

# So erstellen Sie ein einfaches Sprachnetzwerk mit Raspberry Pi

## Ziel

Dieses Dokument enthält Anweisungen zur Konfiguration eines Basissprachnetzwerks mit Raspberry Pi als Kommunikationsserver unter Verwendung von Asterisks. Virtual Local Area Network (VLAN) und Quality of Service (QoS) werden zur Priorisierung des Datenverkehrs durch Trennung von Sprach- und Datenverkehr eingesetzt. Ziel dieses Netzwerks ist es, interne Tests einzurichten. Mit diesen Tests können Sie Ihr Netzwerk entsprechend skalieren, feststellen, ob Sie über ausreichend Bandbreite für die erwartete Sprachmenge verfügen, und mögliche Konflikte zwischen den Geräten finden. Darüber hinaus können Sie damit entscheiden, ob Sie das System lokal oder in der Cloud hosten möchten. Wenn ein Unternehmen eine bestimmte Größe erreicht hat, bevorzugt es möglicherweise einen eigenen lokalen Anrufcontroller wie PBX oder IP PBX. Dies würde interne Anrufe effizienter machen, da Anrufe zwischen Telefonen innerhalb des Unternehmens nicht aus dem Gebäude heraus und dann wieder zurück in das Gebäude geleitet werden müssten.

**Wichtiger Hinweis:** Der Raspberry Pi wird von Cisco nicht unterstützt. Dieses Dokument dient nur Support-Zwecken und ist keine Lösung.

## Einleitung

Damit ein Unternehmen seine Geschäftsprozesse effektiv gestalten kann, benötigen die Mitarbeiter Zugriff auf ein Sprachnetzwerk. Dies erleichtert die Kommunikation zwischen Mitarbeitern und ihren Kunden und ermöglicht den Mitarbeitern die Möglichkeit, intern zu kommunizieren. Jeder Mitarbeiter kann mit einem Festnetztelefon und/oder einem Mobiltelefon ausgestattet werden, was jedoch sehr teuer werden kann. Häufig entscheiden sich Unternehmen dafür, ein Sprachnetzwerk einzurichten, das stattdessen Voice over Internet Protocol (VoIP) verwendet.

Die VoIP-Technologie ermöglicht Ihnen, über das Internet Telefonanrufe von jedem Standort an jeden Standort der Welt zu tätigen und zu empfangen, und zwar mit minimalen, wenn überhaupt, Ferngebühren. Dies kann auf jedem Gerät verwendet werden, das das Internet verwendet.

Mit VoIP kann ein Unternehmen Geld sparen und gleichzeitig die Produktivität, Kommunikation und Kundenzufriedenheit steigern. Mitarbeiter können verschiedene Funktionen nutzen, z. B. Anrufweiterleitung, Warteschleifenmusik und integrierte Voicemail.

Eine gemeinsame Funktion von VoIP, die viele Unternehmen nutzen, ist die Anrufweiterleitung, die auch als automatische Anrufverteilung bezeichnet wird. Die Anrufweiterleitung verteilt eingehende Anrufe an den nächsten verfügbaren Mitarbeiter, anstatt sie an die Voicemail weiterzuleiten. So wird sichergestellt, dass Kundenanrufe so effizient wie möglich beantwortet werden. Nach Geschäftsschluss können Anrufe direkt an die Voicemail weitergeleitet werden.

Das Hinzufügen von Benutzern und das Aktualisieren von Funktionen ist ein einfacher Prozess, der hilfreich ist, wenn Ihr Unternehmen expandiert oder sich Ihre Anforderungen ändern. Im Gegensatz zu herkömmlichen Telefonsystemen ist keine teure Verkabelung erforderlich.

Um ein VoIP-Netzwerk einzurichten, müssen Sie verschiedene Optionen in Betracht ziehen. Sie können einen VoIP-Service für Ihr eigenes Telefonsystem mithilfe von Telefonanlagen ohne Telefonanlage, Telefonanlage (PBX) oder einem anderen VoIP-System hosten.

Berücksichtigen Sie dabei Ihr Budget, die Anzahl der Mitarbeiter und Standorte, die in Ihrer Region verfügbaren Services und das Unternehmenswachstum. Auch Schulungen und zusätzliche Geräte wie Headsets sind möglicherweise erforderlich. VoIP kann Ihre Datennutzung erhöhen, und Sie müssen möglicherweise Ihre Bandbreite erhöhen, um den Sprachdatenverkehr im Netzwerk zu berücksichtigen.

Sie sollten auch ein Backup planen, "Plan B", falls Ihr Netzwerk jemals ausfällt. Wenn Sie den Strom verlieren, wird Ihr VoIP-System nicht verbunden. Diese Redundanz sollte implementiert werden, um die Telefondienste sofort wiederherzustellen und eine Unterbrechung der Geschäftsproduktivität zu verhindern.

In diesem Artikel stellen wir unser eigenes Telefonsystem mithilfe von Asterisk, einer Telefonanlage auf einem Raspberry Pi, bereit.

**Hinweis:** Wenn Sie diese Schritte durchgeführt haben und auch aus Ihrem internen Netzwerk heraus anrufen möchten, müssen Sie einen Internet Telephony Service Provider (ITSP) auswählen.

## Definitionen

Ein **virtuelles LAN (VLAN)** ermöglicht die logische Segmentierung eines LAN (Local Area Network) in verschiedene Broadcast-Domänen. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden. Eine Übertragung kann dann auf ein spezifisches VLAN beschränkt werden. Nur Benutzer in einem bestimmten VLAN können auf Daten in diesem VLAN zugreifen und diese bearbeiten. Mithilfe von VLANs kann auch die Leistung verbessert werden, da Broadcasts und Multicasts seltener an unnötige Ziele gesendet werden müssen.

Alle Ports sind standardmäßig VLAN 1 zugewiesen. Wenn Sie also verschiedene VLANs einrichten, müssen Sie die Ports manuell dem entsprechenden VLAN zuweisen.

Jedes VLAN muss mit einer eindeutigen VLAN-ID (VID) zwischen 1 und 4094 konfiguriert werden. Das Gerät reserviert die VID 4095 als verworfenes VLAN. Alle Pakete, die dem Verwerfungs-VLAN zugewiesen wurden, werden beim Eingang verworfen und nicht an einen Port weitergeleitet.

**Quality of Service (QoS)** ermöglicht die Priorisierung des Datenverkehrs für verschiedene Anwendungen, Benutzer oder Datenflüsse. Sie kann auch verwendet werden, um die Leistung auf einem bestimmten Niveau zu garantieren, was sich auf die QoS für den Client auswirkt. Die QoS wird im Allgemeinen von den folgenden Faktoren beeinflusst: Jitter, Latenz und Paketverlust. In den meisten Fällen wird Video oder VoIP Priorität eingeräumt, da sie am stärksten von QoS beeinflusst werden.

**Eine Telefonanlage (PBX)** ist ein Telefonvermittlungssystem, das ein- und ausgehende Anrufe für interne Benutzer in einem Unternehmen verwaltet. Ein PBX-System ist mit dem öffentlichen Telefonsystem verbunden und leitet eingehende Anrufe automatisch an bestimmte Nebenstellen weiter. Darüber hinaus können mehrere Leitungen gemeinsam genutzt und verwaltet werden. Ein typisches PBX-System für kleine und mittlere Unternehmen umfasst externe und interne Telefonleitungen, einen Computerserver für die Anrufumschaltung und -weiterleitung und eine Konsole für die manuelle Steuerung.

Ein **IP-PBX-System** kann alle Funktionen eines herkömmlichen Small Business-PBX-Systems ausführen und vieles mehr. Er übernimmt das Switching und Verbinden von VoIP- und Festnetzanrufen. Ein IP-PBX-System wird auf einem IP-Datennetzwerk ausgeführt, wodurch Kosten eingespart und die Netzwerkverwaltung minimiert wird. Sie können IP-Telefone, Softphones (die keine andere Telefonhardware als einen Computer und ein Mikrofon-Headset benötigen) und

Festnetztelefone auf einem IP-PBX-Telefonsystem verwenden.

Ein **Raspberry Pi** ist ein kostengünstiger, kleiner, tragbarer Computer, der wie ein Desktop-Computer funktioniert.

**Asterisk** ist ein Open-Source-Framework, das einen Computer, wie z. B. einen Raspberry Pi, zu einem Kommunikationsserver machen kann. Auf diese Weise können Sie Ihr eigenes Telefonanlagensystem für Unternehmen einrichten. In diesem Artikel verwendet Asterisk FreePBX als grafische Benutzeroberfläche (GUI), die Asterisk steuert und verwaltet, wo Sie Erweiterungen, Benutzer usw. konfigurieren können.

## Unterstützte Geräte

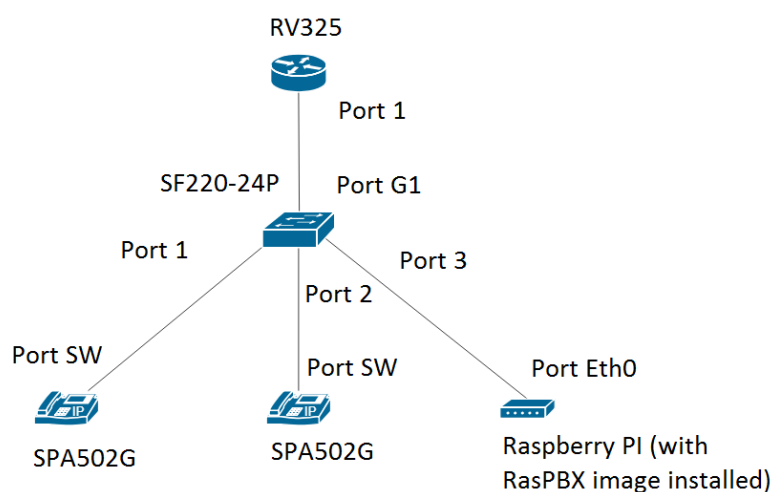
- Router
- Power over Ethernet (PoE)-Switch
- Raspberry Pi (Modelle Pi 3 B+, Pi 3, Pi 3, B+, B und A)
- 2 oder mehr Cisco SPA/MPP IP-Telefone

## Software-Version

- 14.0.1.20 (FreePBX)
- 13.20.0 (Asterisk)
- 1.1.1.06 (RV325-Router)
- 1.1.4.1 (SF220-24P)
- 7,1/3 (SPA 502G)

Um Basic Voice Network mit Raspberry Pi zu konfigurieren, folgen Sie den folgenden Richtlinien:

**Topologie:**



Das Bild für das RasPBX finden Sie [hier](#). Dieses Image muss auf dem Raspberry Pi installiert werden.

**Hinweis:** In diesem Dokument ist der Raspberry Pi mit dem RasPBX-Image bereits konfiguriert. Um auf die grafische Benutzeroberfläche des Raspberry Pi zuzugreifen, geben Sie <http://raspbx.local> oder die IP-Adresse des Raspberry Pi in Ihrem Browser ein, um das PBX-System zu konfigurieren. Die Standard-FreePBX-Anmeldung lautet user: **admin** password: **admin**. Außerdem wurde der Raspberry Pi so vorkonfiguriert, dass er eine statische IP-Adresse hat.

## Inhalt

1. [Einrichten von VLANs auf dem Router](#)
2. [Konfigurieren von SPA-/MPP-Telefonen](#)
3. [Konfigurieren von VLANs auf einem Switch](#)
4. [Einrichten von Sprach-VLANs auf einem Switch](#)
5. [Konfigurieren der Schnittstelleneinstellungen eines Switches](#)
6. [Konfigurieren der Port-VLAN-Zugehörigkeit auf einem Switch](#)
7. [Ändern der IP-Adresse von Raspberry Pi in ein anderes Subnetz](#)
8. [Schlussfolgerung](#)

## Einrichten von VLANs auf dem Router

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und navigieren Sie zu **Port Management > VLAN Membership**.

**Hinweis:** Dies kann je nach Modell variieren. In diesem Beispiel wird RV325 verwendet. Weitere Informationen zum Zugriff auf die webbasierte Setup-Seite finden Sie [hier](#).



Small Business  
Cisco RV325 Gigabit Dual WAN VPN Router

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

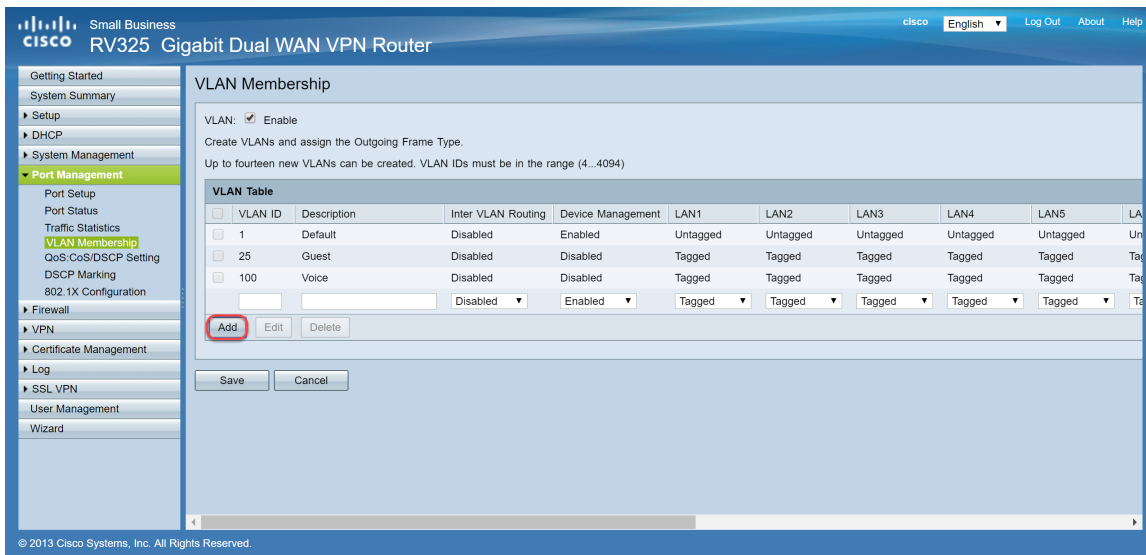
© 2013 Cisco Systems, Inc. All Rights Reserved.

