: El usuario predeterminado: root y la contraseña predeterminada: raspberry

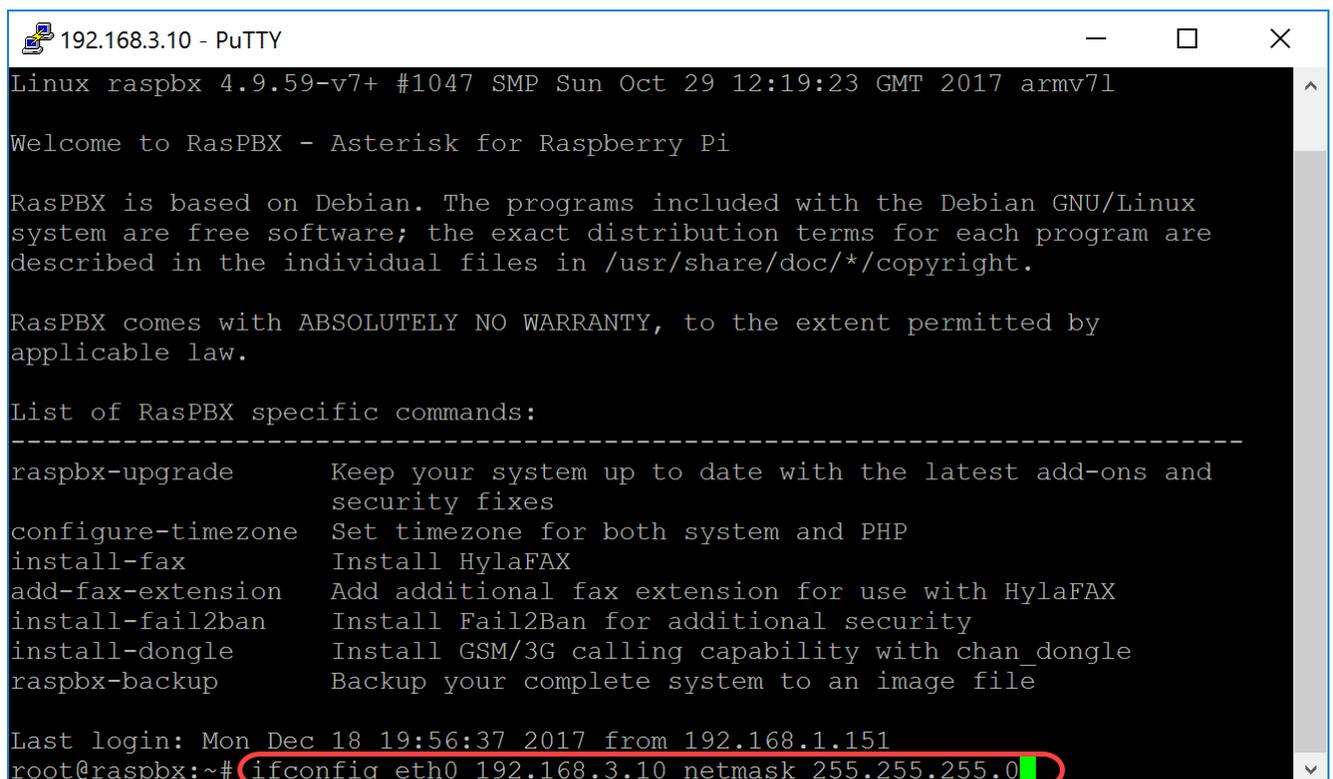


```
192.168.1.10 - PuTTY
login as: root
root@192.168.1.10's password: [ ]
```

Paso 6. Para cambiar la dirección IP de su Ethernet para que sea una dirección IP estática, escriba `ifconfig eth0 [dirección IP] netmask [máscara de red]`. En este ejemplo, utilizaremos 192.168.3.10 y la máscara de red 255.255.255.0

```
ifconfig eth0 192.168.3.10 netmask 255.255.255.0
```

Nota: se le desconectará de la sesión cuando cambie la dirección IP. Para volver a conectarse a Raspberry Pi, el ordenador o portátil debe estar en la misma subred que 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 RasPBX - Asterisk for Raspberry Pi

RasPBX 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.

