

# Hoe maak je een basis spraaknetwerk met behulp van Raspberry Pi

## Doel

Dit document geeft instructies hoe u een basisspraaknetwerk met Raspberry Pi als communicatieserver kunt configureren met behulp van Asterisks. Virtual Local Area Network (VLAN) en Quality of Service (QoS) worden gebruikt om prioriteit aan verkeer te geven door spraak- en gegevensverkeer te scheiden. Het doel van dit netwerk is om interne tests op te zetten. Deze tests zullen u helpen om uw netwerk geschikt te schrapen, zien of hebt u genoeg bandbreedte voor het stemvolume u, verwacht en een andere mogelijke geschil tussen materiaal vindt. Het kan ook helpen bepalen of u het lokaal of in de cloud wilt hosten. Zodra een bedrijf een bepaalde grootte heeft bereikt, kunnen zij er de voorkeur aan geven om hun eigen lokale gesprekscontroller te hebben zoals PBX, of IP PBX. Dit zou interne gesprekken efficiënter maken omdat gesprekken tussen telefoons binnen het bedrijf niet uit het gebouw en dan weer terug naar binnen hoeven te worden gerouteerd.

**Belangrijke opmerking:** De Raspberry Plus is geen door Cisco ondersteund product, dit document is alleen voor ondersteuningsdoeleinden en is geen oplossingsdocument.

## Inleiding

Om een bedrijf effectief zaken te laten doen, moeten werknemers toegang hebben tot een spraaknetwerk. Dit vergemakkelijkt de communicatie tussen werknemers en hun klanten en stelt werknemers in staat om intern te communiceren. Elke werknemer kan worden voorzien van een vaste telefoon en/of een mobiele telefoon, maar dit kan vrij duur worden. Bedrijven kiezen er vaak voor om een spraaknetwerk in te stellen dat in plaats daarvan Voice over Internet Protocol (VoIP) gebruikt.

Met de VoIP-technologie kunt u het internet gebruiken om telefoongesprekken te maken en te ontvangen vanaf elke locatie, naar elke locatie in de wereld met minimale of zelfs minimale kosten voor lange afstanden. Dit kan worden gebruikt op elk apparaat dat het internet gebruikt.

VoIP kan een bedrijf geld besparen terwijl de productiviteit, communicatie en klanttevredenheid toenemen. Werknemers kunnen gebruik maken van verschillende functies zoals oproeproutering, muziek in wachtstand en geïntegreerde voicemail.

Een veel voorkomende functie van VoIP die veel bedrijven gebruiken is oproeproutering, ook wel bekend als een automatische gespreksverdeler. De oproeproutering verdeelt inkomende oproepen naar de volgende beschikbare agent in plaats van ze naar voicemail te sturen. Dit waarborgt dat de vraag van de klant zo efficiënt mogelijk zal worden beantwoord. Na kantooruren kan u rechtstreeks naar een voicemail bellen.

Het toevoegen van gebruikers en upgradering van functies is een eenvoudig proces, dat handig is wanneer uw bedrijf zich uitbreidt of uw behoeften veranderen. In tegenstelling tot een traditioneel telefoonsysteem, hoeft er geen dure bedrading te worden uitgevoerd.

Om een VoIP-netwerk in te stellen, hebt u opties om te overwegen. U kunt een VoIP-service voor uw eigen telefoonsysteem hosten met KSU, KSU-less, Private Branch Exchange (PBX) of een ander VoIP-systeem.

Uw budget, aantal medewerkers en locaties, beschikbare diensten in uw regio en groei van het bedrijf moeten allemaal in aanmerking worden genomen. Ook training en extra apparatuur, zoals headsets,

kunnen nodig zijn. VoIP kan uw gegevensgebruik verhogen en u kunt uw bandbreedte moeten verhogen om rekening te houden met het spraaknetwerkverkeer.

U moet ook een back-up plannen, "Plan B", voor het geval uw netwerk ooit uitvalt. Als u de stroom verliest, maakt uw VoIP-systeem geen verbinding. Deze redundantie moet worden geïmplementeerd om uw telefoonservices onmiddellijk te herstellen en onderbreking van uw bedrijfsproductiviteit te voorkomen.

In dit artikel, zullen wij ons eigen telefoonsysteem gebruiken die Asterisk, een PBX op een Raspberry Pi gebruiken.

**Opmerking:** zodra u deze stappen hebt voltooid en ook de mogelijkheid wilt om uit uw interne netwerk te bellen, moet u een Internet Telephony Service Provider (ITSP) kiezen.

## Definities

Met een Virtual Local Area Network (VLAN) kunt u een Local Area Network (LAN) logisch segmenteren in verschillende broadcastdomeinen. In scenario's waarbij gevoelige gegevens via een netwerk kunnen worden doorgegeven, kunnen VLAN's worden opgezet om data beter te beveiligen door een broadcast aan een specifiek VLAN toe te wijzen. Gebruikers op een specifiek VLAN zijn de enige die toegang hebben tot gegevens over dat VLAN en deze kunnen manipuleren. VLAN's kunnen ook worden gebruikt om prestaties te verbeteren door de behoefte te verminderen om broadcast en multicast pakketten naar onnodige bestemmingen te verzenden.

Alle poorten worden standaard aan VLAN 1 toegewezen. Nadat u verschillende VLAN's hebt ingesteld, dient u elke poort handmatig aan het juiste VLAN toe te wijzen.

Elk VLAN moet worden geconfigureerd met een unieke VLAN-id (VID) met een waarde van 1 tot 4094. Het apparaat reserveert VID 4095 als de verwerping VLAN. Alle pakketten die geclassificeerd zijn in de Discard VLAN worden bij het binnenvaren van de haven vernietigd en worden niet doorgestuurd naar een poort.

**Met Quality of Service (QoS)** kunt u prioriteit geven aan verkeer voor verschillende toepassingen, gebruikers of gegevensstromen. Het kan ook worden gebruikt om prestaties op een bepaald niveau te garanderen, waardoor de QoS voor de klant wordt beïnvloed. QoS wordt over het algemeen beïnvloed door de volgende factoren: jitter, latency en pakketverlies. Meestal wordt video of VoIP prioriteit gegeven omdat ze het meest worden beïnvloed door QoS.

**Private Branch Exchange (PBX)** is een telefoonschakelsysteem dat inkomende en uitgaande gesprekken voor interne gebruikers in een bedrijf beheert. Een PBX is aangesloten op het openbare telefoonsysteem en leidt automatisch inkomende gesprekken naar specifieke extensies. Het deelt en beheert ook meerdere lijnen. Een typisch PBX-systeem voor kleine bedrijven bestaat uit externe en interne telefoonlijnen, een computerserver die gespreksswitching en routing beheert en een console voor handmatige bediening.

Een **IP PBX** kan alles doen wat een traditionele kleine bedrijf PBX kan doen en meer. Het voert de switching en de aansluiting van VoIP evenals vaste telefoongesprekken uit. Een IP PBX-systeem wordt op een IP-datanetwerk uitgevoerd, waardoor kosten worden bespaard en het netwerkbeheer wordt geminimaliseerd. U kunt IP telefoons, softphones (die geen telefoonhardware voorbij een computer en microfoonhoofdtelefoon vereisen), en vaste telefoons op een IP PBX telefoonsysteem gebruiken.

Een **Raspberry Pi** is een goedkope, kleine, draagbare computer die functioneert als een desktopcomputer.

**Asterisk** is een open source framework dat een computer, zoals een Raspberry Pi, kan maken naar een communicatieserver. Dit stelt u in staat om uw eigen zakelijke PBX-telefoonsysteem te bouwen. In dit artikel gebruikt Asterisk FreePBX als een grafische gebruikersinterface (GUI) die Asterisk controleert en beheert waar u extensies, gebruikers, enz. kunt configureren.

## Toepasselijke apparaten

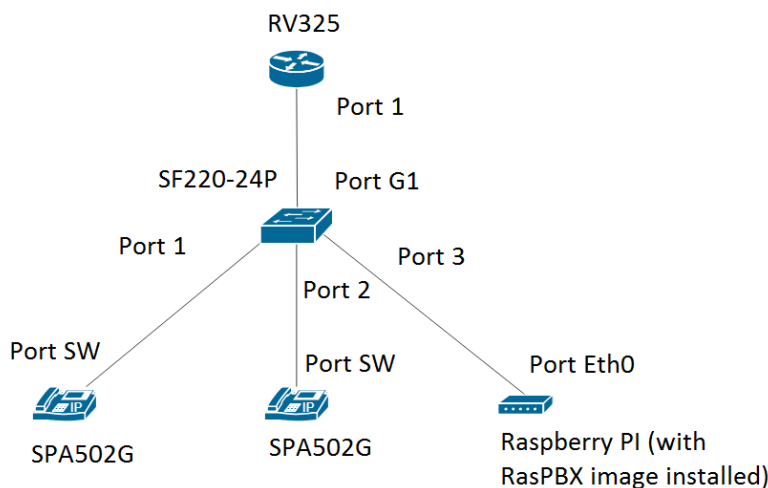
- Router
- Power over Ethernet (PoE) Switch
- Raspberry Pi (Pi 3 B+, Pi 3, Pi 3, B+, B en A modellen)
- 2 of meer Cisco SPA/MPP IP-telefoons

## Softwareversie

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

Om Basic Voice Network te configureren met Raspberry Pi volgt u de onderstaande richtlijn:

### Topologie:



De afbeelding voor de RasPBX staat [hier](#). Deze afbeelding moet worden geïnstalleerd op de Raspberry Pi.

**Opmerking:** In dit document is de Raspberry Pi met de RasPBX afbeelding al ingesteld. Om toegang te krijgen tot de GUI van de Raspberry Pi, typ in <http://raspbx.local> of het IP-adres van de Raspberry Pi in uw browser om de PBX te configureren. De standaard FreePBX login is gebruiker: **admin** wachtwoord: **admin**. Ook was de Raspberry Pi vooraf geconfigureerd om een statisch IP-adres te

hebben.

## Inhoud

1. [VLAN's instellen op de router](#)
2. [SPA/MPP-telefoons configureren](#)
3. [VLAN's op een Switch configureren](#)
4. [Sprak VLAN's op een Switch instellen](#)
5. [Interface-instellingen configureren op een Switch](#)
6. [Port VLAN-lidmaatschap op een Switch configureren](#)
7. [Veranderend Raspberry IP Adres om op een Verschillende Subnet te zijn](#)
8. [Conclusie](#)

## VLAN's instellen op de router

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en navigeer naar **Port Management > VLAN-lidmaatschap**.

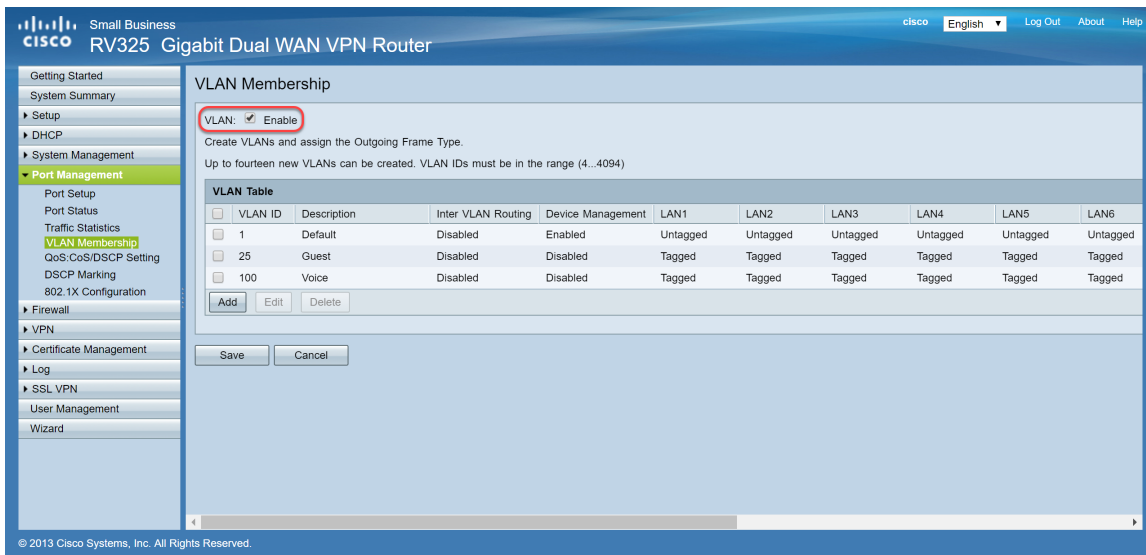
**Opmerking:** dit kan per model verschillen. In dit voorbeeld wordt RV325 gebruikt. Klik [hier](#) voor meer informatie over het openen van de webpagina voor webgebaseerde instellingen.

The screenshot shows the Cisco RV325 web interface. The left sidebar contains a navigation menu with 'Port Management' selected. The main content area is titled 'VLAN Membership' and includes a 'VLAN' checkbox (unchecked) and a 'VLAN Table' with the following data:

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

Buttons for 'Add', 'Edit', 'Delete', 'Save', and 'Cancel' are visible at the bottom of the table.

Stap 2. Schakel het selectievakje **Enable** in om VLAN op de router in te schakelen.