Schritt 2: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um VLAN auf dem Router zu aktivieren.



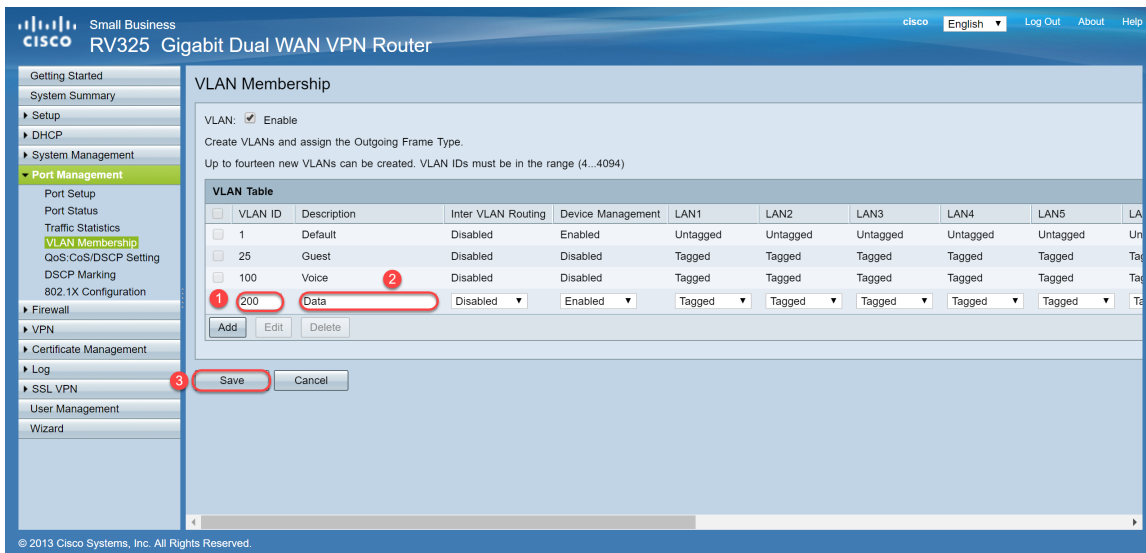


Schritt 3: Klicken Sie im Abschnitt *VLAN Table* (*VLAN-Tabelle*) auf **Add (Hinzufügen)**, um eine neue VLAN-ID zu erstellen.



Schritt 4: Geben Sie im Feld für die *VLAN-ID* eine VLAN-Nummer ein. Die VLAN-IDs müssen zwischen 4 und 4094 liegen. In diesem Beispiel wird 200 als VLAN-ID für Daten verwendet. Geben Sie als Nächstes eine Beschreibung für das VLAN in das Feld *Description* (*Beschreibung*) ein. Als Beispiel für die Beschreibung werden Daten eingegeben. Klicken Sie dann auf **Speichern**.

**Hinweis:** VLAN 100 für Sprache wurde standardmäßig auf diesem Router erstellt. Es können bis zu vierzehn neue VLANs erstellt werden.



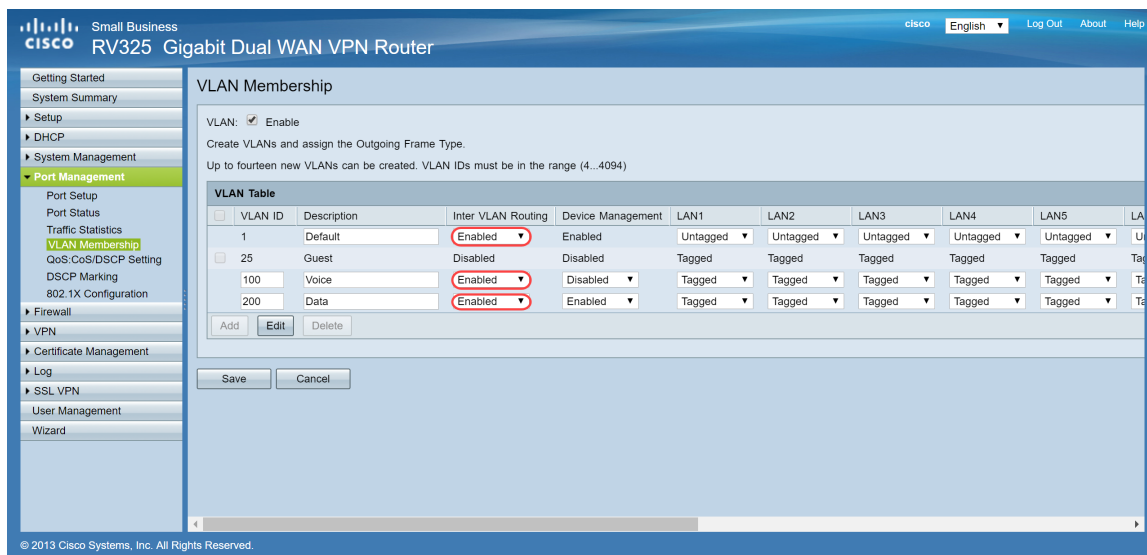
Schritt 5: Um ein VLAN zu bearbeiten, aktivieren Sie das Kontrollkästchen des entsprechenden VLAN. In diesem Beispiel werden VLAN 1, 100 und 200 bearbeitet. Klicken Sie anschließend auf **Edit** (Bearbeiten), um die VLANs zu bearbeiten.



Schritt 6: Wählen Sie optional in der Dropdown-Liste "*Inter VLAN Routing*" die Option **Enabled** (Aktiviert) oder **Disabled** (Deaktiviert) aus, um Pakete von einem VLAN zu einem anderen VLAN weiterzuleiten. Die Aktivierung dieser Funktion ist nützlich, da interne Netzwerkadministratoren von einem entfernten Standort aus auf Ihre Geräte zugreifen können, um Probleme zu beheben. Dadurch wird die Zeit reduziert, die erforderlich ist, um ständig VLANs wechseln zu müssen, um auf die Geräte zuzugreifen.

- Disabled (Deaktiviert): Das bedeutet, dass Inter-VLAN-Routing inaktiv ist.
- Enabled (Aktiviert): Stellt dar, dass VLAN-übergreifendes Routing in diesem VLAN aktiv ist. Beim VLAN-übergreifenden Routing werden die Pakete nur an die VLANs weitergeleitet, in denen sie aktiviert sind.

**Hinweis:** In diesem Beispiel wird Inter-VLAN-Routing für die VLAN-ID 1, 100 und 200 aktiviert.



Schritt 7. Wählen Sie die gewünschte Option aus der Dropdown-Liste für den LAN-Port aus, mit dem Sie verbunden sind, und die Einstellung muss mit dem verbundenen Port übereinstimmen. Wenn Sie mit mehr als einem Port verbunden sind, müssen Sie für jeden Port, den Sie verbinden, dieselben Einstellungen wählen. Der Standardwert ist tagged, für VLAN 1 jedoch untagged.

**Hinweis:** Wenn Sie in Schritt 6 Inter-VLAN-Routing aktivieren, müssen Sie das VLAN mit Tags versehen, um den Datenverkehr zu unterscheiden.

#### Markiert

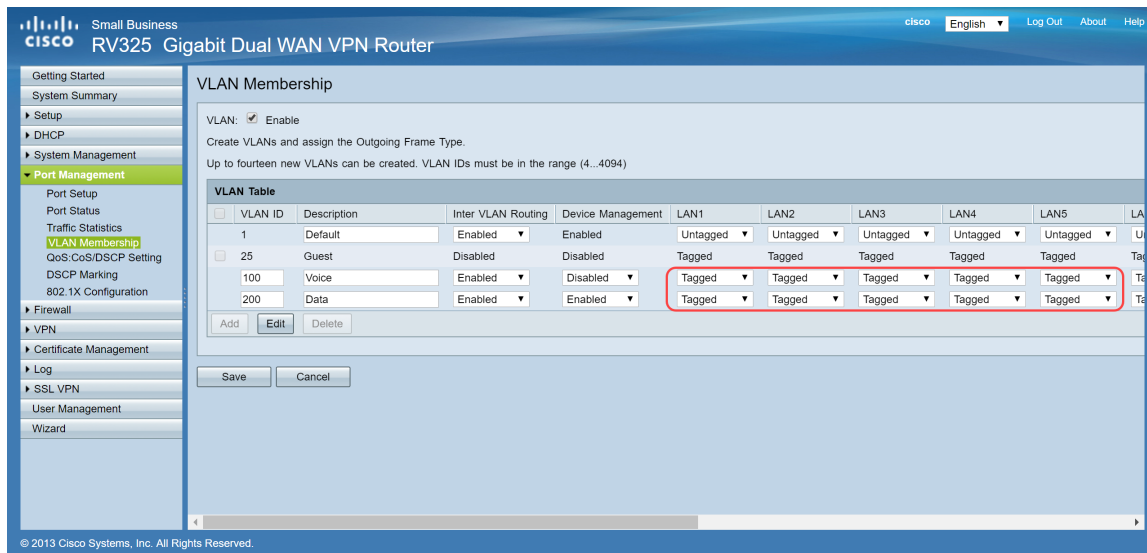
- Stellt dar, dass die Zuordnung zwischen dem Port und dem VLAN als markiert ist.
- Tagged wird verwendet, um zu bestimmen, zu welchem VLAN der Datenverkehr über die eindeutige VLAN-ID gehört, wenn mehrere VLANs für denselben Port erstellt werden.

#### Nicht markiert

- Stellt dar, dass die Zuordnung zwischen dem Port und dem VLAN nicht markiert ist.
- Sie wird verwendet, wenn nur ein VLAN erstellt wird und der Datenverkehr das VLAN erkennt. Nur ein VLAN kann für jeden LAN-Port als nicht markiert werden.
- Wenn sich das Standard-VLAN auf dem Port befindet, sollte die Markierung immer aufgehoben werden, auch wenn der Port über mehrere VLANs verfügt.

#### Ausgeschlossen

- Stellt dar, dass die Schnittstelle kein Mitglied des VLAN ist.
- Wenn Sie diese Option auswählen, wird der Datenverkehr zwischen dem VLAN und dem Port deaktiviert.



Schritt 8: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

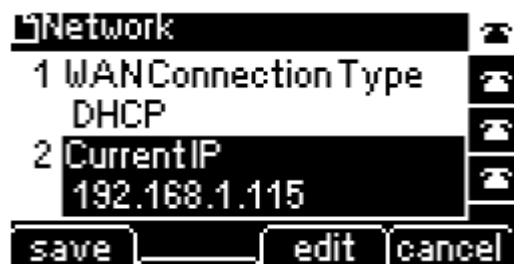
**Hinweis:** Sie können sich auf dem Router beim webbasierten Dienstprogramm anmelden und zu **DHCP > DHCP Setup** navigieren, um die VLANs für ein bestimmtes Subnetz zu konfigurieren. Standardmäßig sind die VLANs in einem anderen Subnetz konfiguriert.

## Konfigurieren von SPA-/MPP-Telefonen

Benutzer können die Telefone auch so konfigurieren, dass sie ein Profil von einem manuell konfigurierten Profilstandort, einem über die DHCP-Option 150 gefundenen Standort, oder von einem Cisco EDOS-Server abrufen. Nachfolgend finden Sie ein Beispiel für eine manuelle Konfiguration.

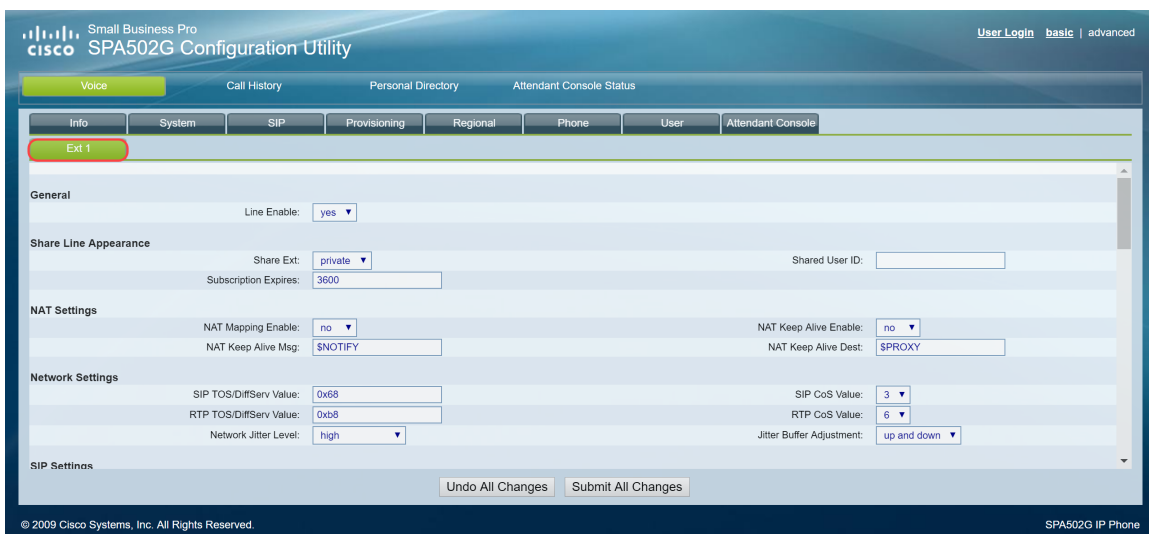
Schritt 1: Geben Sie die IP-Adresse des SPA/MPP in Ihren Browser ein, und navigieren Sie zu **Admin Login (Admin-Anmeldung)** und dann zu **Advanced (Erweitert)**.

**Hinweis:** Die Konfiguration für das SPA-/MPP-Telefon kann je nach Modell variieren. In diesem Beispiel wird das SPA502G verwendet. Um die IP-Adresse Ihres IP-Telefons zu finden, navigieren Sie zu **DHCP > DHCP Status (DHCP-Status auf Ihrem Router)** (kann je nach Modell variieren). Eine weitere Möglichkeit besteht darin, die **Setup**-Taste zu drücken und auf Ihrem Cisco Telefon zu **Network (Netzwerk)** zu navigieren (Menüs und Optionen können je nach Telefonmodell variieren).