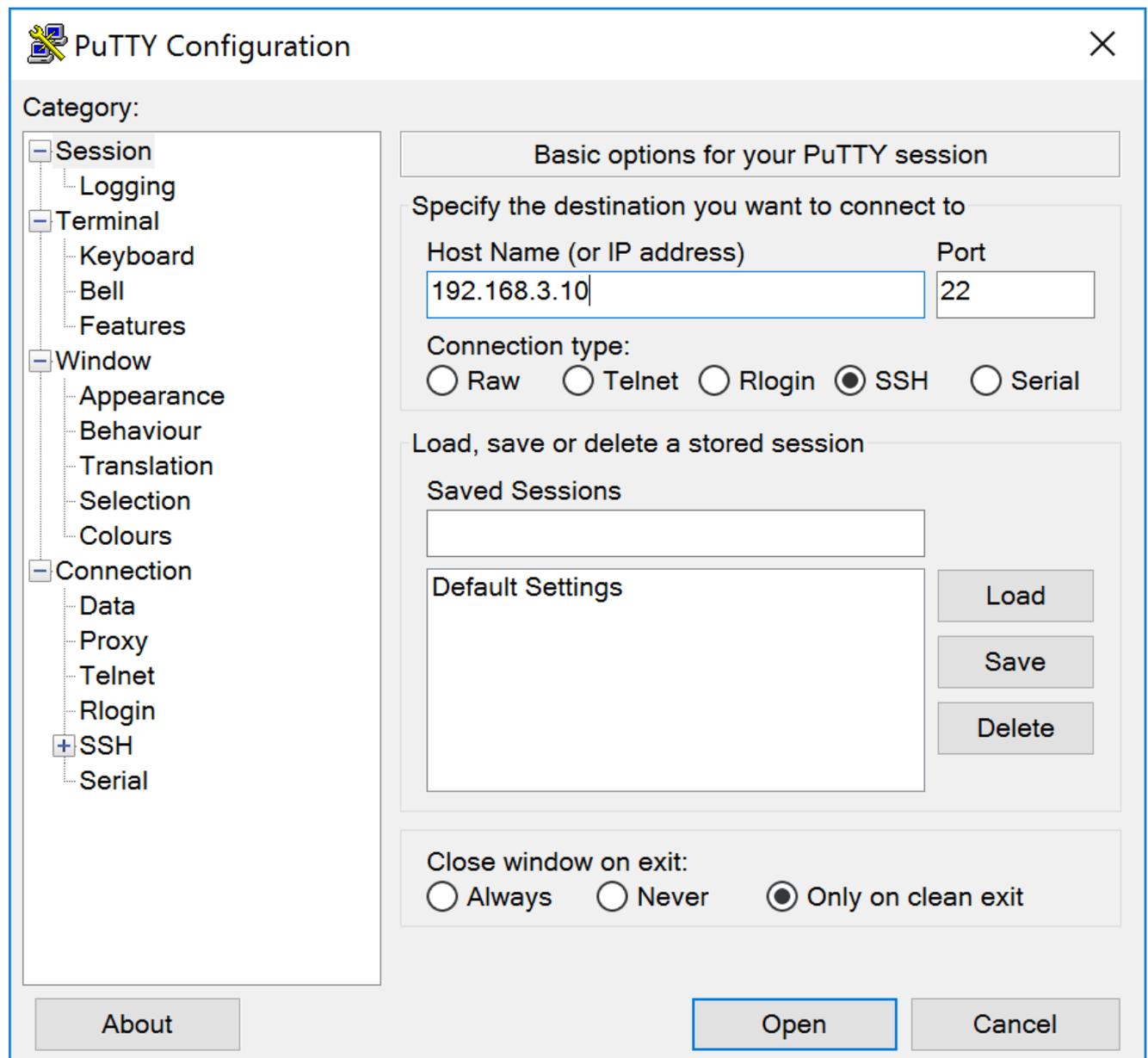
RasPBX comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

List of RasPBX 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
```

Paso 7. Vuelva a conectarse a su Raspberry Pi mediante la dirección IP estática que se configuró en el paso 6. En este ejemplo, utilizamos 192.168.3.10 para volver a conectar.

Nota: Asegúrese de que el ordenador/portátil se encuentra en la misma subred que el Raspberry Pi, así como la VLAN. Si su computadora/laptop está en la misma VLAN que Raspberry Pi y usted no tiene la dirección IP correcta, puede ir al símbolo del sistema y escribir `ipconfig /release` y luego `ipconfig /renew` para solicitar una nueva dirección IP o puede configurar su dispositivo para tener una dirección IP estática en las propiedades Ethernet.



Paso 8. En la línea de comandos, escriba `route add default gw [dirección IP del router de la subred]` para agregar una puerta de enlace predeterminada.

Nota: puede utilizar el comando `route` para ver la tabla de ruteo.

```
route add default gw 192.168.3.1
```

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

RasPBX 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.

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

List of RasPBX 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 14:45:13 2017 from 192.168.3.102
root@raspbx:~# route add default gw 192.168.3.1
```

## Conclusión

Ahora debería haber configurado correctamente una red de voz básica. Para comprobarlo, descuelgue uno de los teléfonos SPA/MPP y oirá un tono de marcado. En este documento, uno de los teléfonos SPA/MPP tiene la extensión 1002 y el otro tiene 1003. Debería poder llamar a la extensión 1003 cuando utilice el teléfono SPA/MPP de la extensión 1002.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).