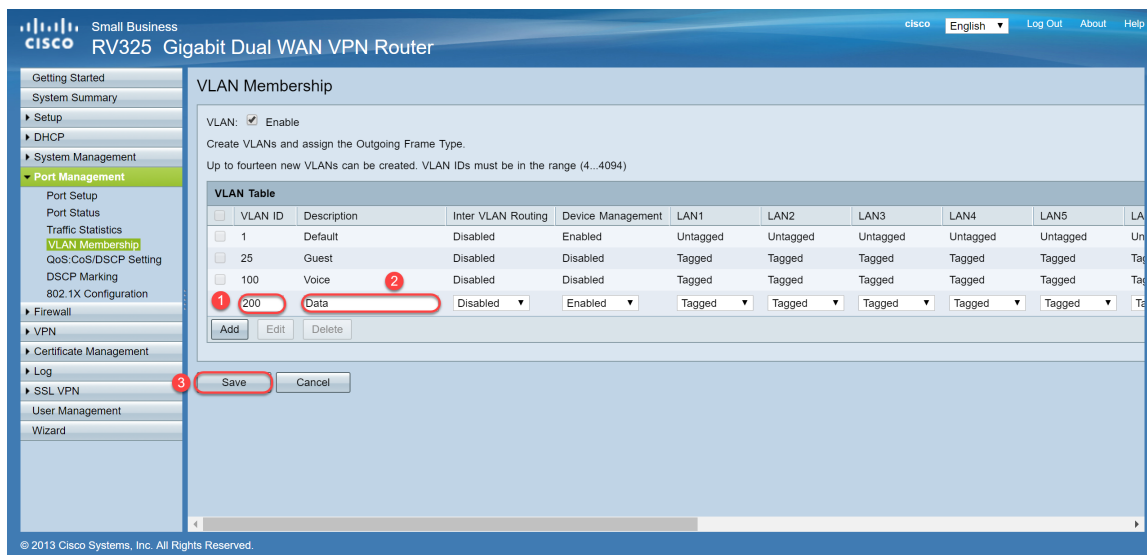


Stap 3. In de sectie *VLAN-tabel* klikt u op **Add** om een nieuwe VLAN-id te maken.

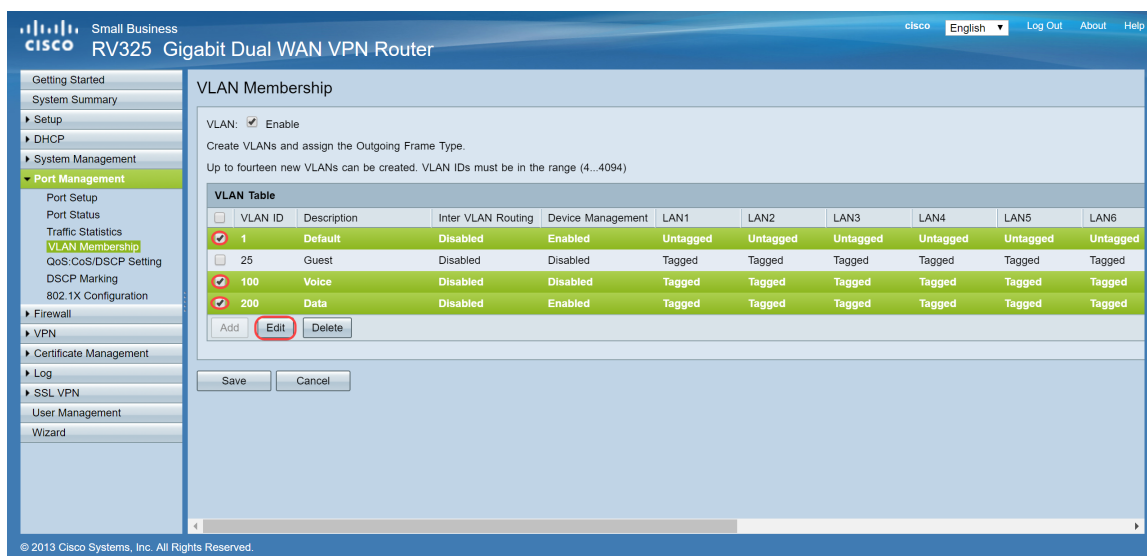


Stap 4. Voer een VLAN-nummer in in het veld *VLAN-id*. VLAN-ID's moeten in bereik 4 tot 4094 liggen. In dit voorbeeld wordt 200 gebruikt voor gegevens als VLAN-id. Typ vervolgens een beschrijving voor het VLAN in het veld *Description*. Er worden gegevens ingevoerd als voorbeeld voor de beschrijving. Klik vervolgens op **Opslaan**.

**Opmerking:** VLAN 100 voor spraak is standaard op deze router gemaakt. Er kunnen maximaal veertien nieuwe VLAN's worden gemaakt.



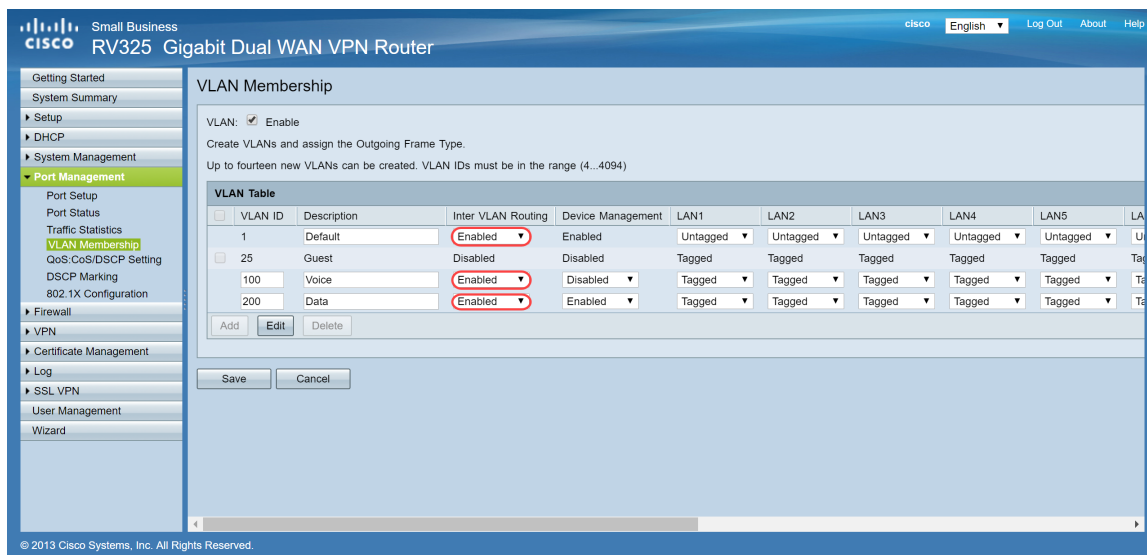
Stap 5. Als u een VLAN wilt bewerken, schakelt u het selectievakje van het juiste VLAN in. In dit voorbeeld worden VLAN 1, 100 en 200 bewerkt. Klik vervolgens op **Bewerken** om de VLAN's te bewerken.



Stap 6. (Optioneel) In de vervolgkeuzelijst *Inter VLAN Routing* kies **Ingeschakeld** of **Uitgeschakeld** om pakketten van het ene VLAN naar een ander VLAN te routeren. Het is handig om dit ingeschakeld te hebben, omdat interne netwerkbeheerders op afstand toegang zullen hebben tot uw apparaten om problemen op te lossen. Dit reduceert de tijd van het voortdurend switches van VLAN's om toegang te krijgen tot de apparaten.

- Uitgeschakeld - Dit geeft aan dat Inter VLAN Routing inactief is
- Ingeschakeld - Het vertegenwoordigt dat Inter VLAN Routing actief is op dit VLAN. Inter VLAN-routing routeert de pakketten alleen onder die VLAN's waarvoor het is ingeschakeld.

**Opmerking:** in dit voorbeeld zullen we Inter VLAN Routing inschakelen voor VLAN-id 1, 100 en 200.



Stap 7. Kies de gewenste optie in de vervolgkeuzelijst voor de LAN poort waarmee u verbonden bent en de instelling moet overeenkomen met de aangesloten poort. Als u verbonden bent met meer dan één poort, moet u voor elke poort waarmee u verbonden bent dezelfde instellingen kiezen. Het gebrek wordt geëtiketteerd maar voor VLAN 1 wordt untagged.

**Opmerking:** als u inter VLAN-routing in stap 6 inschakelt, moet u het VLAN labelen om het verkeer te onderscheiden.

### Gelabeld

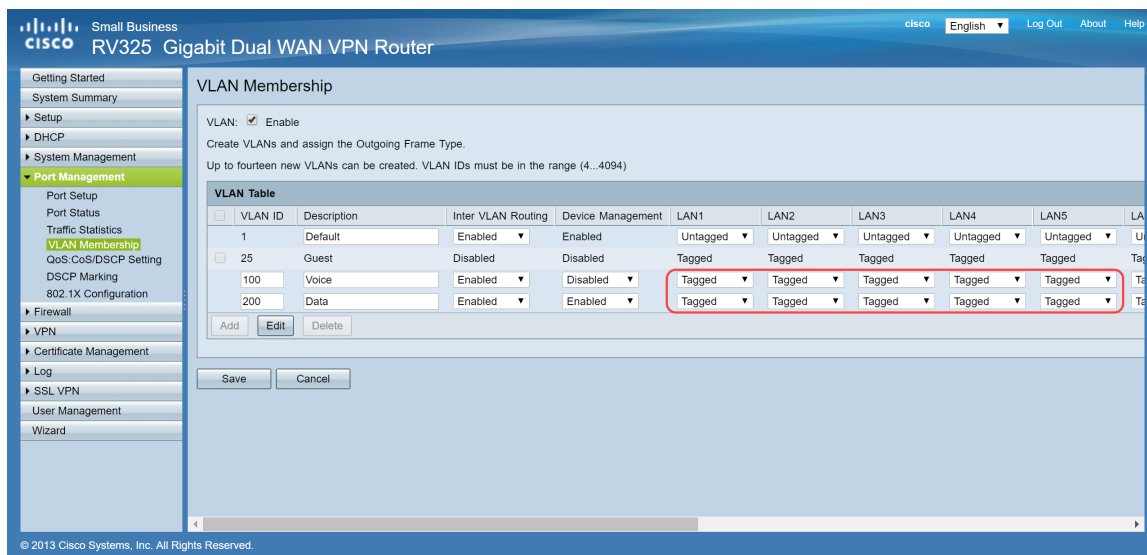
- Vertegenwoordigt dat de vereniging tussen de poort en het VLAN is gelabeld.
- Tagged wordt gebruikt om te bepalen welk VLAN het verkeer via de unieke VLAN-id behoort wanneer er meerdere VLAN's voor dezelfde poort worden gemaakt.

### Ongelabeld

- Vertegenwoordigt dat de vereniging tussen de poort en het VLAN niet is gelabeld.
- Het wordt gebruikt wanneer slechts één VLAN wordt gecreëerd en het verkeer zich van VLAN bewust is. Er kan slechts één VLAN worden gemarkeerd als niet-gelabeld voor elke LAN-poort.
- Als het standaard VLAN zich op de poort bevindt, moet het altijd worden verwijderd, zelfs als de poort meerdere VLAN's heeft.

### Uitgesloten

- Vertegenwoordigt dat de interface geen lid van VLAN is.
- Als u deze optie kiest, is het verkeer uitgeschakeld tussen het VLAN en de poort.



Stap 8. Klik op **Opslaan** om de instellingen op te slaan.

**Opmerking:** op de router kunt u inloggen op het webgebaseerde hulpprogramma en naar **DHCP > DHCP Setup** navigeren om de VLANs te configureren voor een specifiek subnet dat u wilt. In de standaardinstelling zijn de VLANs ingesteld om op een andere subnetverbinding te worden geïnstalleerd.

## SPA/MPP-telefoons configureren

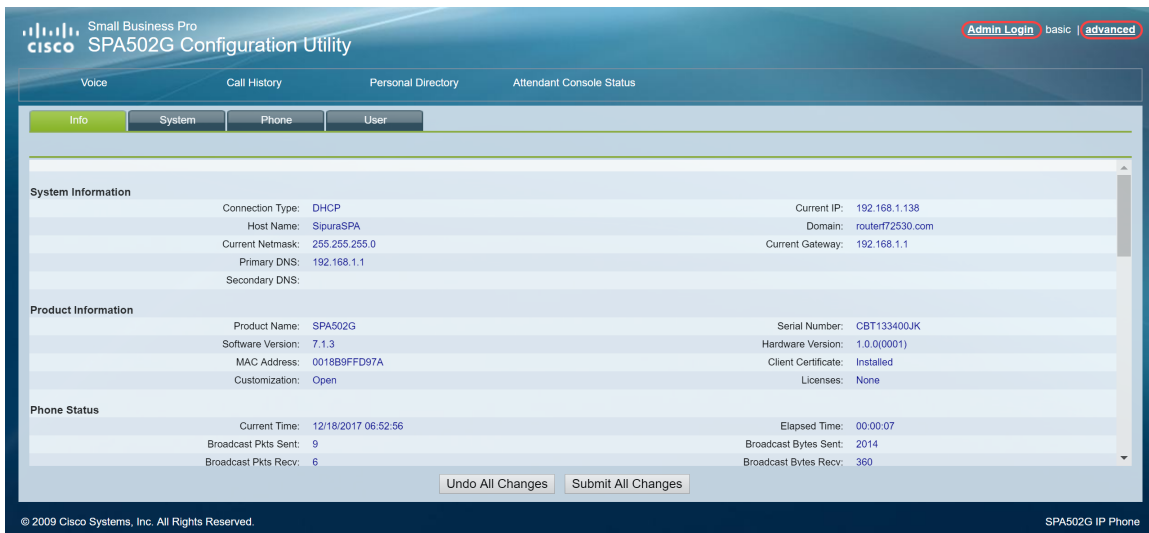
Gebruikers kunnen de telefoons ook configureren om een profiel te halen van een handmatig ingestelde profiellocatie, een locatie gevonden via DHCP-optie 150 of van een Cisco EDOS-server. Het volgende is een voorbeeld van een handconfiguratie.