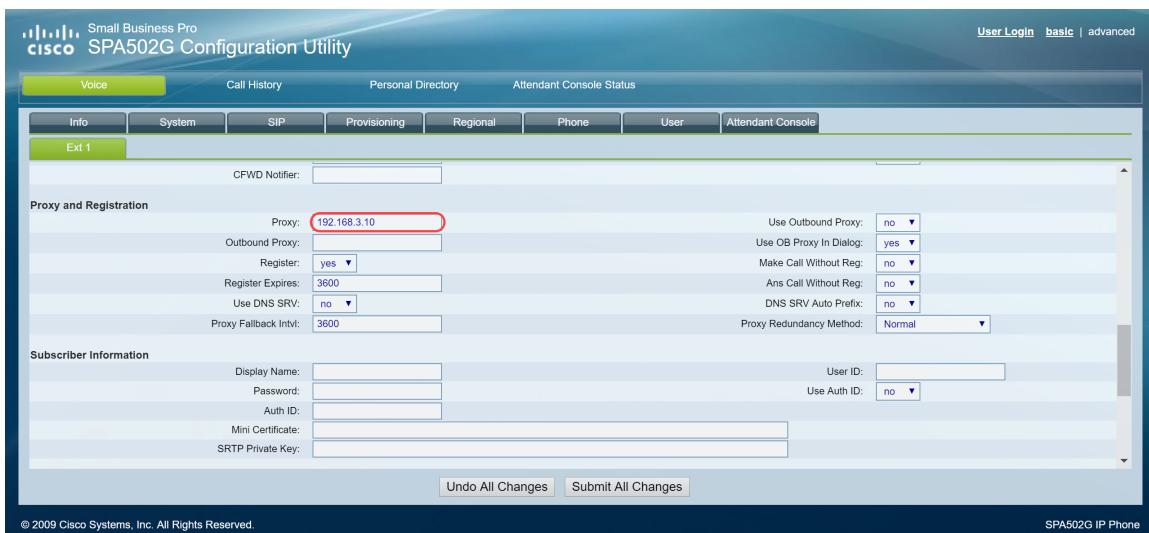


Schritt 2: Navigieren Sie zu **Voice > Ext 1**, die Durchwahlseite wird geöffnet.



Schritt 3: Geben Sie im Abschnitt *Proxy and Registration (Proxy und Registrierung)* den Proxyserver in das Feld *Proxy (Proxy) ein*. In diesem Beispiel wird die Adresse des Raspberry Pi (192.168.3.10) als Proxyserver verwendet. VLAN 100 befindet sich im Subnetz mit 192.168.3.x.

**Hinweis:** Sie konfigurieren die IP-Adresse des Himbeer-Pi später in diesem Artikel, wenn Sie mehr erfahren möchten, klicken Sie auf den Link zu diesem Abschnitt umgeleitet werden: [Ändern der Adresse des Himbeer-Pi auf ein anderes Subnetz.](#)



Schritt 4: Geben Sie unter *Subscriber Information (Teilnehmerinformationen)* den Anzeigenamen und die Benutzer-ID (Durchwahlnummer) für die freigegebene Durchwahlnummer ein. In diesem Beispiel wird die Durchwahl 1003 verwendet.

**Hinweis:** Die Durchwahl 1003 wurde bereits auf dem Raspberry Pi erstellt und konfiguriert.

The screenshot shows the Cisco SPA502G Configuration Utility interface. The 'Subscriber Information' section is highlighted, showing the following fields:

Display Name:	1003	User ID:	1003
Password:		Use Auth ID:	no
Auth ID:			
Mini Certificate:			
SRTTP Private Key:			

Other visible fields include: Regional CAPTEL: 3000, Use DNS SRV: no, Proxy Fallback Intvl: 3600, DNS SRV Auto Prefix: no, Proxy Redundancy Method: Normal, 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.

Schritt 5: Geben Sie das Passwort der Erweiterung ein, die Sie im Raspberry Pi-Erweiterungsabschnitt konfiguriert haben. Dies ist auch als *Geheim* unter dem *Edit Extension* Abschnitt in der Himbeer Pi. In diesem Beispiel wurde das Kennwort **12345** verwendet.

**Hinweis:** Das Kennwort **12345** wurde nur als Beispiel verwendet. Ein komplexeres Kennwort wird empfohlen.

The screenshot shows the same Cisco SPA502G Configuration Utility interface as in Step 4. The 'Subscriber Information' section is highlighted, and the 'Password' field is now filled with '12345'.

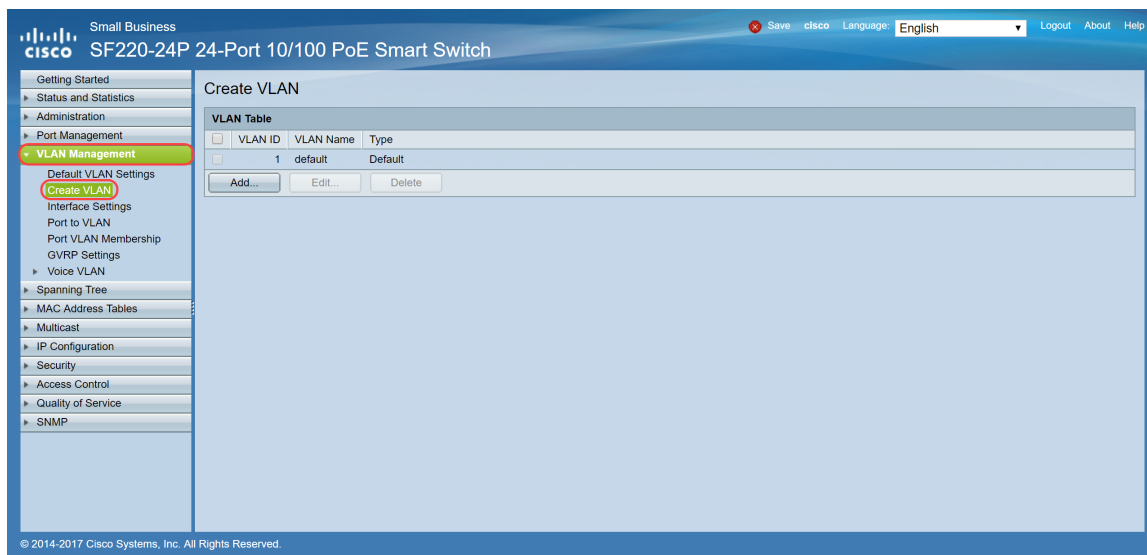
Display Name:	1003	User ID:	1003
Password:	12345	Use Auth ID:	no
Auth ID:			
Mini Certificate:			
SRTTP Private Key:			

Other visible fields are the same as in Step 4.

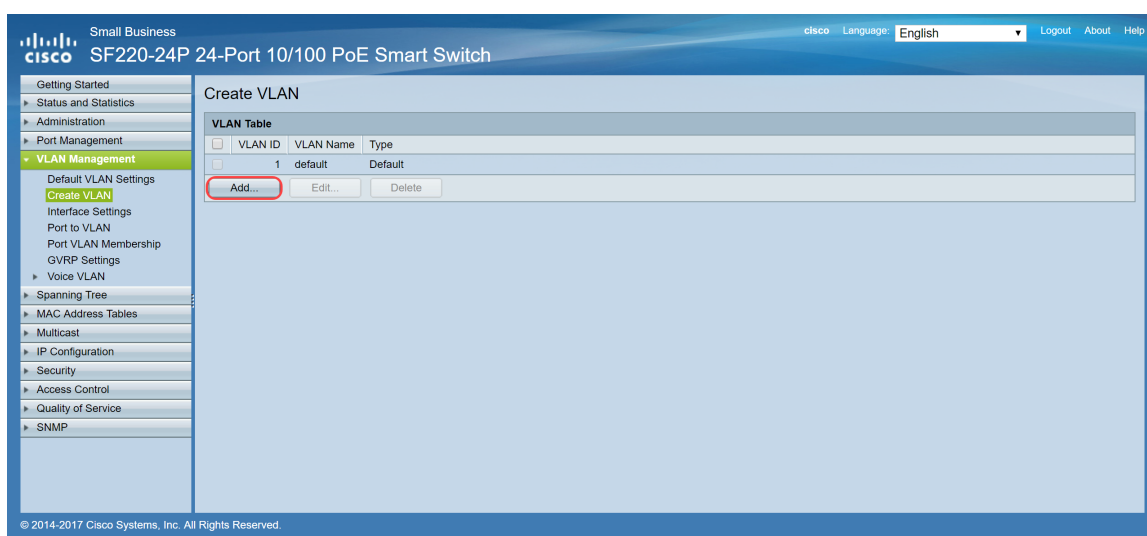
Schritt 6: Wählen Sie die gewünschte Option aus der Dropdown-Liste *Auth-ID verwenden*. Die Optionen lauten **Ja** und **Nein**. Um die SIP-Authentifizierung (Session Initiation Protocol) zu aktivieren, bei der SIP-Nachrichten angefordert werden können, um zu bestimmen, ob sie autorisiert sind, bevor sie übertragen können, wählen Sie **Ja** aus der *Auth ID*-Dropdown-Liste aus. In diesem Beispiel haben wir **Ja** gewählt.







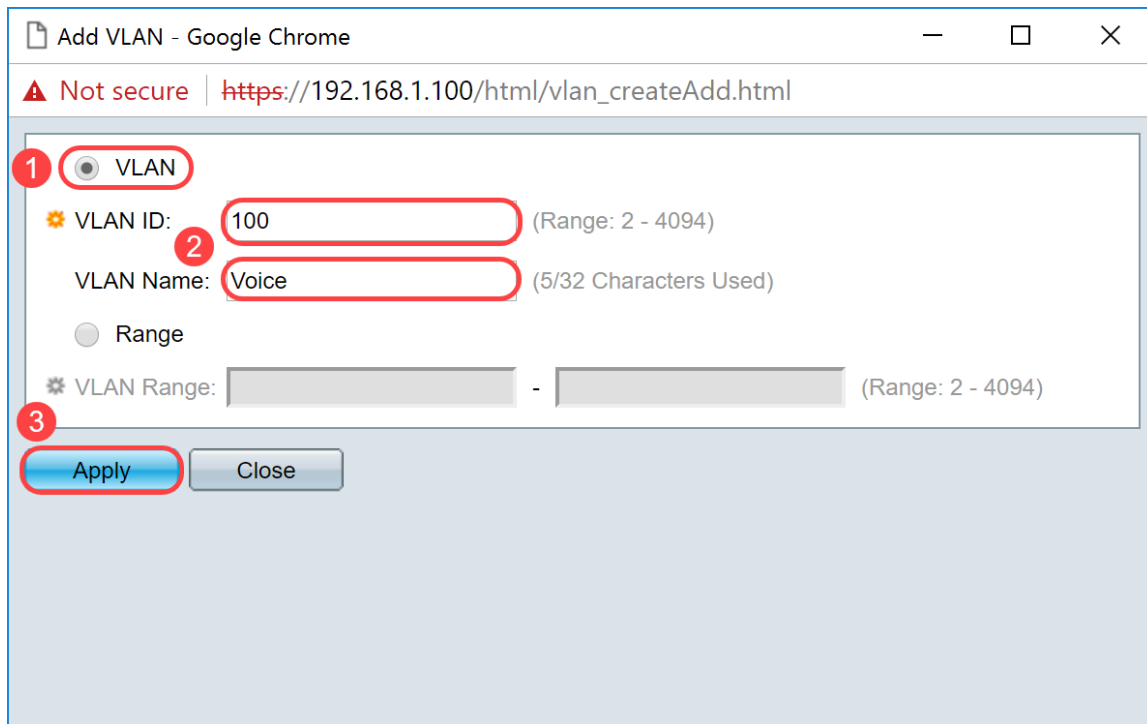
Schritt 2: Klicken Sie auf **Hinzufügen...** um ein neues VLAN zu erstellen.



Schritt 3: Um ein einzelnes VLAN zu erstellen, wählen Sie das Optionsfeld **VLAN** aus. Geben Sie die **VLAN-ID** und den **VLAN-Namen** ein. Klicken Sie anschließend auf **Apply**, um das VLAN zu speichern. In diesem Beispiel erstellen wir VLAN 100 für Sprache und 200 für Daten.

**Hinweis:** Einige VLANs werden vom System für die interne Systemnutzung benötigt und können daher nicht durch Eingabe der Start-VID und End-VID erstellt werden. Wenn Sie die **Range**-Funktion verwenden, können Sie maximal 100 VLANs gleichzeitig erstellen.



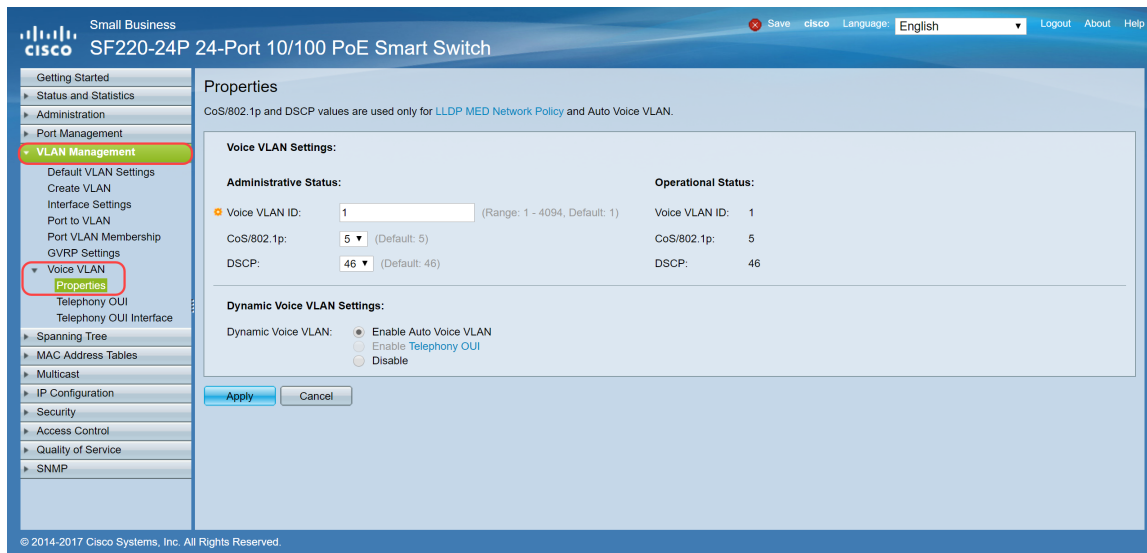


**Hinweis:** Wiederholen Sie Schritt 2, wenn Sie ein weiteres einzelnes VLAN erstellen müssen.

## Einrichten des Sprach-VLANs auf dem Switch

Schritt 1: Melden Sie sich bei der Webkonfiguration an, und navigieren Sie zu **VLAN Management > Voice VLAN > Properties**.

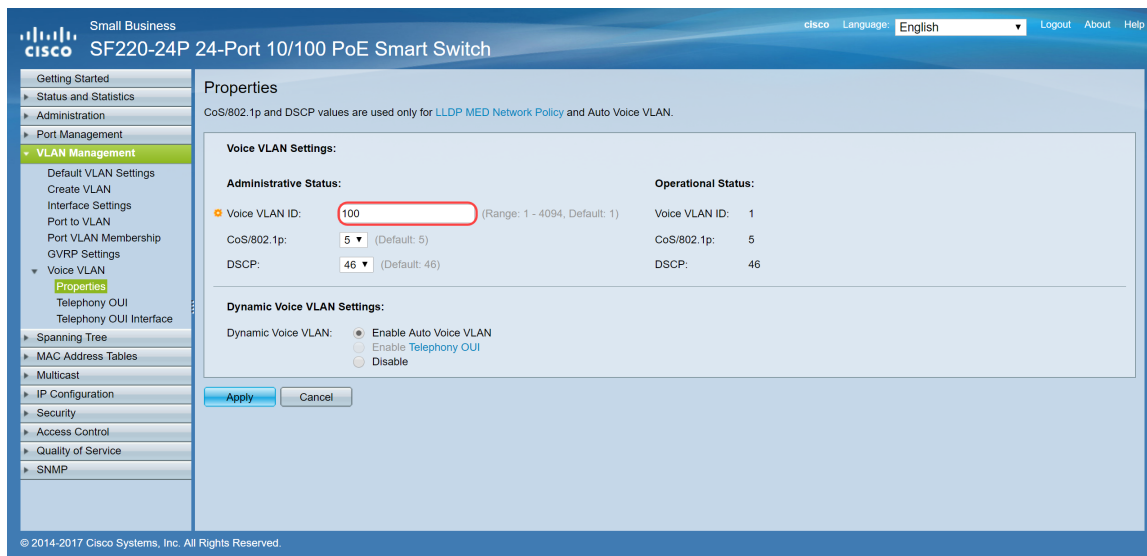
**Hinweis:** Bei der Konfiguration des Auto Voice VLAN werden automatisch QoS-Einstellungen für das Sprach-VLAN angewendet, und der Sprachverkehr wird priorisiert.



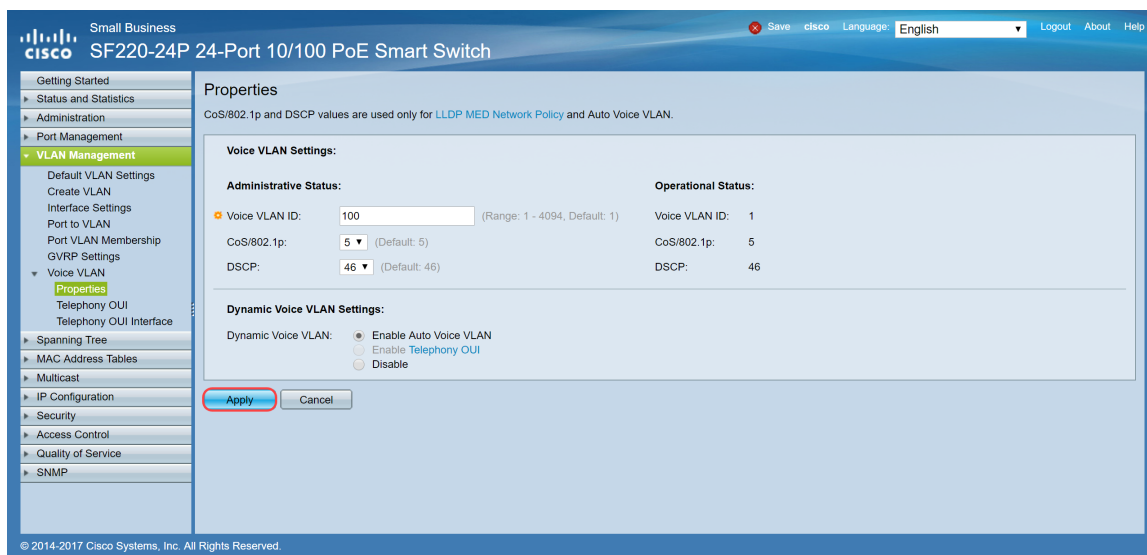
Schritt 2: Geben Sie unter *Administrative Status (Verwaltungsstatus)* im Feld Voice VLAN ID (*Sprach-VLAN-ID*) das VLAN ein, das das Sprach-VLAN sein soll. In diesem Beispiel wird VLAN 100 als Sprach-VLAN eingegeben.

**Hinweis:** Änderungen an der Sprach-VLAN-ID, der Class of Service (CoS)/802.1p und/oder dem Differentiated Service Code Point (DSCP) veranlassen das Gerät, das administrative Sprach-VLAN als statisches Sprach-VLAN anzukündigen. Wenn die Option "Auto Voice VLAN Activation" (Durch

externes Sprach-VLAN ausgelöste *automatische Sprach-VLAN-Aktivierung*) ausgewählt ist, müssen die Standardwerte beibehalten werden. In diesem Beispiel wird CoS/802.1p als Standardwert von 5 und DSCP als Standardwert von 46 belassen.



Schritt 3: Klicken Sie auf **Apply**, um Ihre Einstellungen zu speichern.

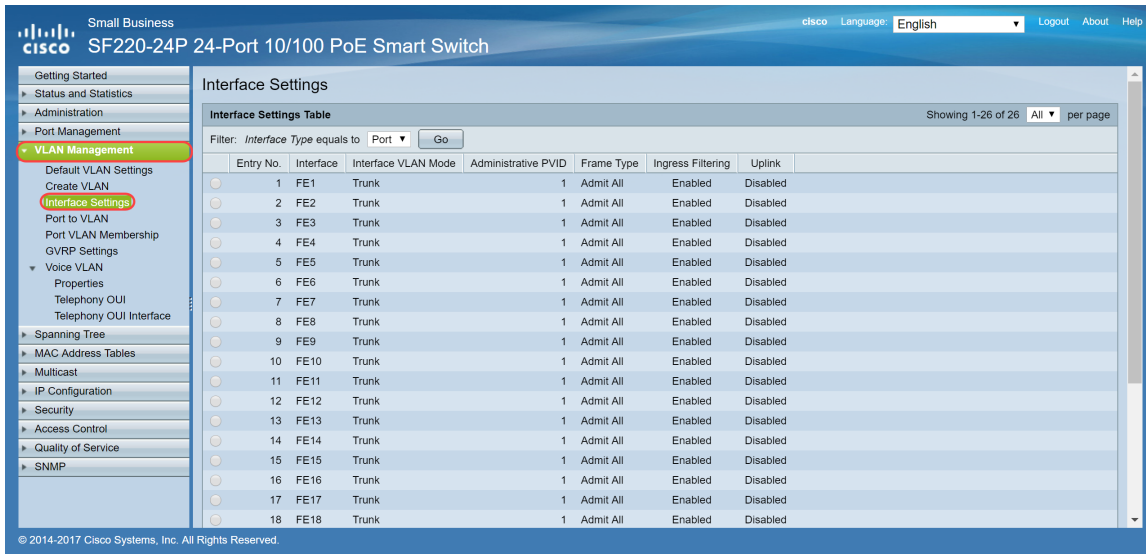


## Konfigurieren der Schnittstelleneinstellungen des Switches

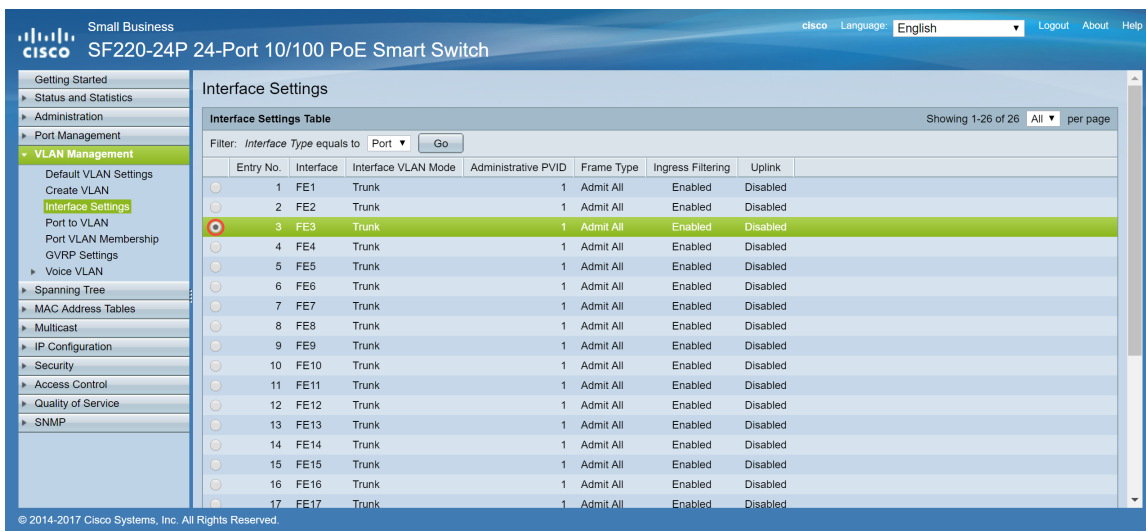
Die Schnittstellen, die physischen Ports am Switch, können einer der folgenden Einstellungen zugewiesen werden:

- Allgemein: Der Port kann alle Funktionen unterstützen, die in der IEEE 802.1q-Spezifikation definiert sind. Bei der Schnittstelle kann es sich um ein getaggttes oder nicht getaggttes Mitglied eines oder mehrerer VLANs handeln.
- Zugriff: Auf der Schnittstelle kann nur ein VLAN konfiguriert sein, und es kann nur ein VLAN übertragen werden.
- Trunk: Kann den Datenverkehr mehrerer VLANs über eine einzige Verbindung übertragen und ermöglicht die Erweiterung von VLANs über das Netzwerk.
- Dot1p-Tunnel: versetzt die Schnittstelle in den QinQ-Modus. So kann der Benutzer seine eigenen VLAN-Anordnungen (PVID) im Anbieternetzwerk verwenden. Der Switch befindet sich im QinQ-Modus, wenn er über einen oder mehrere dot1p-tunnel-Ports verfügt.

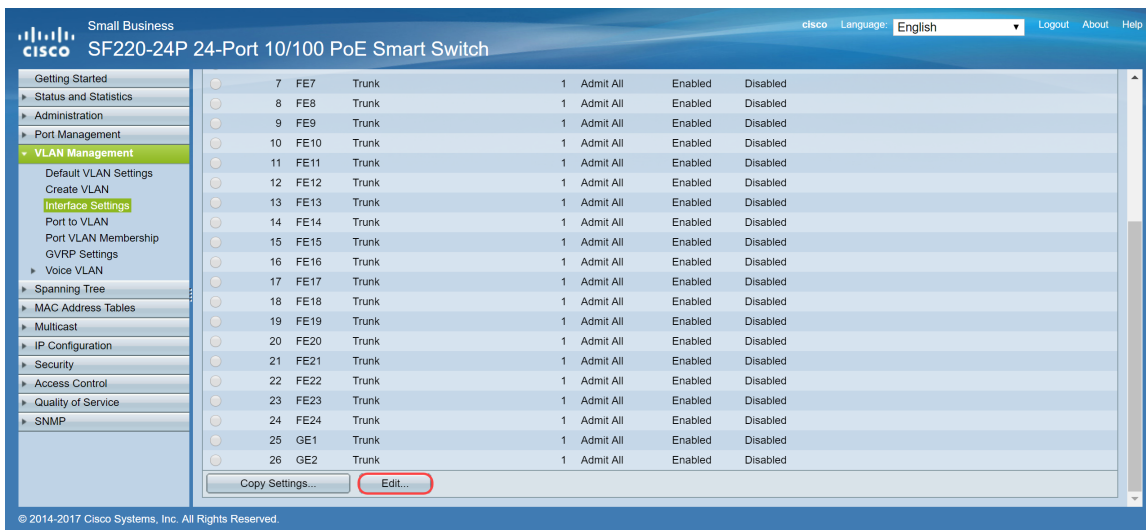
Schritt 1: Melden Sie sich bei der Webkonfiguration an, und navigieren Sie zu **VLAN Management > Interface Settings**.



Schritt 2: Wählen Sie den Schnittstellenmodus für das VLAN aus. In diesem Beispiel wird der Raspberry Pi (Port: FE3) als Access-Port konfiguriert.



Schritt 3: Klicken Sie dann auf **Bearbeiten...** um die Schnittstelle zu bearbeiten.



Schritt 4: Wählen Sie im Feld *Interface VLAN Mode (Schnittstellen-VLAN-Modus)* **Access (Zugriff)** aus, um die Schnittstelle als nicht markiertes Mitglied eines einzelnen VLANs zu konfigurieren.

The screenshot shows a web browser window titled 'Edit Interface Settings - Google Chrome'. The address bar displays 'https://192.168.1.100/html/vlan\_intfEdit.html?port=FE3'. The main content area contains the following settings:

- Interface:  Port FE3  LAG 1
- Interface VLAN Mode:  General,  Access,  Trunk,  Dot1q-Tunnel (The switch will be in Q-in-Q mode when it has one or more Dot1q-Tunnel ports)
- \* Administrative PVID: 1 (Range: 1 - 4094, Default: 1)
- Frame Type:  Admit All,  Admit Tagged Only,  Admit Untagged Only
- Ingress Filtering:  Enable
- Uplink:  Enable
- TPID: 0x8100

At the bottom, there are two buttons: 'Apply' and 'Close'.