Stap 1. Voer het IP-adres van de SPA/MPP in op uw browser en navigeer naar **Admin Login** en vervolgens **geavanceerde**.

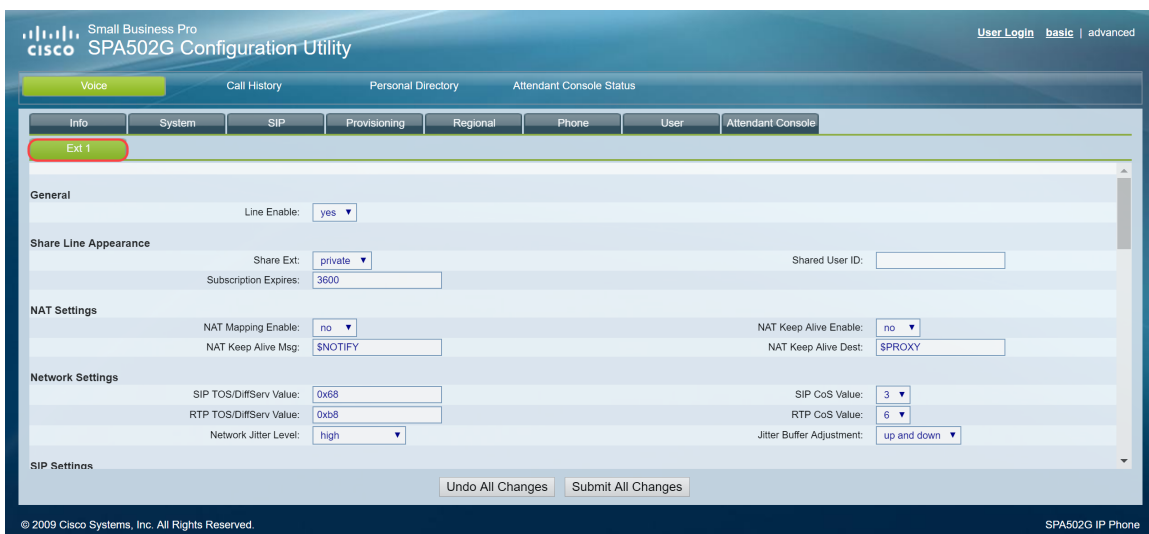
**Opmerking:** de configuratie voor de SPA/MPP-telefoon kan per model verschillen. In dit voorbeeld gebruiken we de SPA502G. Om het IP-adres van uw IP-telefoon te vinden, navigeer naar **DHCP > DHCP Status** op uw router (kan afhankelijk van het model variëren). Een andere manier is om op de knop **Setup** te drukken en op uw Cisco-telefoon naar **Netwerk** te navigeren (menu's en opties kunnen afwijken, afhankelijk van het telefoonmodel).





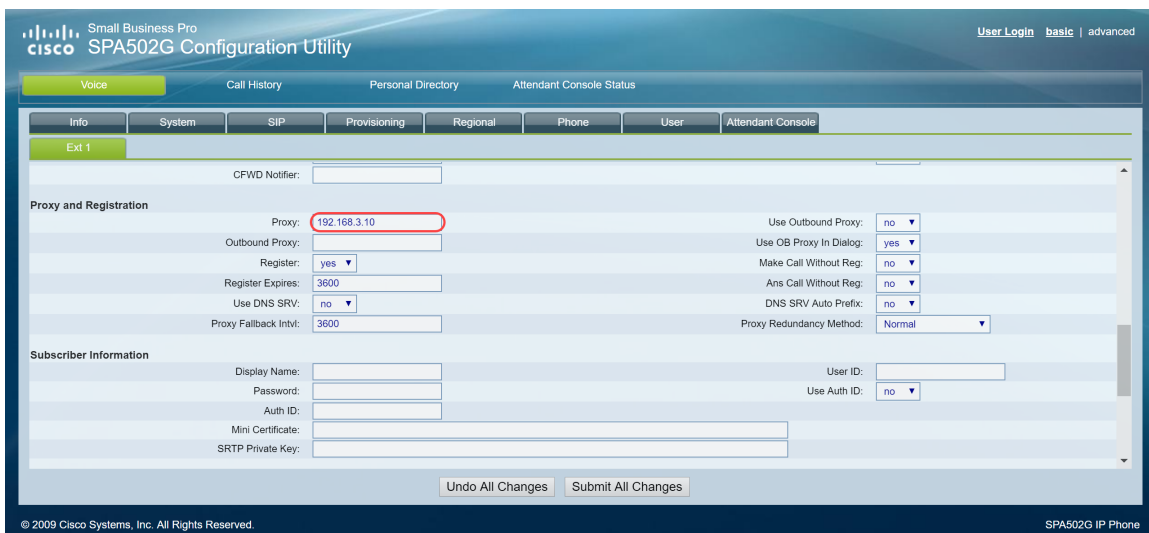


Stap 2. Navigeer naar **Voice > Ext 1**, de extensiepagina opent.



Stap 3. In de sectie *Proxy en registratie* typt u de proxyserver in het veld *Proxy*. In dit voorbeeld zal het adres van de Raspberry Pi (192.168.3.10) worden gebruikt als de proxyserver. VLAN 1000 bevindt zich op het subsystem met 192.168.3.x.

**Opmerking:** U zal het IP-adres van de Raspberry Pi later in dit artikel configureren, als u meer wilt leren klik op de link om te worden doorgestuurd naar die sectie: [Veranderen van het adres van de Raspberry Pi om op een andere Subnet.](#)



Stap 4. Voer onder de *Subscriber Information* de weergavenaam en de gebruikers-ID (uitbreidingsnummer) in voor de gedeelde extensie. In dit voorbeeld gebruiken we de extensie 1003.

**Opmerking:** Extension 1003 is al gemaakt en geconfigureerd op de Raspberry Pi.

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:			
SRTP Private Key:			

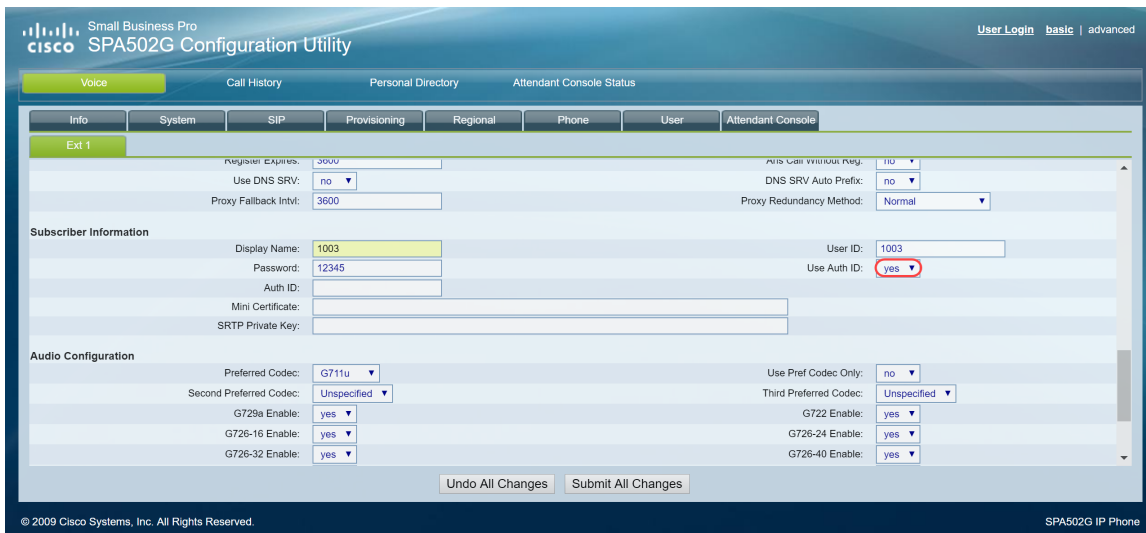
Other visible fields include: Register Expires: 3000, Use DNS SRV: no, Proxy Fallback Intvl: 3600, DNS SRV Auto Prefix: no, Proxy Redundancy Method: Normal, Preferred Codec: G711u, Second Preferred Codec: Unspecified, G729a Enable: yes, G726-16 Enable: yes, G726-32 Enable: yes, Use Pref Codec Only: no, Third Preferred Codec: Unspecified, G722 Enable: yes, G726-24 Enable: yes, G726-40 Enable: yes.

Stap 5. Voer het wachtwoord in van de extensie die u hebt geconfigureerd in de Raspberry Pi extensie sectie. Dit is ook bekend als *Secret* onder de *Edit Extension* Sectie in de Raspberry Pi. In dit voorbeeld is het wachtwoord **12345** gebruikt.

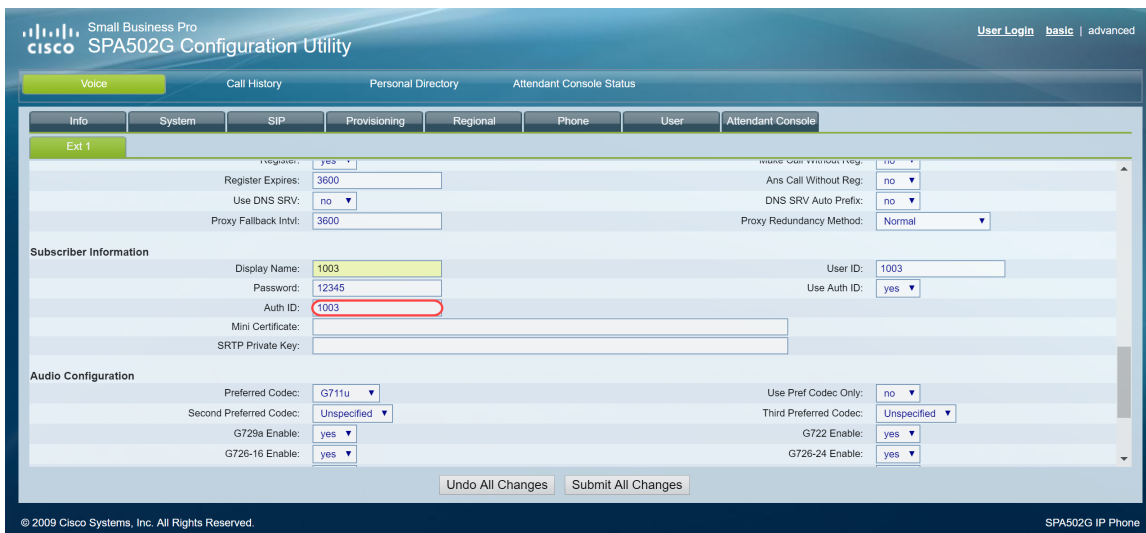
**Opmerking:** Het wachtwoord **12345** is alleen als voorbeeld gebruikt; een complexer wachtwoord wordt aanbevolen.

The screenshot shows the same Cisco SPA502G Configuration Utility interface as in Step 4, but with the 'Password' field in the 'Subscriber Information' section filled with '12345'. The 'Display Name' is still '1003' and the 'User ID' is '1003'. The 'Use Auth ID' is set to 'no'.

Stap 6. Kies de gewenste optie in de vervolgkeuzelijst *Gebruik autorisatie-ID*. De opties zijn **Ja** en **Nee**. Om de verificatie van Session Initiation Protocol (SIP) in te schakelen, waarbij SIP-berichten kunnen worden uitgedaagd om te bepalen of deze zijn geautoriseerd voordat ze kunnen verzenden, kiest u **Ja** in de vervolgkeuzelijst *Auto-ID*. In dit voorbeeld hebben we **Ja** gekozen.



Stap 7. Voer de extensie in die u voor deze telefoon probeert te configureren in het veld *Auto-id*. De verificatie-ID is voor SIP-verificatie.



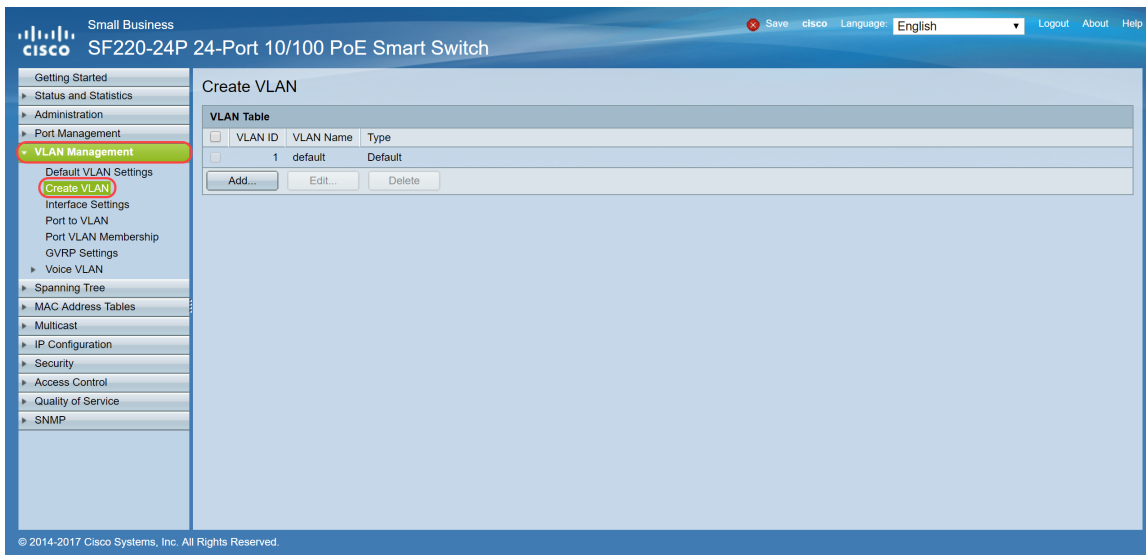
Stap 8. Klik vervolgens op **Alle wijzigingen verzenden**.