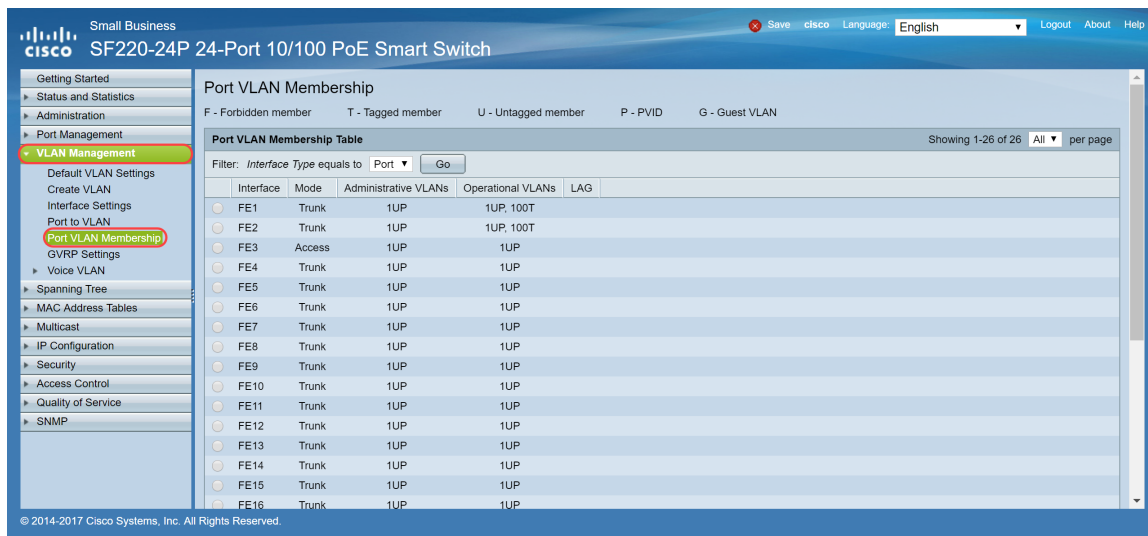
Schritt 5: Klicken Sie auf **Apply**, um Ihre Einstellungen zu speichern.

This screenshot is identical to the previous one, showing the same configuration page. The 'Apply' button at the bottom left is now highlighted with a red circle, indicating the next step in the process.

## Konfigurieren der Port-VLAN-Zugehörigkeit auf dem Switch

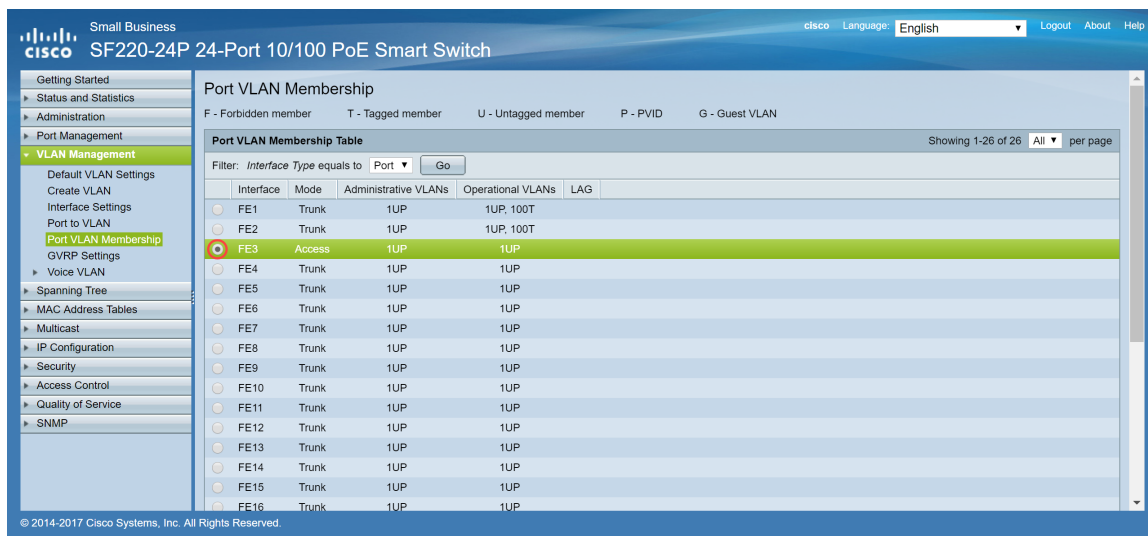
Nachdem die VLANs erstellt wurden, müssen Sie den Ports, die Sie anschließen möchten, VLANs zuweisen.

Schritt 1: Melden Sie sich bei der Webkonfiguration an, und navigieren Sie zu **VLAN Management** > **Port VLAN Membership**.



Schritt 2: Wählen Sie in der *Table "Port VLAN Membership"* die Schnittstelle aus, die Sie für die VLAN-Mitgliedschaft konfigurieren möchten. In diesem Beispiel wird der Raspberry Pi (Port: FE3) für VLAN 100 konfiguriert.

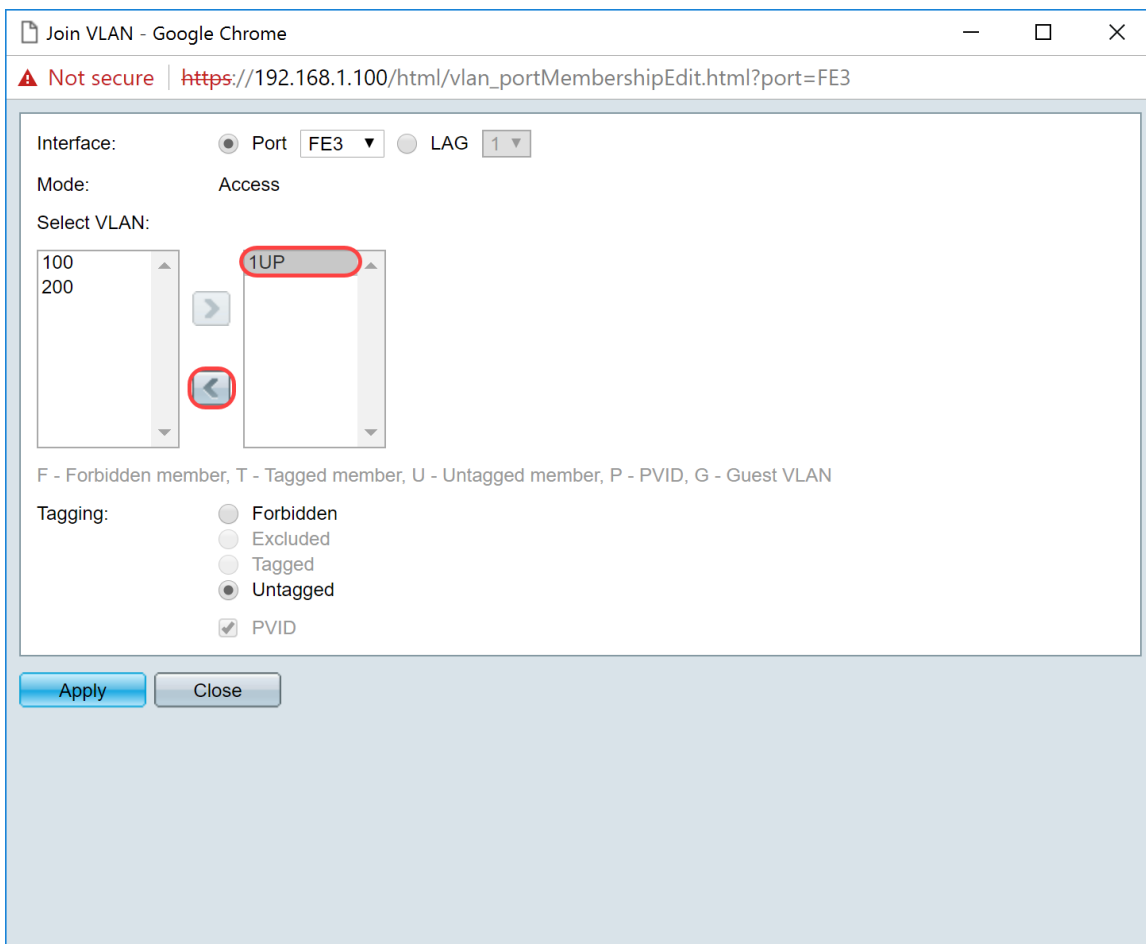
**Hinweis:** Alle Sprachgeräte werden bereits für das Sprach-VLAN konfiguriert, das Sie im Abschnitt [Einrichten von Sprach-VLAN auf dem Switch](#) ausgewählt haben.



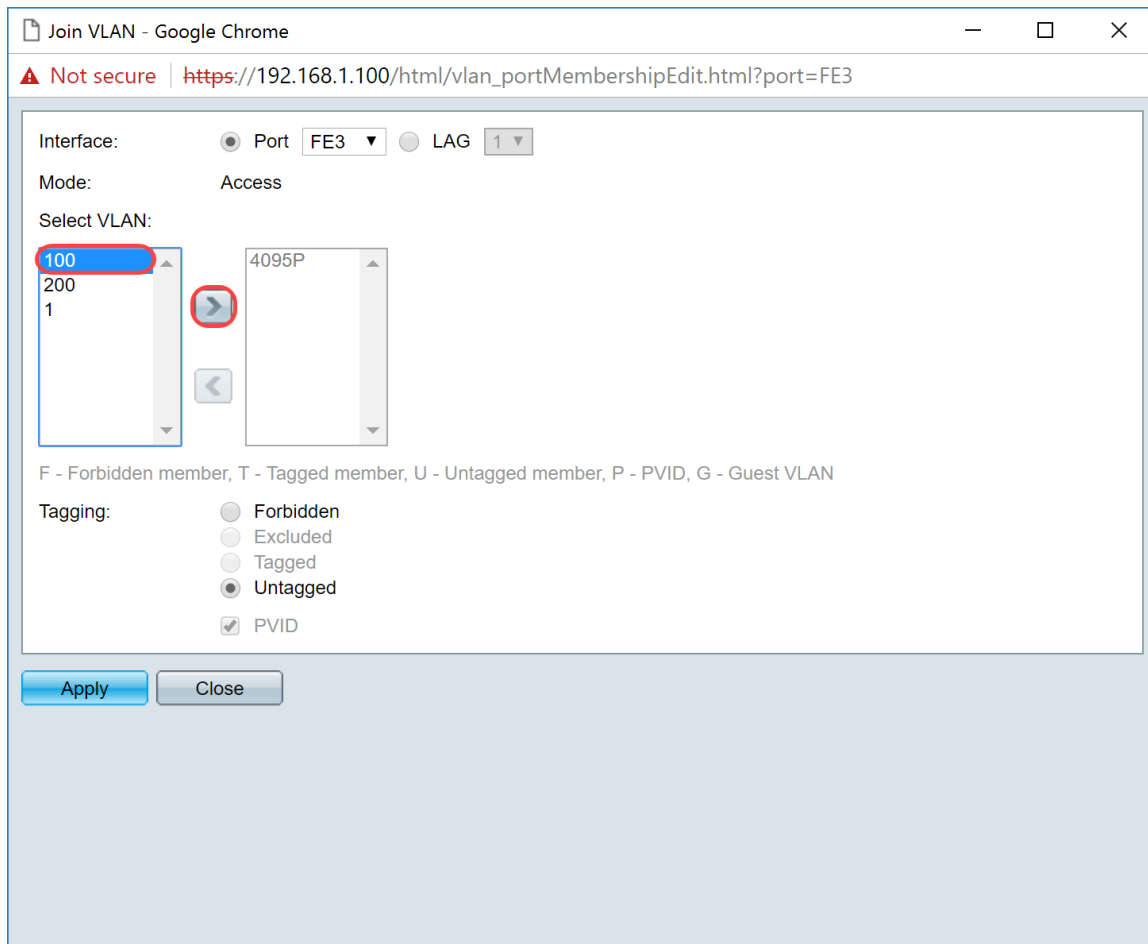
Schritt 3: Klicken Sie auf **Join VLAN...** um den Port zu ändern, den Sie VLANs konfigurieren möchten.



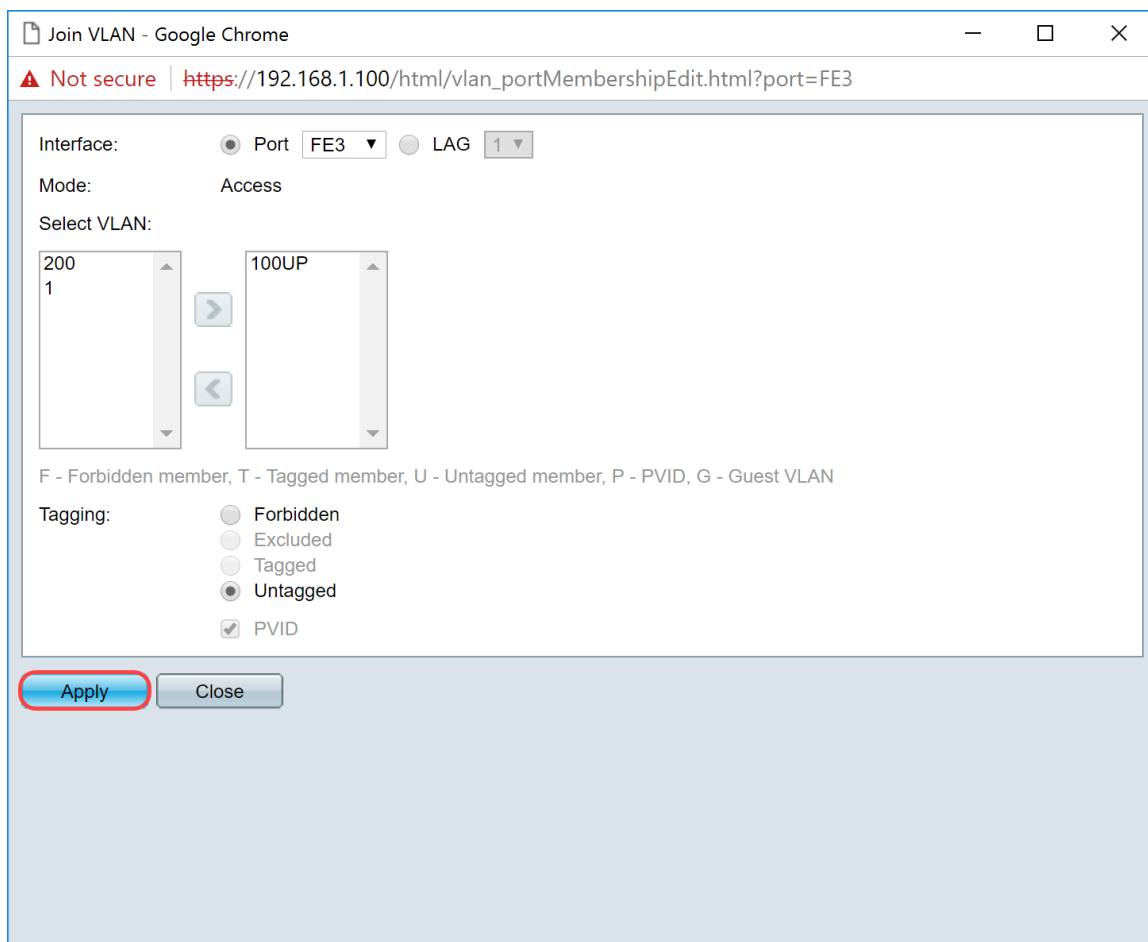
Schritt 4: Wählen Sie **1UP** aus, und klicken Sie auf den Befehl <, um VLAN 1 aus der Schnittstelle im Abschnitt *Select VLAN (VLAN auswählen)* zu entfernen. Nur ein nicht markiertes VLAN kann der Schnittstelle hinzugefügt werden, wenn es sich um einen Zugriffspport handelt.



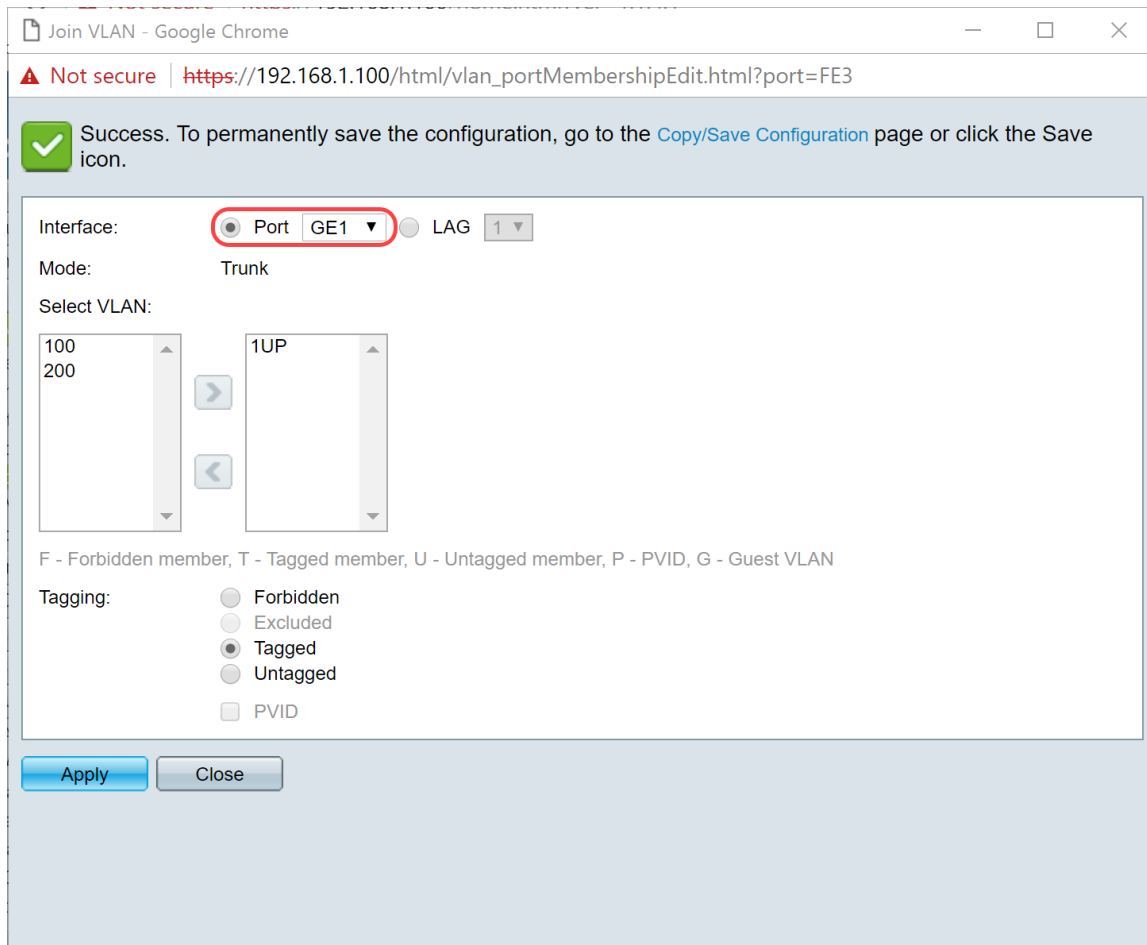
Schritt 5: Wählen Sie **100** aus, und klicken Sie auf >, um der Schnittstelle das nicht gekennzeichnete VLAN hinzuzufügen.



Schritt 6: Klicken Sie auf **Apply**, um Ihre Einstellungen zu speichern.



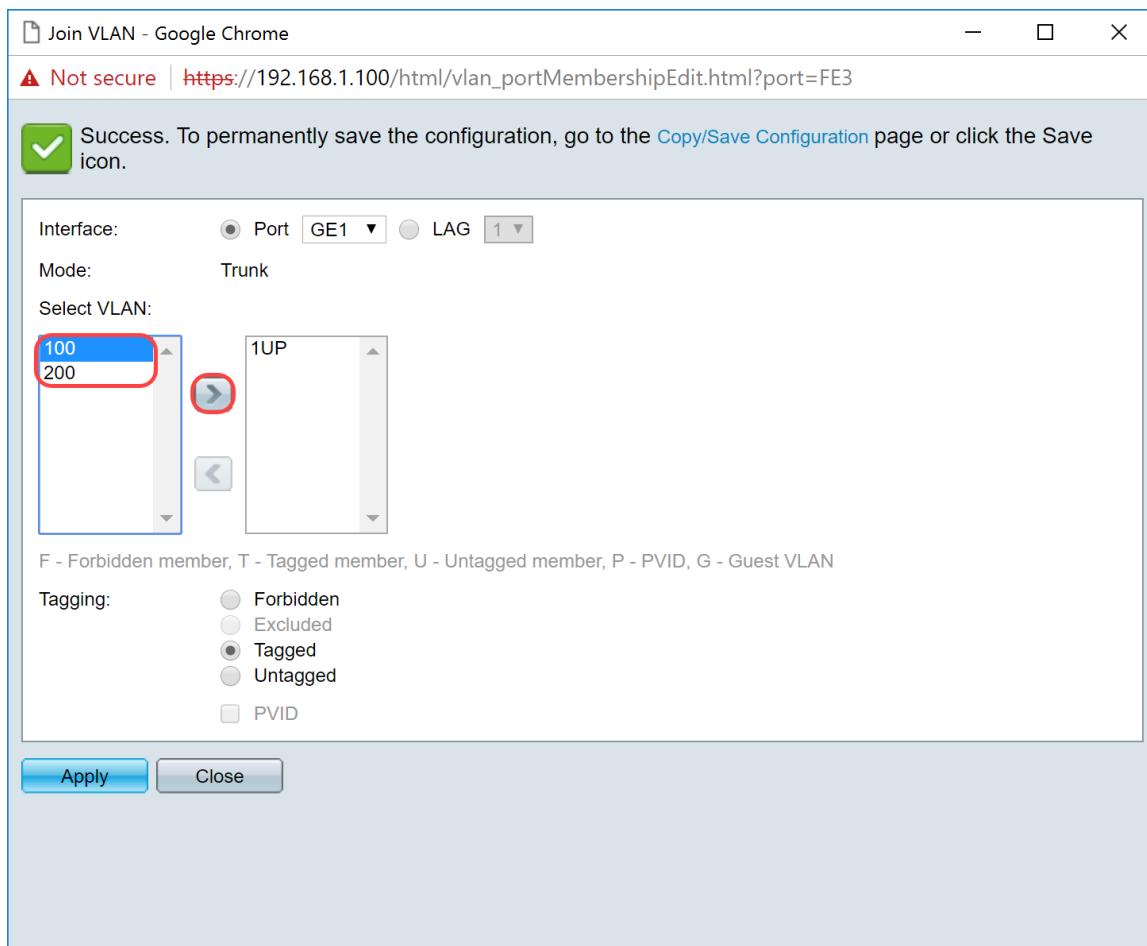
Schritt 7. Wählen Sie im Feld Interface (*Schnittstelle*) den Schnittstellenport aus, der mit dem Router verbunden ist. In diesem Beispiel ist Port GE1 ausgewählt.



The screenshot shows a web browser window titled "Join VLAN - Google Chrome" with the URL "https://192.168.1.100/html/vlan\_portMembershipEdit.html?port=FE3". A success message at the top states: "Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon." Below this, the configuration form is displayed. The "Interface:" field has "Port GE1" selected and is circled in red. The "Mode:" is set to "Trunk". The "Select VLAN:" section contains two lists: the left list has "100" and "200" selected, and the right list has "1UP" selected. Below the lists are "Apply" and "Close" buttons. A legend at the bottom explains the tagging options: F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN. The "Tagging:" section has radio buttons for "Forbidden", "Excluded", "Tagged" (which is selected), "Untagged", and a checkbox for "PVID".

Schritt 8: Wählen Sie das VLAN aus, das der ausgewählten Schnittstelle hinzugefügt werden soll, und klicken Sie dann im Abschnitt *Select VLAN (VLAN auswählen) auf >*, um das VLAN hinzuzufügen. In diesem Beispiel werden VLAN **100** und **200** ausgewählt.





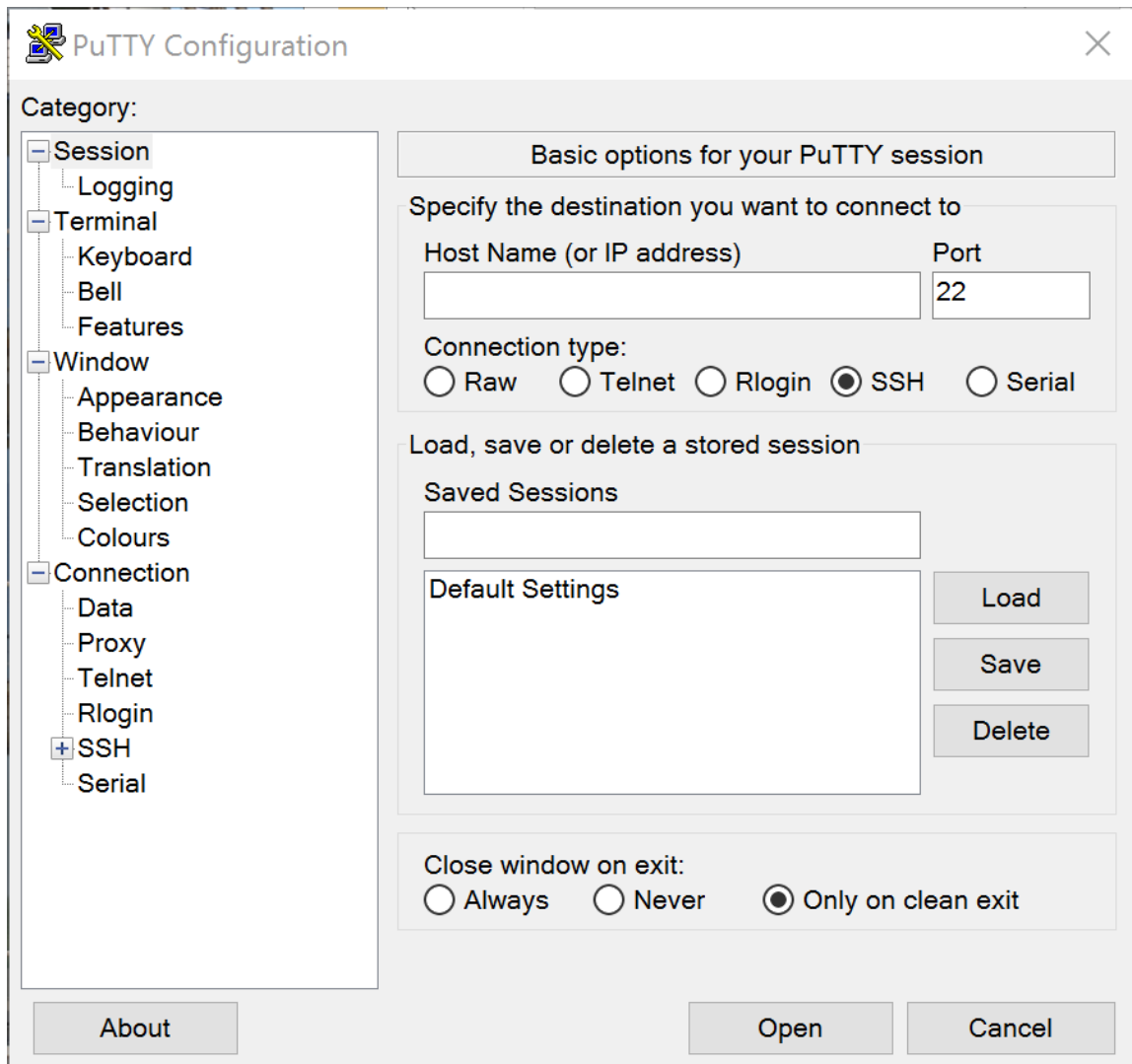
Schritt 9. Klicken Sie auf **Apply**, um Ihre Einstellungen zu speichern.