**Opmerking:** Ga terug naar Stap 1 van het gedeelte SPA/MPP-telefoons configureren als u meer SPA/MPP-telefoons hebt om te configureren.

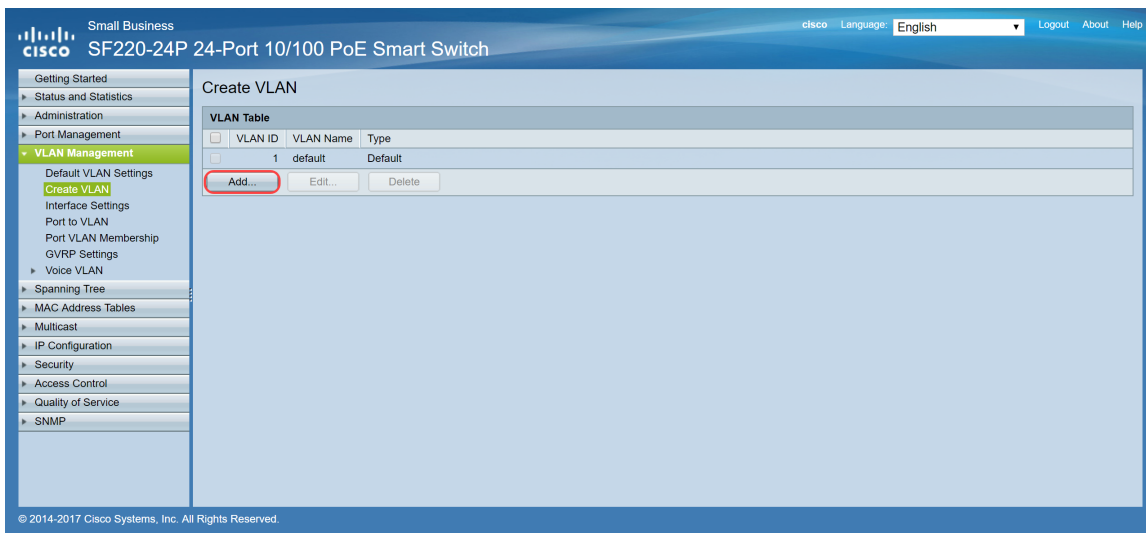
## VLANs op de Switch configureren

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en navigeer naar **VLAN Management > VLAN maken**.

**Opmerking:** de configuratie kan per apparaat verschillen. In dit voorbeeld gebruiken we de SF220-24P om VLANs te configureren.

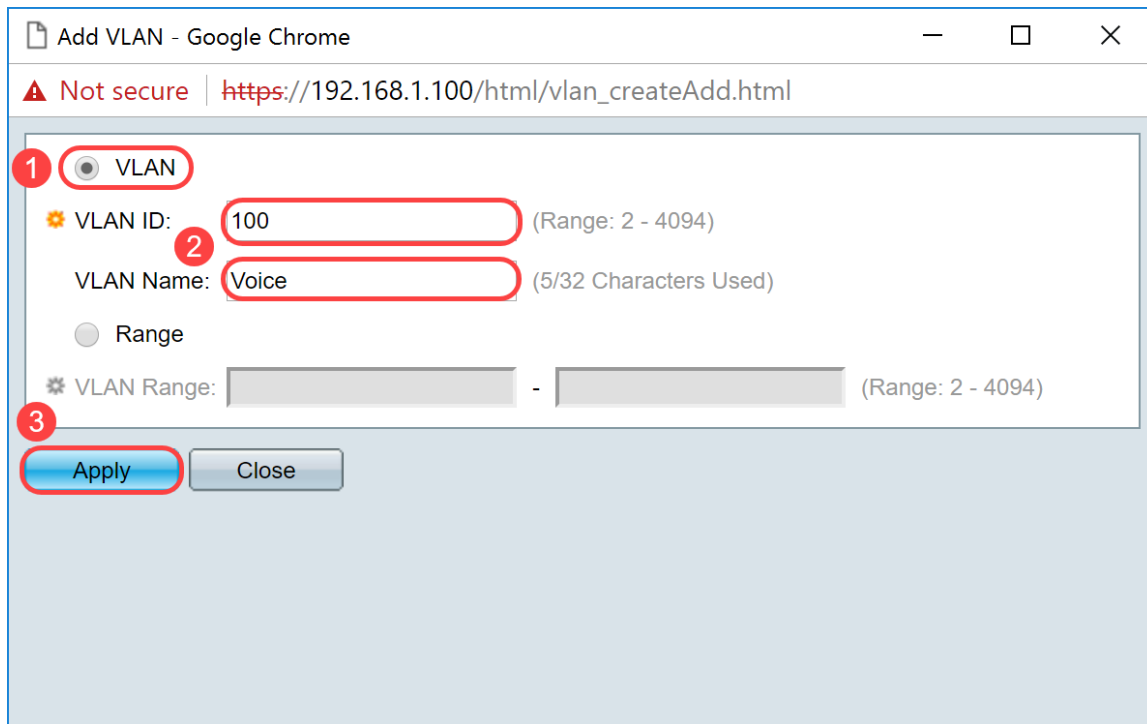


Stap 2. Klik op **Toevoegen...** om een nieuw VLAN te maken.



Stap 3. Als u één VLAN wilt maken, selecteert u **een VLAN-radioknop**. Voer de **VLAN-id** en **VLAN-naam in**. Klik vervolgens op **Toepassen** om het VLAN op te slaan. In dit voorbeeld, zullen wij VLAN 100 voor stem en 200 voor gegevens creëren.

**Opmerking:** sommige VLAN's zijn vereist door het systeem voor intern systeemgebruik en kunnen daarom niet worden gemaakt door de eerste VID in te voeren en de laatste VID, inclusief. Wanneer u de functie **Bereik** gebruikt, is het maximale aantal VLAN's dat u tegelijk kunt maken 100.

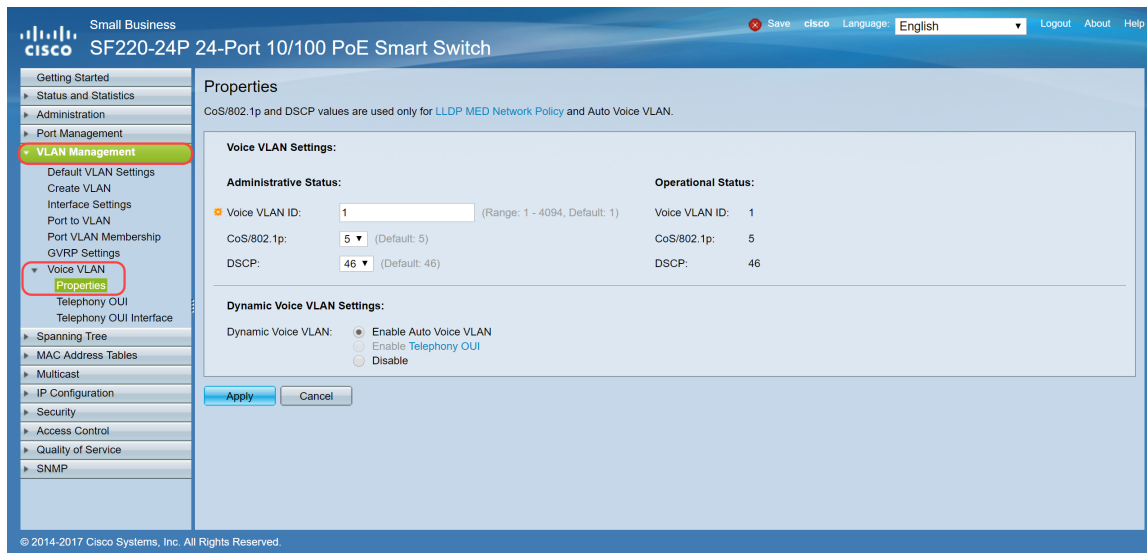


**Opmerking:** Herhaal stap 2 als u nog één VLAN moet maken.

## Voice VLAN instellen op de Switch

Stap 1. Log in op de webconfiguratie en navigeer naar **VLAN-beheer > Voice VLAN > Eigenschappen**.

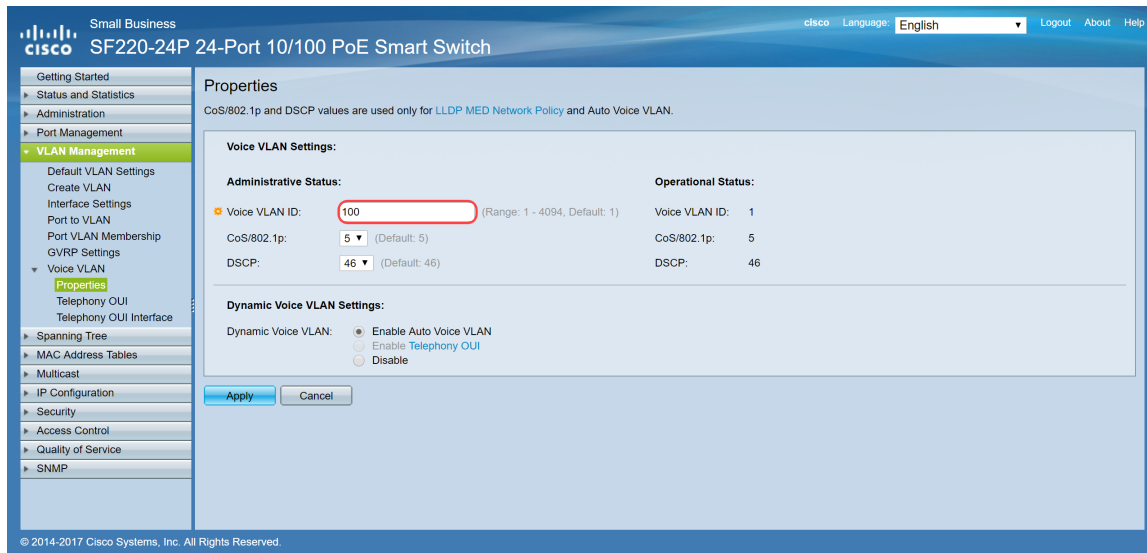
**Opmerking:** bij het configureren van Auto Voice VLAN worden automatisch QoS-instellingen voor spraak VLAN toegepast en wordt prioriteit gegeven aan het spraakverkeer.



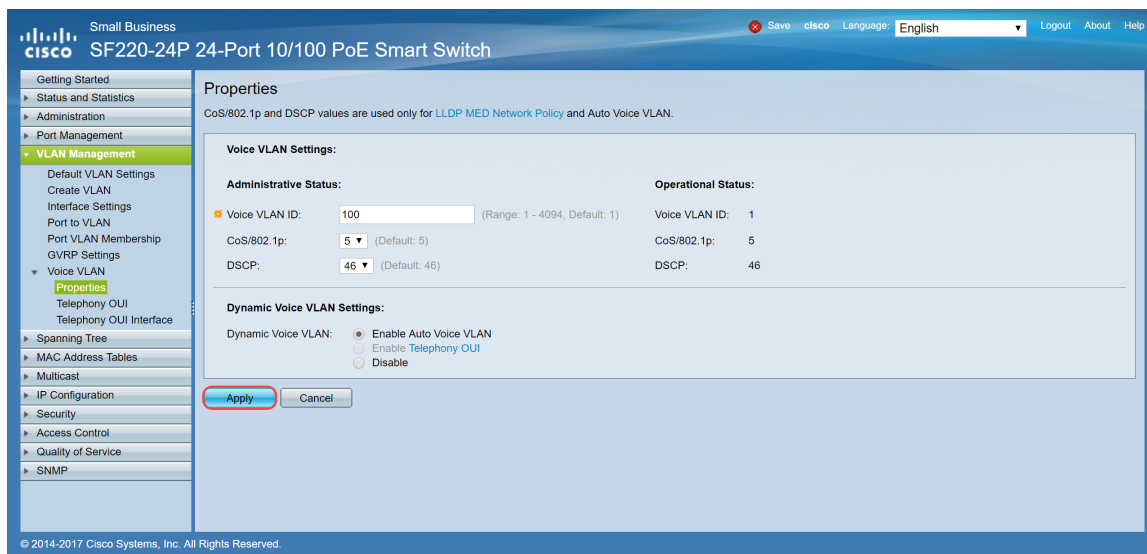
Stap 2. Voer onder de *beheerstatus* het VLAN in dat de spraak VLAN moet zijn in het veld *Voice VLAN-id*. In dit voorbeeld is VLAN 100 ingevoerd als spraak-VLAN.

**Opmerking:** wijzigingen in de spraak-VLAN-id, serviceklasse (CoS)/802.1p en/of gedifferentieerd servicecode (DSCP) maken dat het apparaat de administratieve spraak VLAN adverteert als een statische spraak-VLAN. Als de optie *Auto Voice VLAN-activering* die door externe spraak VLAN wordt geactiveerd, is geselecteerd, moeten de standaardwaarden worden gehandhaafd. In dit

voorbeeld, wordt CoS/802.1p verlaten als gebrek van 5 en DSCP wordt verlaten als gebrek van 46.



Stap 3. Klik op **Toepassen** om de instellingen op te slaan.



## Interface-instellingen configureren op de Switch

De interfaces, de fysieke poorten op de switch, kunnen aan een van de volgende instellingen worden toegewezen:

- **Algemeen:** de poort kan alle functies ondersteunen die zijn gedefinieerd in de IEEE 802.1q-specificatie. De interface kan een gelabeld of niet-gelabeld lid van een of meer VLANs zijn.
- **Toegang:** Kan slechts één VLAN geconfigureerd hebben op de interface en kan slechts één VLAN dragen.
- **Trunk:** kan het verkeer van meerdere VLANs via één link transporteren en u in staat stellen VLANs via het netwerk uit te breiden.
- **Dot1p-Tunnel:** zet de interface in QinQ-modus. Dit stelt de gebruiker in staat om hun eigen VLAN-regelingen (PVID) te gebruiken via het providernetwerk. De switch bevindt zich in de QinQ-modus wanneer er een of meer dot1p-tunnelpoorten zijn.

Stap 1. Log in op de webconfiguratie en navigeer naar **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.

Stap 2. Selecteer de interfacemodus voor VLAN. In dit voorbeeld zullen we de Raspberry Pi (poort: FE3) configureren als een toegangspoort.

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

Showing 1-26 of 26 All per page

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

Stap 3. Klik vervolgens op **Bewerken** om de interface te bewerken.

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

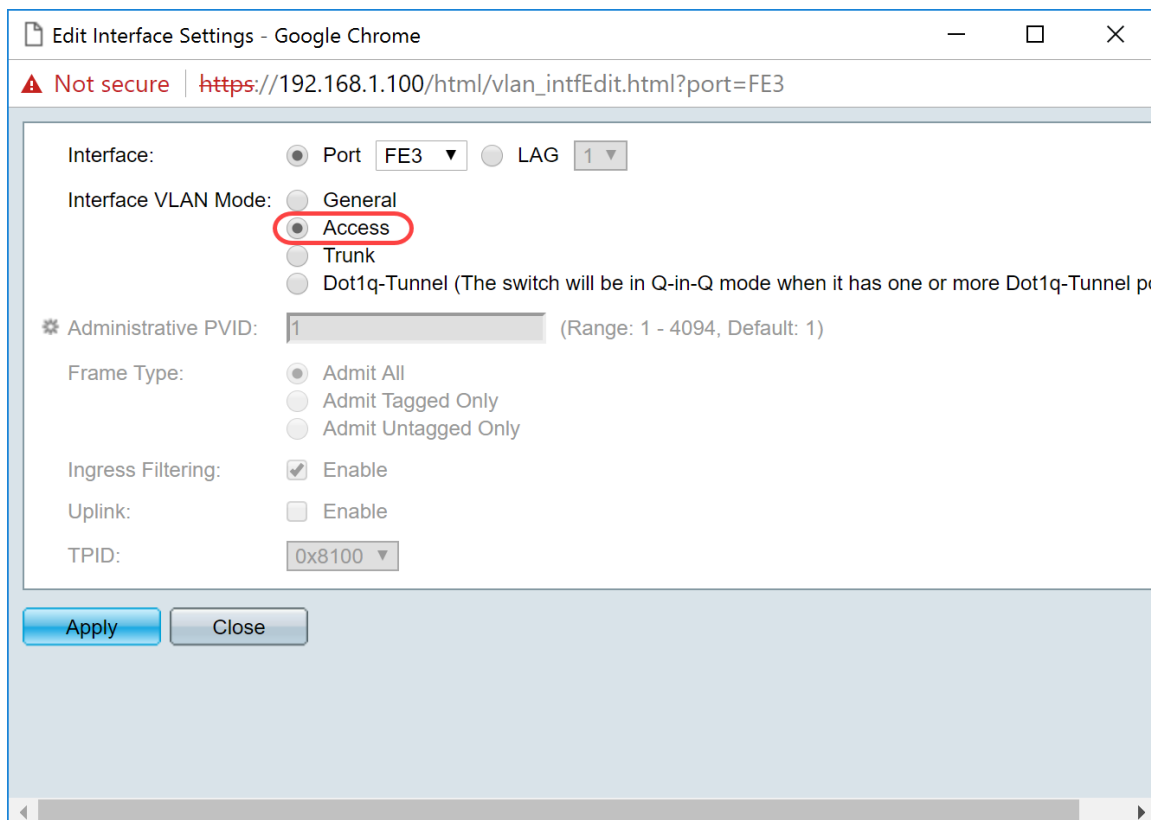
Filter: Interface Type equals to Port Go

Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Uplink
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

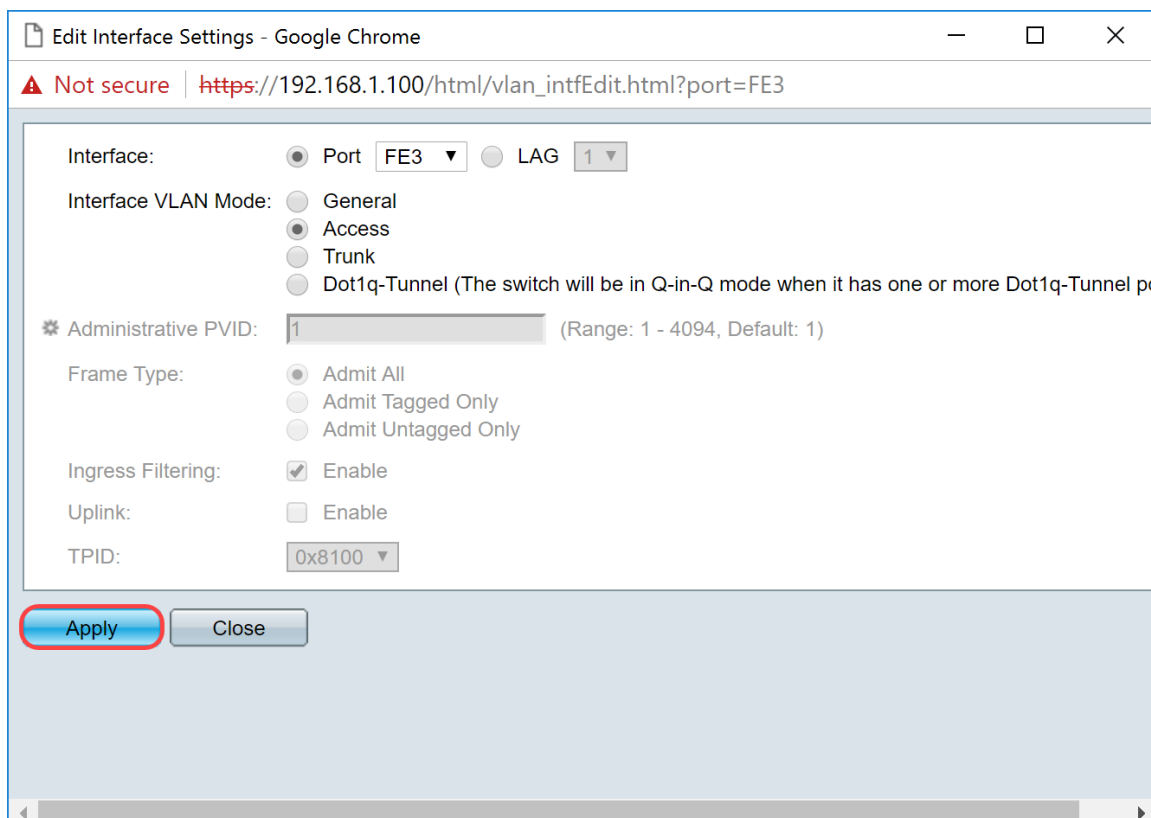
Copy Settings... Edit...

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

Stap 4. Kies in het veld *Interface VLAN Mode* **Access** om de interface te configureren als een niet-gelabeld lid van één VLAN.



Stap 5. Klik op **Toepassen** om de instellingen op te slaan.



## Het configureren van poortVLAN-lidmaatschap op de Switch

Nadat de VLAN's zijn gemaakt, moet u VLAN's toewijzen aan de poorten die u wilt toevoegen.



Stap 1. Meld u aan bij de webconfiguratie en navigeer naar **VLAN Management > Port VLAN Membership**.

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

Port VLAN Membership

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

Port VLAN Membership Table

Showing 1-26 of 26 All per page

Filter: Interface Type equals to Port Go

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	

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

Stap 2. In de *Lijst van het Lidmaatschap van Port VLAN*, selecteer de interface die u het lidmaatschap van VLAN wilt vormen. In dit voorbeeld zullen we de Raspberry Pi (poort: FE3) configureren om op VLAN 100 te zijn.

**Opmerking:** alle spraakapparaten worden al geconfigureerd voor de spraak-VLAN die u hebt geselecteerd in het gedeelte [Voice VLAN instellen op de Switch](#).

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

Port VLAN Membership

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

Port VLAN Membership Table

Showing 1-26 of 26 All per page

Filter: Interface Type equals to Port Go

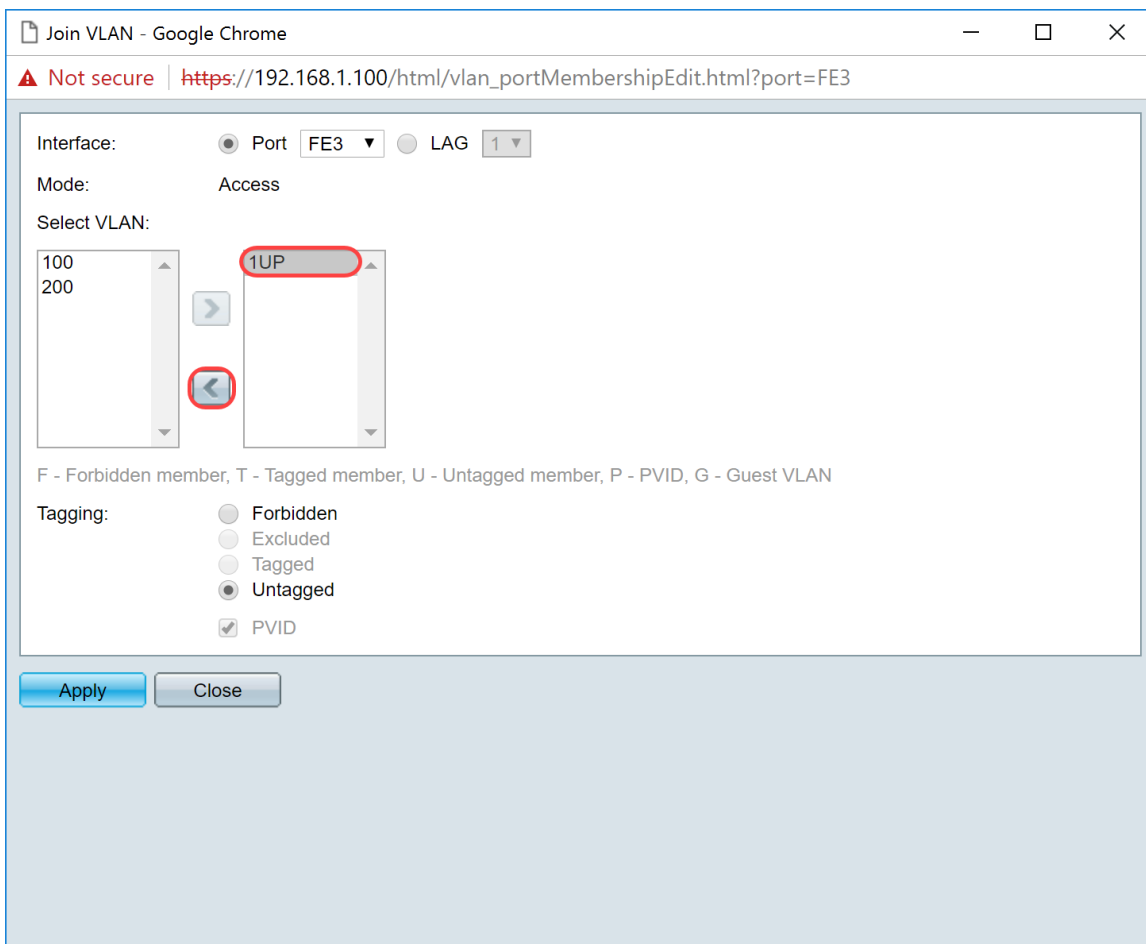
Interface	Mode	Administrative VLANs	Operational VLANs	LAG
FE1	Trunk	1UP	1UP, 100T	
FE2	Trunk	1UP	1UP, 100T	
FE3	Access	1UP	1UP	
FE4	Trunk	1UP	1UP	
FE5	Trunk	1UP	1UP	
FE6	Trunk	1UP	1UP	
FE7	Trunk	1UP	1UP	
FE8	Trunk	1UP	1UP	
FE9	Trunk	1UP	1UP	
FE10	Trunk	1UP	1UP	
FE11	Trunk	1UP	1UP	
FE12	Trunk	1UP	1UP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