**Hinweis:** Möglicherweise ist ein Neustart der IP-Telefone erforderlich, damit die IP-Adresse in das richtige Subnetz geändert wird.

## Änderung der IP-Adresse von Raspberry Pi in einem anderen Subnetz

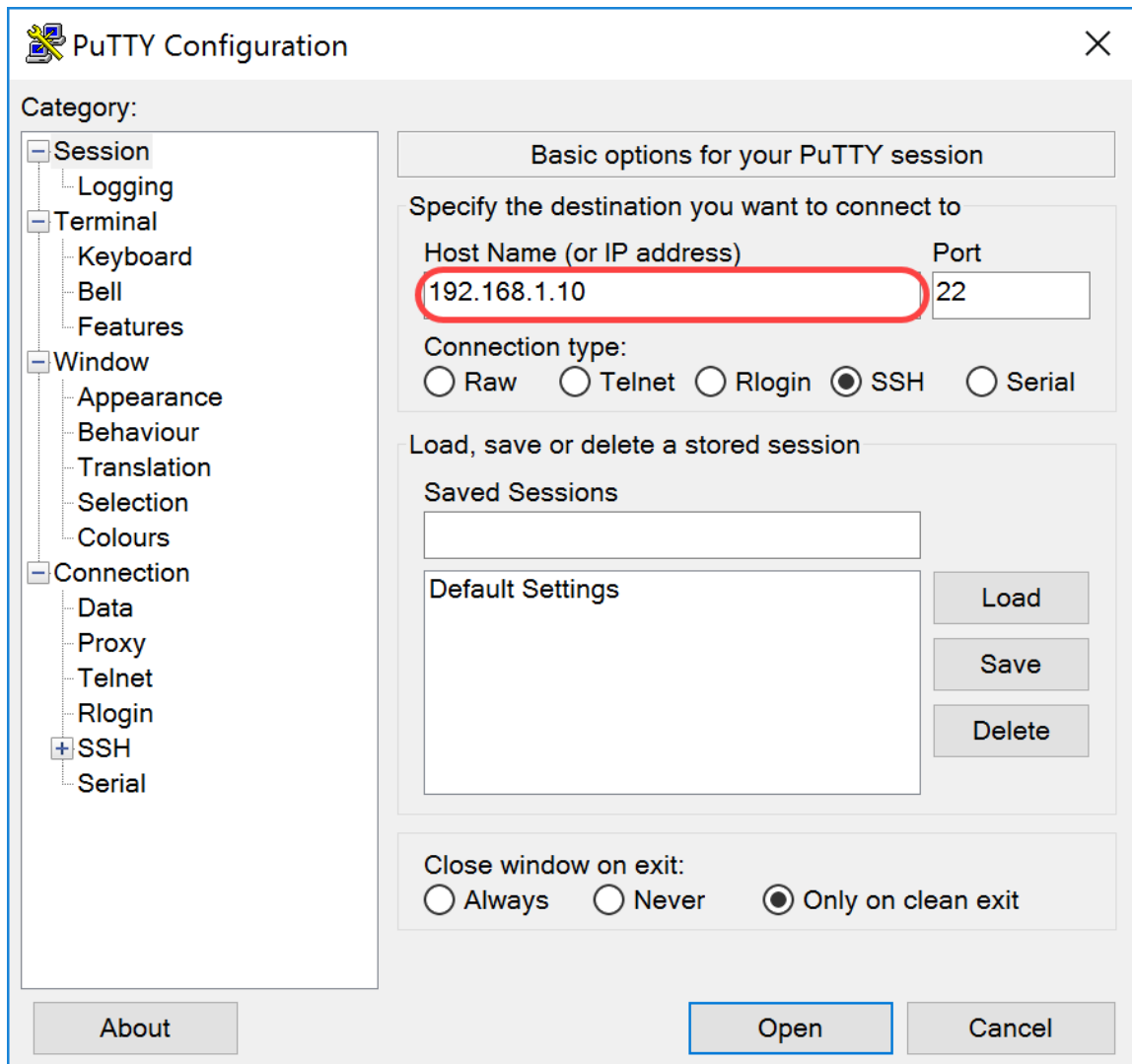
Schritt 1: Verbinden Sie Ihren Raspberry Pi mit Secure Shell (SSH) oder schließen Sie Ihren Raspberry Pi an einen Computermonitor an. In diesem Beispiel wird SSH verwendet, um den Raspberry Pi zu konfigurieren.

**Hinweis:** Der Port am Switch für Ihren Computer/Laptop muss sich im selben VLAN wie der Raspberry Pi befinden und als Zugriffsport konfiguriert werden, wenn Sie die Schnittstelleneinstellungen einrichten. Siehe [Konfigurieren der Schnittstelleneinstellungen für einen Switch](#) und [Konfigurieren der Port-VLAN-Zugehörigkeit im Abschnitt Switch](#) in diesem Artikel, um die Details zu überprüfen. Stellen Sie sicher, dass Ihre IP-Adresse im gleichen Netzwerk wie Ihr Raspberry Pi ist, um SSH in sie zu integrieren. Wenn sich Ihr Gerät nicht im selben Netzwerk wie der Raspberry Pi befindet, verwenden Sie eine statische IP-Adresse und ändern Sie Ihre IP-Adresse manuell in das gleiche Netzwerk. Alternativ können Sie den Befehl **ipconfig /release** und **ipconfig/renew** in der Eingabeaufforderung eingeben, um eine neue IP-Adresse zu erhalten. SSH-Clients können je nach Betriebssystem variieren. In diesem Beispiel wurde PuTTY verwendet, um SSH in den Raspberry Pi einzufügen. Weitere Informationen zu SSH erhalten Sie [hier](#).

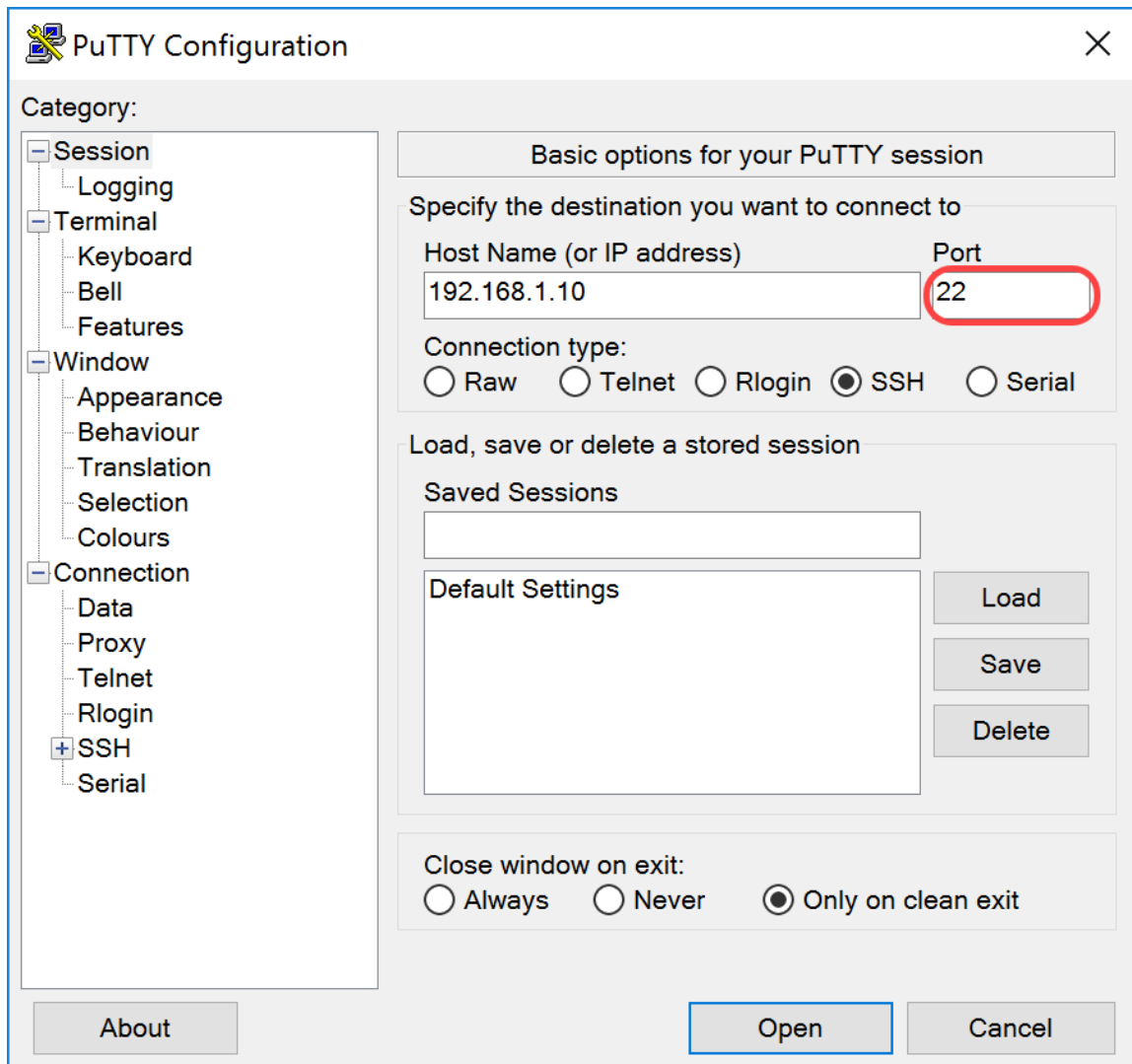


Schritt 2: Geben Sie die IP-Adresse Ihres Raspberry Pi in das Feld *Hostname (oder IP-Adresse)* ein. In diesem Beispiel wird 192.168.1.10 eingegeben.

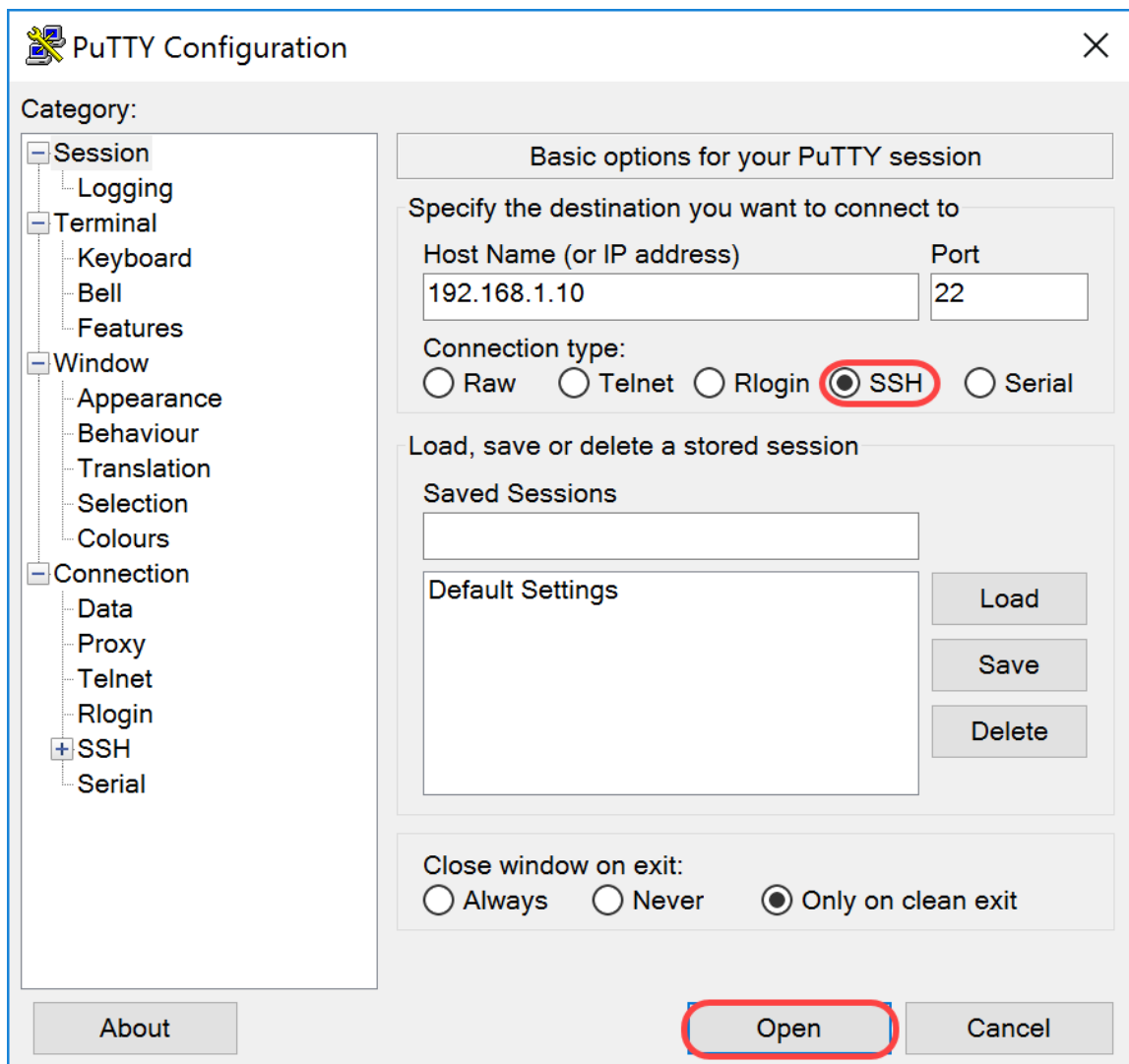
**Hinweis:** Sie können die DHCP-Tabelle im Router verwenden, um die Adresse des Raspberry Pi zu finden. In diesem Dokument wurde dieser Raspberry Pi so vorkonfiguriert, dass er eine statische IP-Adresse hat.



Schritt 3: Geben Sie **22** als Portnummer in das Feld *Port* ein. Port 22 ist der Standardport für das SSH-Protokoll.