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

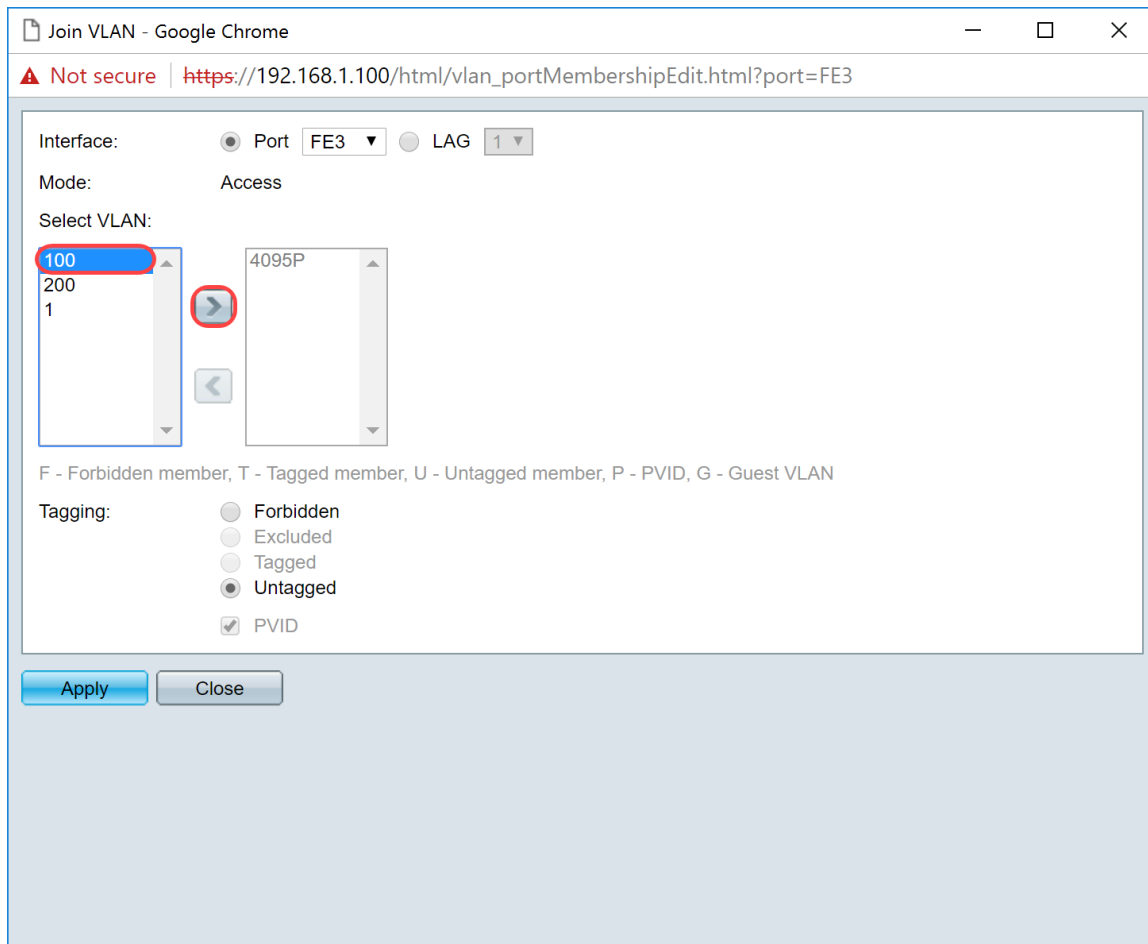
Stap 3. Klik op **Aanmelden bij VLAN...** om de poort aan te passen die u VLAN's wilt configureren.



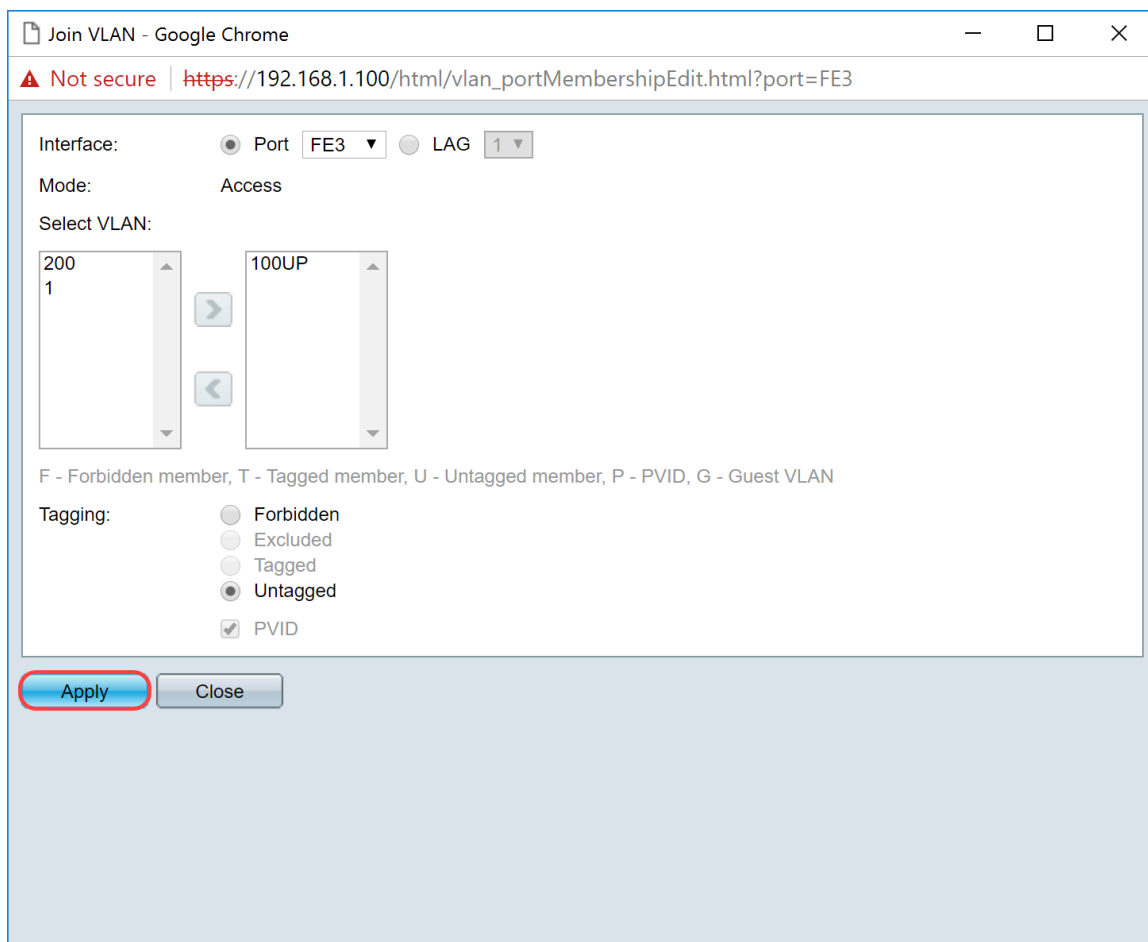
Stap 4. Selecteer **1UP** en klik op < om VLAN 1 te verwijderen uit de interface in de sectie *Selecteer VLAN*. Slechts 1 untagged VLAN kan aan de interface worden toegevoegd wanneer het een toegangshaven is.



Stap 5. Selecteer **100** en klik > om het niet-gelabelde VLAN aan de interface toe te voegen.



Stap 6. Klik op **Toepassen** om de instellingen op te slaan.



Stap 7. Selecteer de interfacepoort die is aangesloten op de router in het *veld Interface*. In dit voorbeeld is poort GE1 geselecteerd.

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

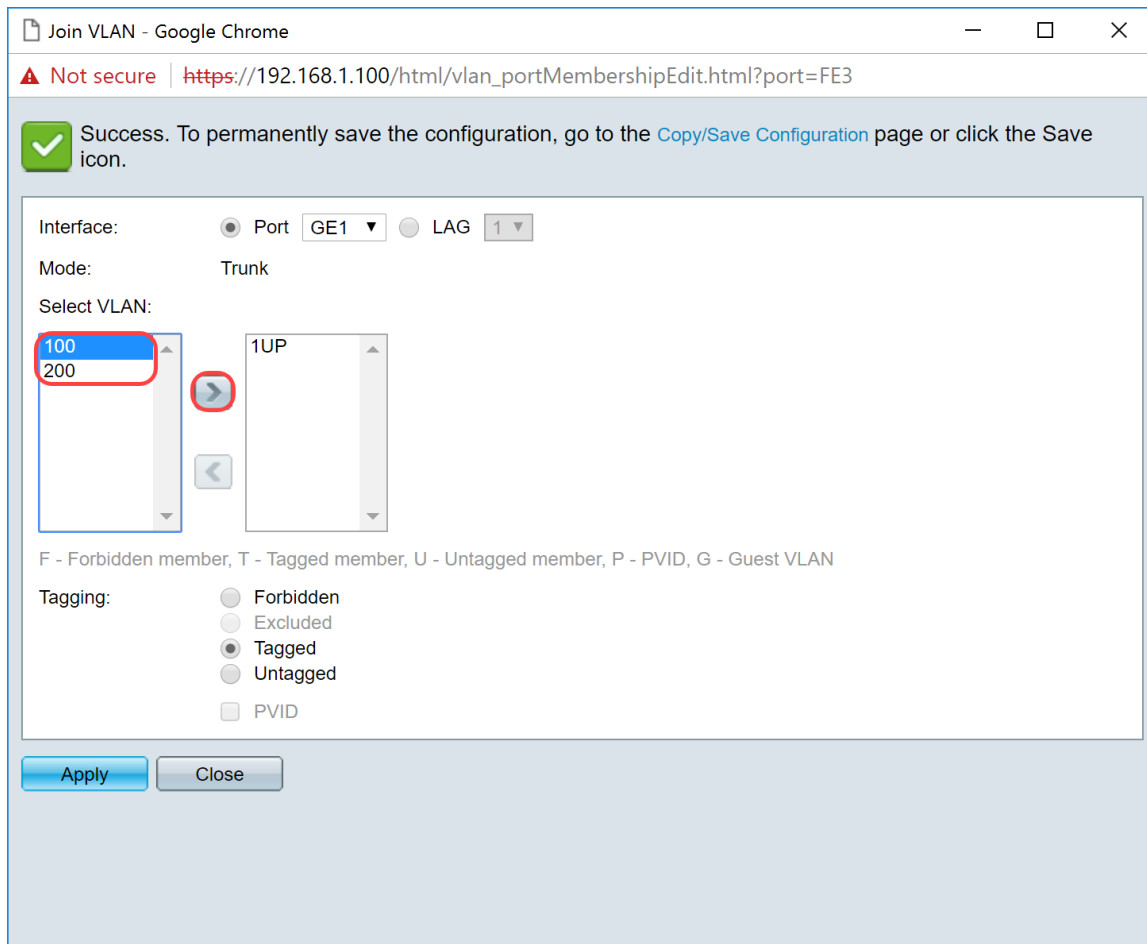
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN

Tagging:

Forbidden  
 Excluded  
 Tagged  
 Untagged  
 PVID

Apply Close

Stap 8. Kies het VLAN dat wordt toegevoegd aan de geselecteerde interface en klik vervolgens > om het toe te voegen in de sectie *VLAN selecteren*. In dit voorbeeld selecteren we VLAN **100** en **200**.



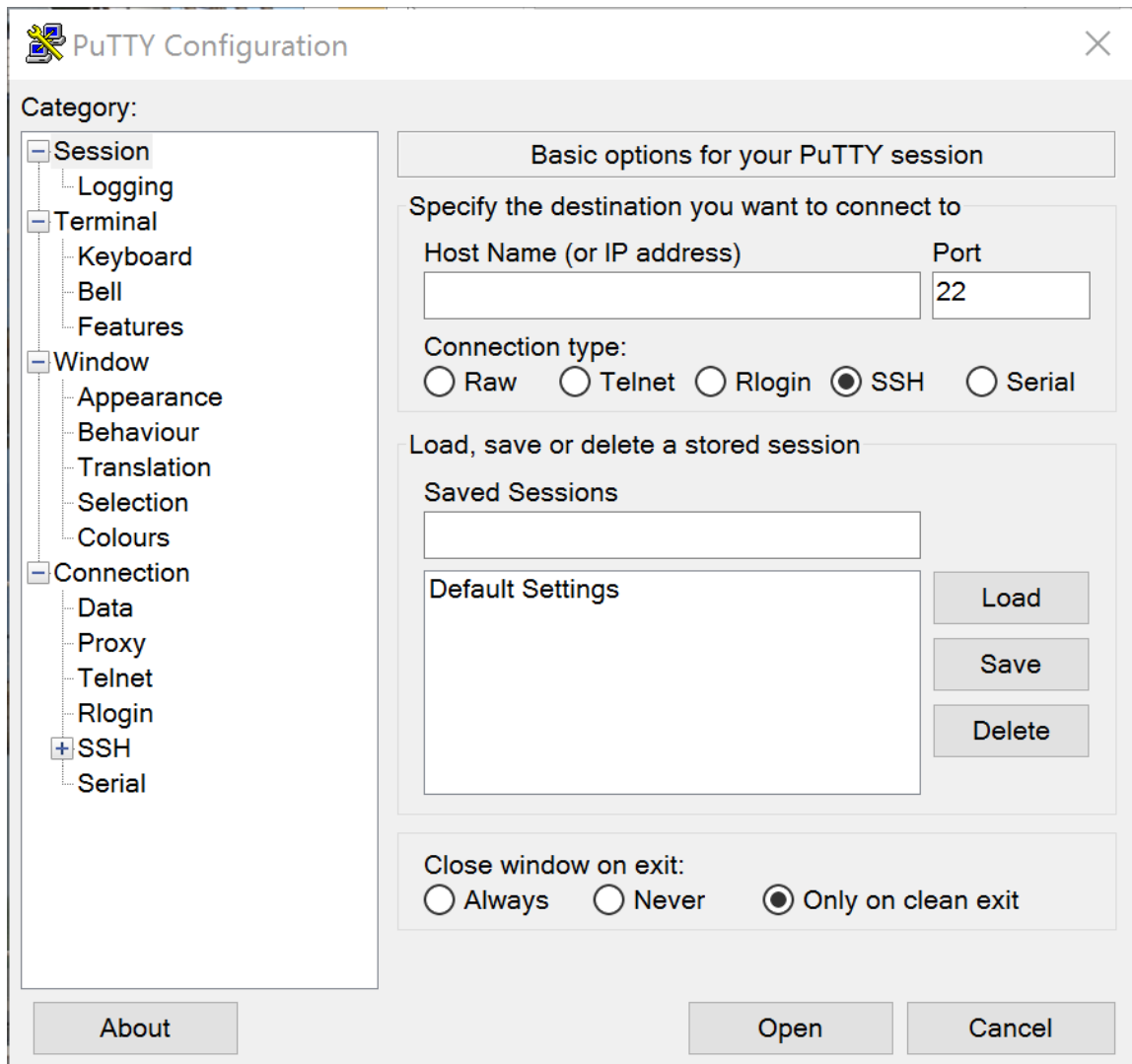
Stap 9. Klik op **Toepassen** om de instellingen op te slaan.

**Opmerking:** mogelijk moet de IP-telefoon opnieuw worden opgestart om het IP-adres in het juiste subnetnummer te kunnen wijzigen.

## Veranderend IP-adres van Raspberry Pi om op een andere Subnet te zijn

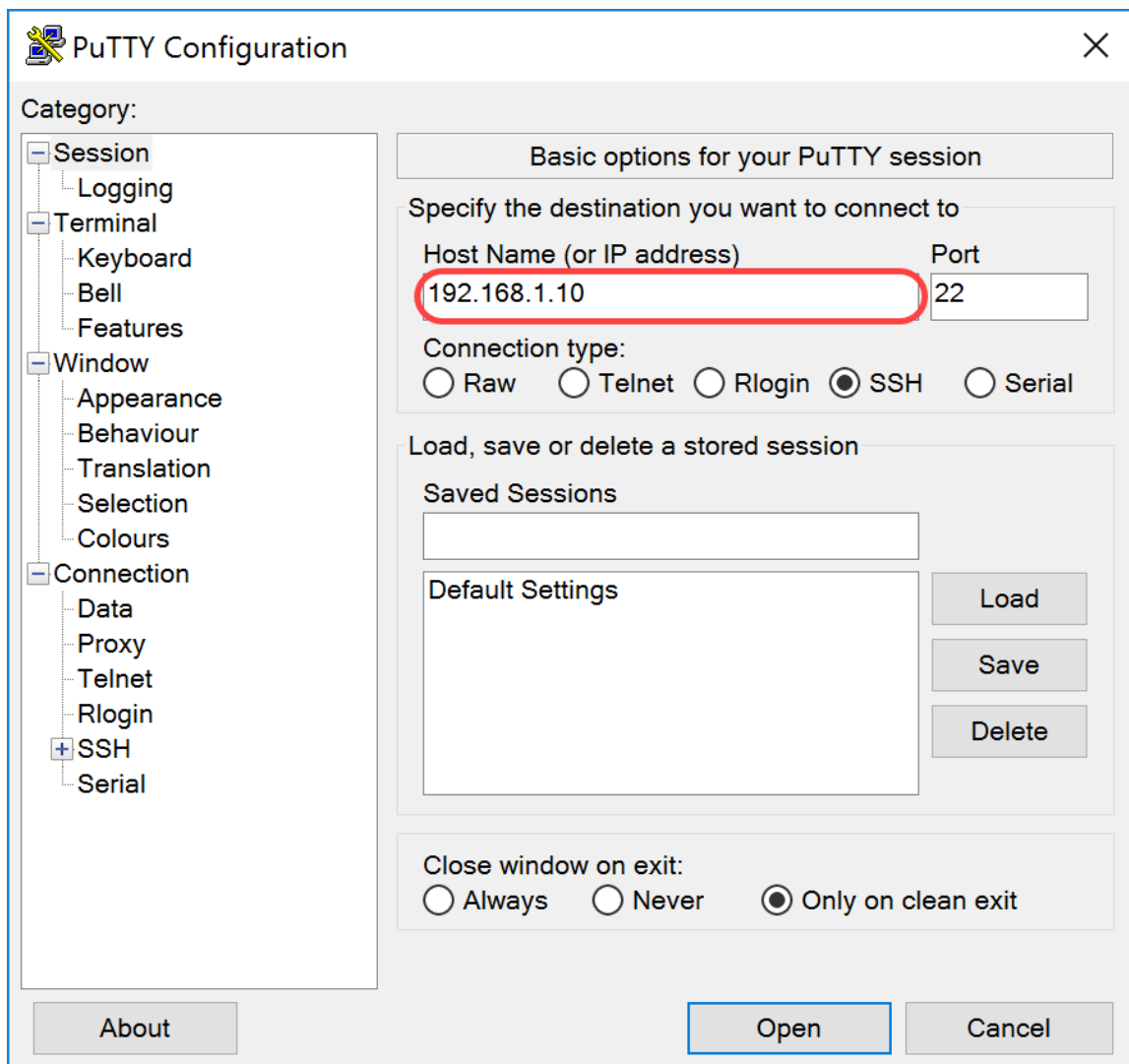
Stap 1. Maak verbinding met uw Raspberry Pi door Secure Shell (SSH) of sluit uw Raspberry Pi aan op een computermonitor. In dit voorbeeld zullen we SSH gebruiken om de Raspberry Pi te configureren.

**Opmerking:** de poort op de switch voor uw computer / laptop zal op hetzelfde VLAN als de Raspberry Pi moeten zijn en geconfigureerd als een toegangspoort bij het instellen van interfacestypen. Zie [Interfaceinstellingen configureren op een Switch](#) en [Port VLAN-lidmaatschap configureren in het gedeelte Switch](#) van dit artikel voor review. Zorg ervoor dat uw IP-adres op hetzelfde netwerk staat als uw Raspberry Pi om er SSH in te krijgen. Als uw apparaat niet op hetzelfde netwerk als de Raspberry Pi staat, gebruik dan een statisch IP-adres en verander uw IP-adres handmatig om op hetzelfde netwerk te staan of u kunt de opdracht **ipconfig /release** en **ipconfig/renew** intypen in de opdrachtprompt om een nieuw IP-adres te verkrijgen. SSH-clients kunnen variëren, afhankelijk van uw besturingssysteem. In dit voorbeeld werd PuTTY gebruikt om de Raspberry Pi in te snijden. Voor meer informatie over SSH, klik [hier](#).

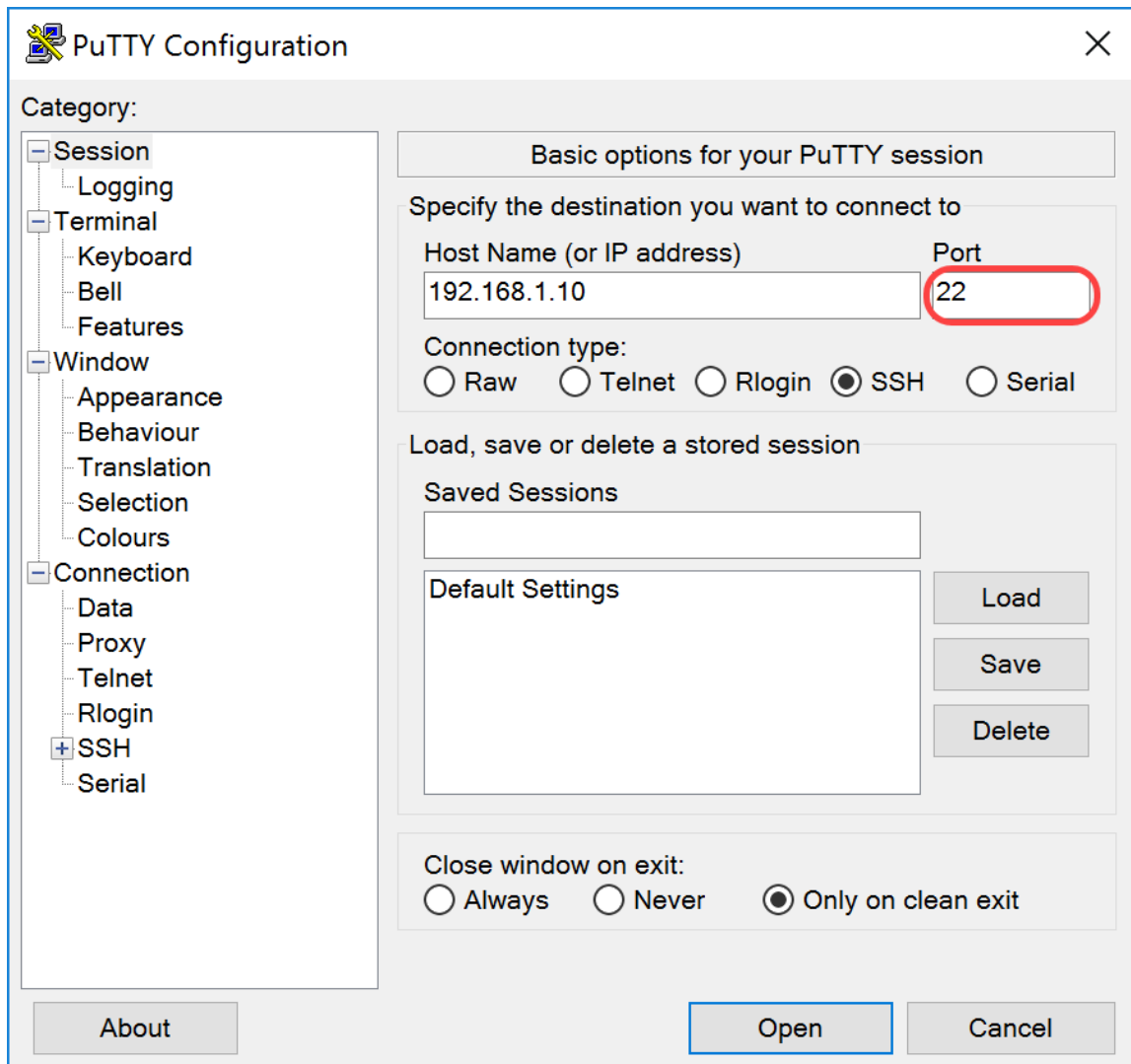


Stap 2. Typ het IP-adres van uw Raspberry Pi in het veld *Host Name (of IP-adres)*. In dit voorbeeld wordt 192.168.1.10 ingevuld.

**Opmerking:** U kunt DHCP-tabel in de router gebruiken om het adres van de Raspberry Pi te vinden. In dit document is deze Raspberry Pi vooraf geconfigureerd om een statisch IP-adres te hebben.

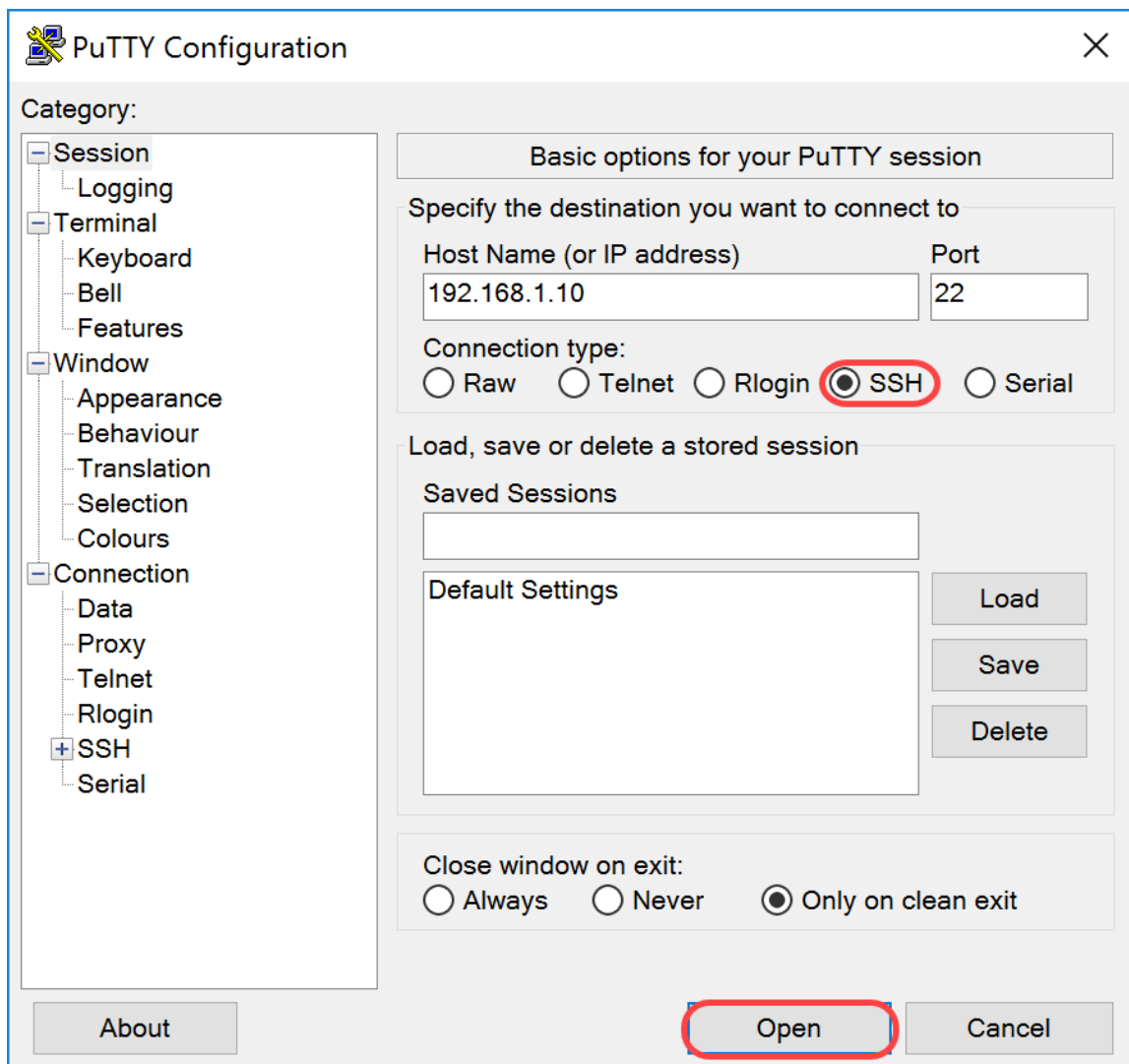


Stap 3. Voer **22** in als poortnummer in het veld *Port*. Port 2 is de standaardpoort voor SSH-protocol.