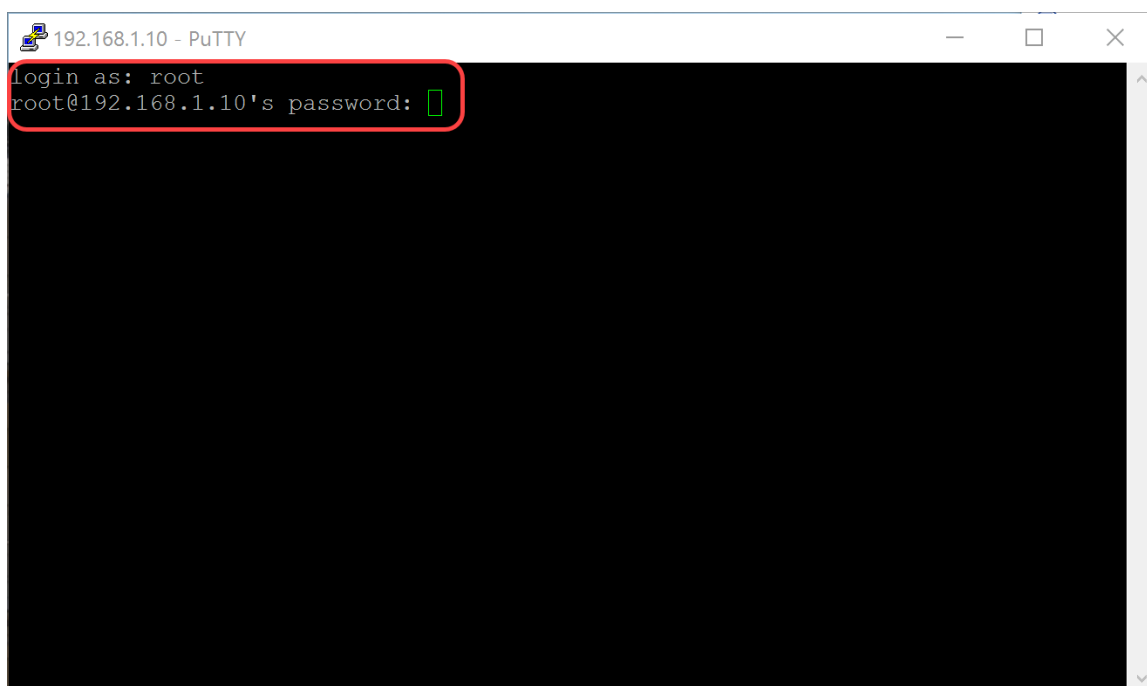


Schritt 4: Klicken Sie im Abschnitt *Verbindungstyp* auf das Optionsfeld **SSH**, um SSH als Methode für die Verbindung mit dem Switch auszuwählen. Klicken Sie dann auf **Öffnen**, um die Sitzung zu starten.



Schritt 5: Geben Sie den Benutzernamen und das Kennwort des RasPBX-Systems in das Feld *Anmelden als* und *Kennwort ein*.

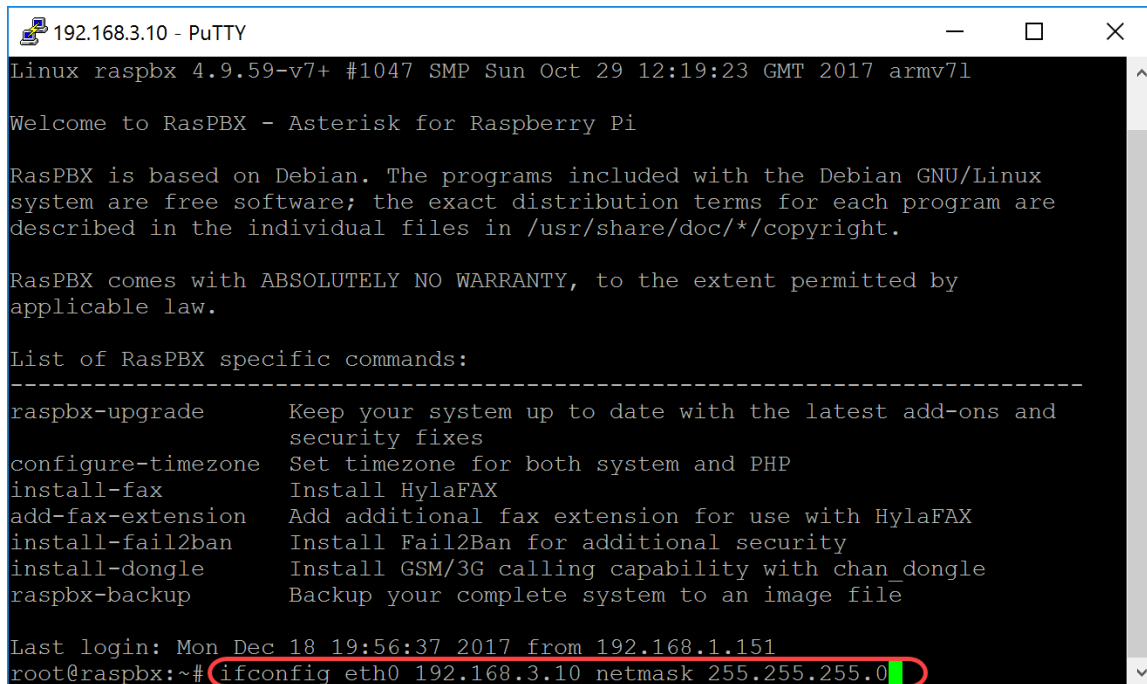
**Hinweis:** Standardbenutzer: **root** und Standardkennwort: **Himbeere**



Schritt 6: Um die IP-Adresse Ihres Ethernet in eine statische IP-Adresse zu ändern, geben Sie `ifconfig eth0 [IP-Adresse] netmask [Netzmaske]` ein. In diesem Beispiel verwenden wir 192.168.3.10 und die Netzmaske 255.255.255.0.

```
ifconfig eth0 192.168.3.10 netmask 255.255.255.0
```

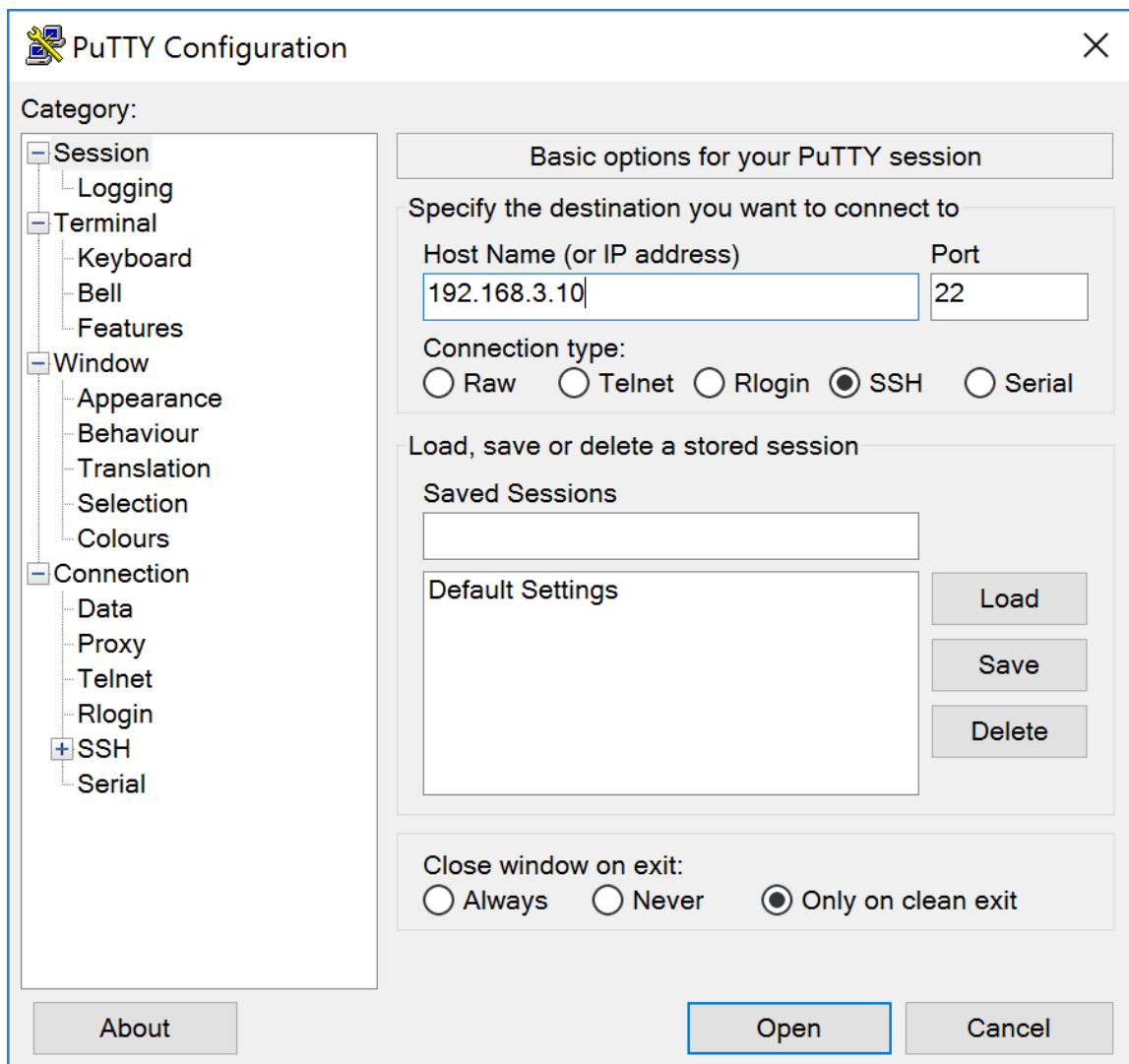
**Hinweis:** Wenn Sie die IP-Adresse ändern, wird die Verbindung zur Sitzung getrennt. Um sich wieder mit dem Raspberry Pi zu verbinden, muss sich Ihr Computer/Laptop im gleichen Subnetz wie der Raspberry Pi befinden (192.168.3.x).



```
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
```

Schritt 7. Stellen Sie mithilfe der statischen IP-Adresse, die in Schritt 6 konfiguriert wurde, eine Verbindung zu Ihrem Raspberry Pi her. In diesem Beispiel verwenden wir 192.168.3.10, um eine Verbindung herzustellen.

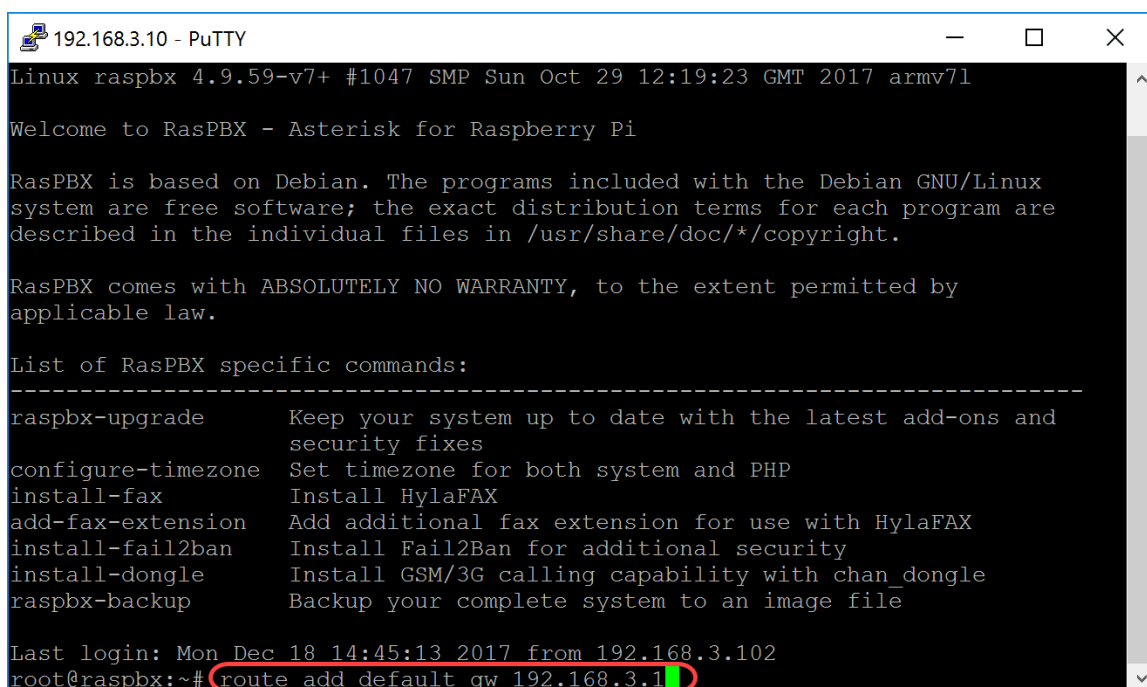
**Hinweis:** Stellen Sie sicher, dass sich Ihr Computer/Laptop im gleichen Subnetz wie der Raspberry Pi und das VLAN befindet. Wenn sich Ihr Computer/Laptop im selben VLAN wie der Raspberry Pi befindet und Sie nicht über die richtige IP-Adresse verfügen, können Sie zu Ihrer Eingabeaufforderung wechseln und **ipconfig /release** und dann **ipconfig /renew** eingeben, um eine neue IP-Adresse anzufordern, oder Sie können Ihr Gerät so konfigurieren, dass es eine statische IP-Adresse in den Ethernet-Eigenschaften hat.



Schritt 8: Geben Sie in der Befehlszeile `route add default gw [Router-IP-Adresse des Subnetzes]` ein, um ein Standard-Gateway hinzuzufügen.

**Hinweis:** Sie können die Routing-Tabelle mithilfe der **Befehlsroute** anzeigen.

```
route add default gw 192.168.3.1
```



## **Schlussfolgerung**

Sie sollten nun erfolgreich ein einfaches Sprachnetzwerk eingerichtet haben. Um dies zu überprüfen, nehmen Sie eines der SPA/MPP-Telefone, und Sie sollten einen Wählton hören. In diesem Dokument hat eines der SPA/MPP-Telefone die Durchwahl 1002 und das andere die Durchwahl 1003. Sie sollten in der Lage sein, die Durchwahl 1003 anzurufen, wenn Sie die SPA-/MPP-Durchwahl 1002 verwenden.



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.