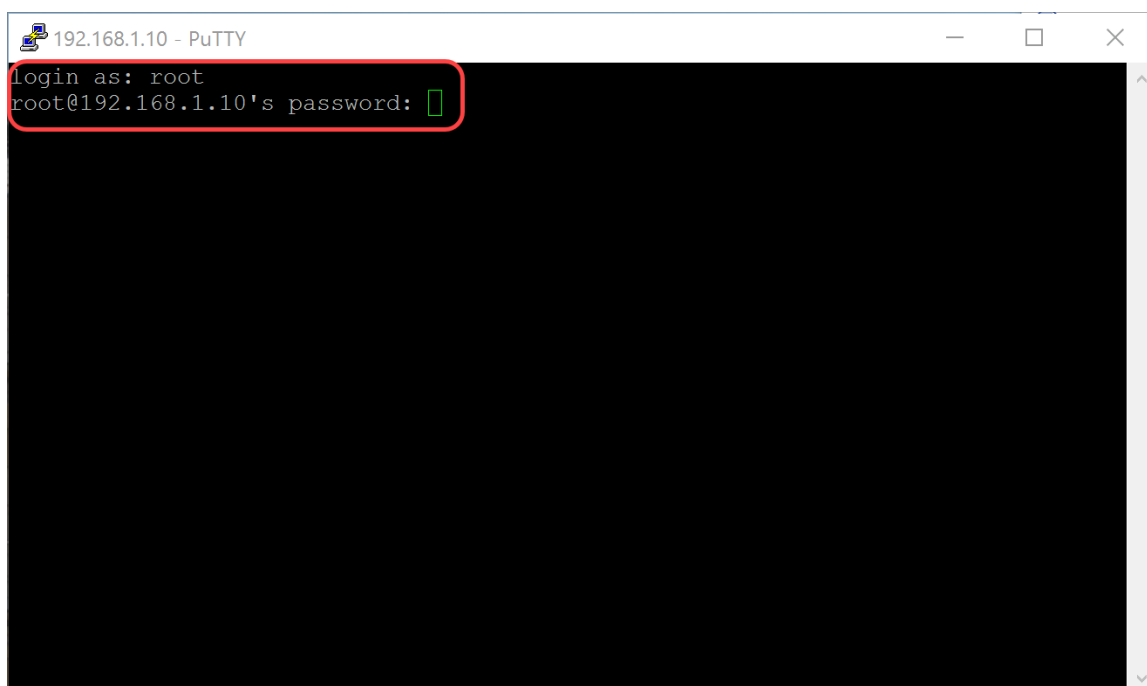
Stap 4. Klik in het gedeelte *Verbindingstype*: op de **SSH**-radioknop om SSH te kiezen als uw verbindingsmethode met de switch. Klik vervolgens op **Openen** om de sessie te starten.





Stap 5. Voer de gebruikersnaam en het wachtwoord van de RasPBX in het veld *Aanmelden als* en *wachtwoord*.

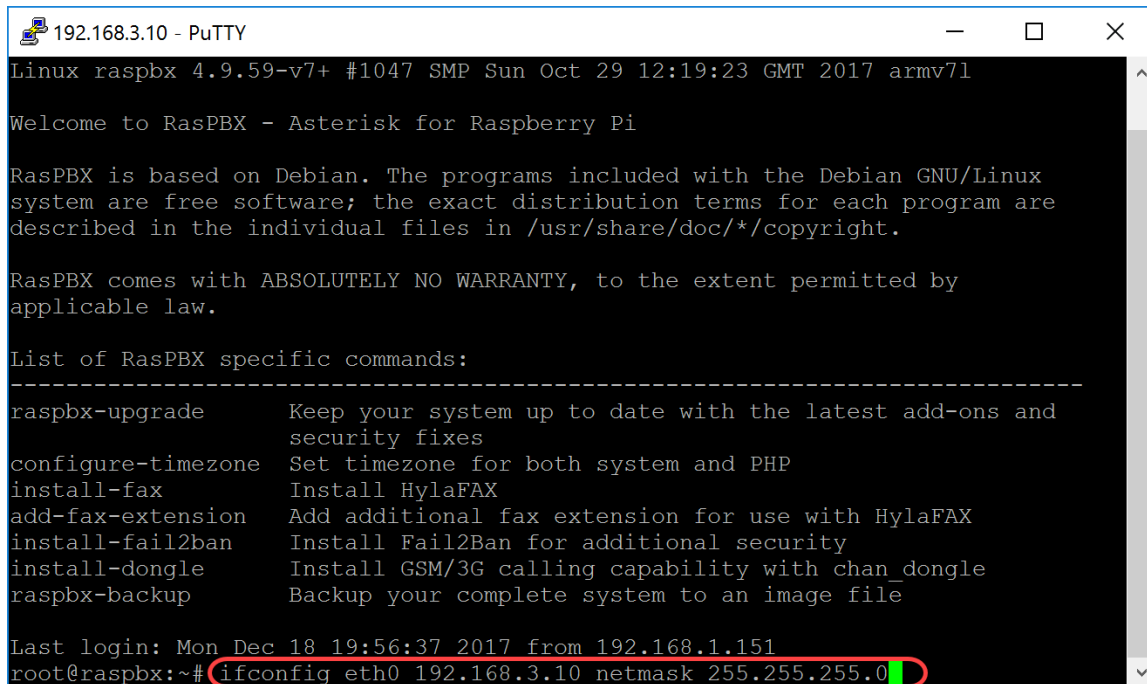
**Opmerking:** De standaardgebruiker: **wortel** en het standaardwachtwoord: **framboos**



Stap 6. Als u het IP-adres van uw Ethernet als een statisch IP-adres wilt wijzigen, typt u `ifconfig eth0 [IP-adres] netmask [netmasker]`. In dit voorbeeld gebruiken we 192.168.3.10 en het netmasker van 255.255.255.0

```
ifconfig eth0 192.168.3.10 netmask 255.255.255.0
```

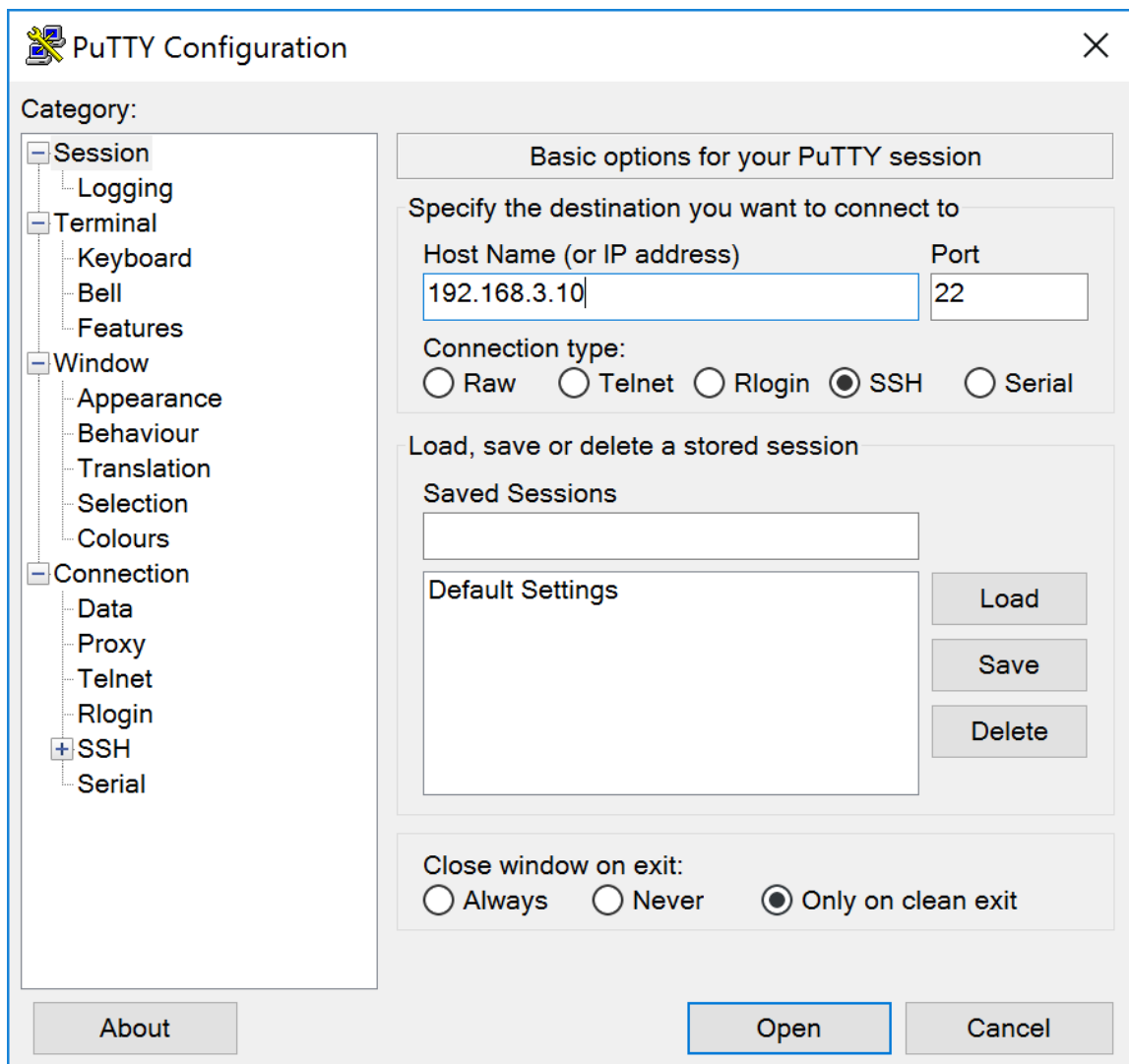
**Opmerking:** de verbinding met de sessie wordt verbroken wanneer u het IP-adres wijzigt. Om verbinding te maken met de Raspberry Pi, moet uw computer / laptop op dezelfde sub als de Raspberry Pi (192.168.3.x).



```
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
```

Stap 7. Sluit terug naar uw Raspberry Pi met behulp van het statische IP-adres dat in stap 6 is ingesteld. In dit voorbeeld gebruiken we 192.168.3.10 om terug te verbinden.

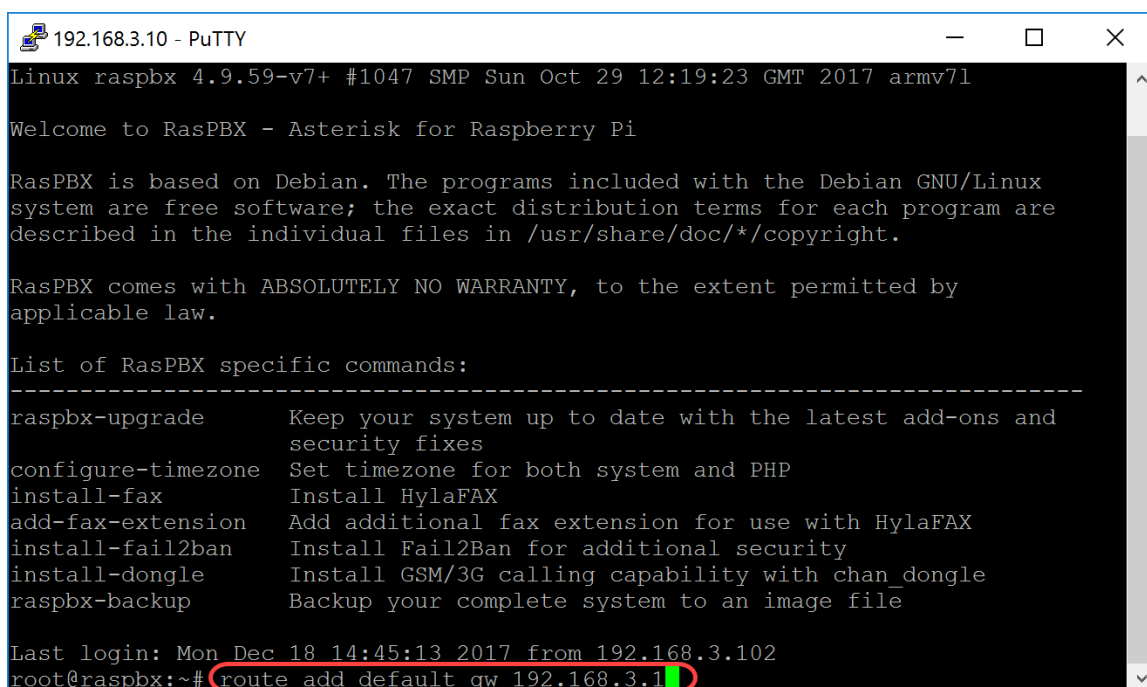
**Opmerking:** Zorg ervoor dat uw computer/laptop op dezelfde subnetverbinding staat als de Raspberry Pi en ook de VLAN. Als uw computer / laptop op hetzelfde VLAN als de Raspberry Pi is en u niet het juiste IP-adres hebt, kunt u naar uw opdrachtprompt gaan en in `ipconfig /release` typen en vervolgens `ipconfig /renew` om een nieuw IP-adres te vragen of u kunt uw apparaat configureren om een statisch IP-adres in de Ethernet-eigenschappen te hebben.



Stap 8. Typ in de opdrachtregel standaard gw [IP-adres van router van het subnet] toe om een standaardgateway toe te voegen.

**Opmerking:** u kunt de opdrachtroute gebruiken om de routertabel te zien.

```
route add standaard gw 192.168.3.1
```



## Conclusie

U zou nu met succes een basisspraaknetwerk moeten hebben opgezet. Om dit te verifiëren, neem één van de SPA/MPP telefoons en u zou een kiestoon moeten horen. In dit document heeft een van de SPA/MPP-telefoons de extensie 1002 en de andere 1003. U zou de extensie 1003 moeten kunnen bellen als u de extensie 1002 SPA/MPP-telefoon gebruikt.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.