Come creare una rete voce di base utilizzando Raspberry Pi

Obiettivo

In questo documento viene spiegato come configurare una rete vocale di base con Raspberry Pi come server di comunicazione usando Asterisks. Le tecnologie VLAN (Virtual Local Area Network) e QoS (Quality of Service) verranno utilizzate per assegnare le priorità al traffico separando il traffico di voce da quello di dati. L'obiettivo di questa rete è l'impostazione di test interni. Questi test consentono di scalare la rete in modo appropriato, verificare se si dispone di una larghezza di banda sufficiente per il volume vocale previsto e individuare eventuali altri possibili conflitti tra le apparecchiature. Può inoltre essere utile per determinare se si desidera ospitarlo localmente o nel cloud. Una volta raggiunte determinate dimensioni, un'azienda può scegliere di utilizzare un proprio sistema di controllo delle chiamate locale, ad esempio PBX o IP PBX. Ciò renderebbe più efficienti le chiamate interne, dal momento che le chiamate tra i telefoni all'interno dell'azienda non dovrebbero essere indirizzate fuori dall'edificio e poi rientrare.

Nota importante: Raspberry Pi non è un prodotto supportato da Cisco, questo documento è solo per scopi di supporto e non è un documento della soluzione.

Introduzione

Affinché un'azienda possa svolgere un'attività commerciale efficace, i dipendenti devono avere accesso a una rete vocale. Ciò facilita la comunicazione tra i dipendenti e i loro clienti, oltre a permettere ai dipendenti di comunicare internamente. A ogni dipendente possono essere forniti un telefono fisso e/o un telefono cellulare, ma questo può diventare piuttosto costoso. Spesso le aziende scelgono di configurare una rete voce che utilizzi invece il protocollo VoIP (Voice over Internet Protocol).

La tecnologia VoIP consente di utilizzare Internet per effettuare e ricevere chiamate telefoniche da qualsiasi luogo e da qualsiasi luogo nel mondo con costi minimi, se esistenti, per lunghe distanze. Può essere utilizzato su qualsiasi dispositivo che utilizzi Internet.

La tecnologia VoIP consente di risparmiare denaro all'azienda aumentando al contempo la produttività, le comunicazioni e la soddisfazione dei clienti. I dipendenti possono utilizzare diverse funzioni come il routing delle chiamate, la musica in attesa e la segreteria telefonica integrata.

Una caratteristica comune del VoIP utilizzata da molte aziende è il routing delle chiamate, noto anche come distributore automatico di chiamate. Il servizio di routing delle chiamate distribuisce le chiamate in arrivo al successivo agente disponibile anziché inviarle alla segreteria telefonica. Ciò garantisce che le chiamate dei clienti ricevano una risposta nel modo più efficiente possibile. Al di fuori dell'orario di lavoro, le chiamate possono essere inviate direttamente alla segreteria telefonica.

L'aggiunta di utenti e l'aggiornamento delle funzionalità è un processo semplice, utile quando l'azienda è in espansione o le esigenze cambiano. A differenza di un sistema telefonico tradizionale, non è necessario eseguire costosi cablaggi.

Per configurare una rete VoIP, è necessario valutare alcune opzioni. È possibile ospitare un servizio VoIP per il proprio sistema telefonico utilizzando KSU, KSU-less, Private Branch Exchange (PBX) o un altro sistema VoIP.

È necessario tenere in considerazione il budget, il numero di dipendenti e sedi, i servizi disponibili nella propria area e la crescita dell'azienda. Potrebbe essere necessario disporre anche di apparecchiature di formazione e supplementari, ad esempio cuffie. Il protocollo VoIP può aumentare l'utilizzo dei dati e potrebbe essere necessario aumentare la larghezza di banda per tenere conto del traffico della rete vocale.

Dovreste anche pianificare un backup, "Piano B", nel caso in cui la rete dovesse andare in tilt. Se l'alimentazione viene interrotta, il sistema VoIP non si collegherà. Questa ridondanza deve essere implementata per ripristinare immediatamente i servizi telefonici e prevenire l'interruzione della produttività aziendale.

In questo articolo, implementeremo il nostro sistema telefonico utilizzando Asterisk, un PBX su un Raspberry Pi.

Nota: dopo aver completato questi passaggi e avere la possibilità di effettuare chiamate dalla rete interna, è necessario scegliere un provider di servizi di telefonia Internet (ITSP, Internet Telephony Service Provider).

Definizioni

Una LAN virtuale o VLAN (Virtual Local Area Network) consente di segmentare logicamente una LAN (Local Area Network) in più domini di broadcast. Quando sulla rete vengono trasmessi anche dati sensibili, la creazione di VLAN offre una maggiore sicurezza e il traffico viene quindi indirizzato a VLAN specifiche. Gli utenti di una VLAN specifica sono gli unici in grado di accedere e modificare i dati trasmessi su tale rete. L'uso delle VLAN inoltre può migliorare le prestazioni in quanto riduce la necessità di inviare pacchetti broadcast e multicast a destinazioni non necessarie.

Per impostazione predefinita, tutte le porte sono assegnate alla VLAN 1, quindi una volta configurate diverse VLAN, è necessario assegnare manualmente ciascuna porta alla VLAN appropriata.

Ciascuna VLAN deve essere configurata con un ID VLAN (VID) univoco con un valore compreso tra 1 e 4094. Il dispositivo riserva il VID 4095 come VLAN di eliminazione. Tutti i pacchetti classificati sulla VLAN scartata vengono scartati all'ingresso e non vengono inoltrati a una porta.

QoS (Quality of Service) consente di assegnare priorità al traffico per diverse applicazioni, utenti o flussi di dati. e può essere utilizzato anche per garantire prestazioni fino a un livello specificato, influendo in tal modo sulla QoS del client. QoS è generalmente influenzato dai seguenti fattori: jitter, latenza e perdita di pacchetti. Molto spesso, video o VoIP hanno la priorità in quanto sono maggiormente interessati da QoS.

Private Branch Exchange (PBX) è un sistema di commutazione telefonica che gestisce le chiamate in entrata e in uscita per gli utenti interni di una società. Un PBX è connesso al sistema telefonico pubblico e instrada automaticamente le chiamate in arrivo a estensioni specifiche. Condivide e gestisce inoltre più linee. Un tipico sistema PBX per piccole imprese include linee telefoniche interne ed esterne, un server informatico che gestisce la commutazione e il routing delle chiamate e una console per il controllo manuale.

Un **PBX IP** può fare tutto ciò che un PBX tradizionale per le piccole imprese può fare e molto di più. Esegue la commutazione e la connessione di VoIP così come le chiamate di linea fissa. Un sistema IP PBX viene eseguito su una rete di dati IP, consentendo di risparmiare sui costi e di ridurre al minimo la gestione della rete. Su un sistema telefonico IP PBX è possibile utilizzare telefoni IP, softphone (che non richiedono alcun hardware oltre a un computer e cuffie microfoniche) e telefoni fissi.

Un **Raspberry Pi** è un piccolo computer portatile e poco costoso che funziona come un computer

desktop.

Asterisco è un framework open source che può trasformare un computer, come un Raspberry Pi, in un server di comunicazione. Ciò consente di creare un sistema telefonico PBX aziendale personalizzato. In questo articolo, Asterisk utilizza FreePBX come interfaccia grafica utente (GUI) che controlla e gestisce Asterisk dove è possibile configurare estensioni, utenti, ecc.

Dispositivi interessati

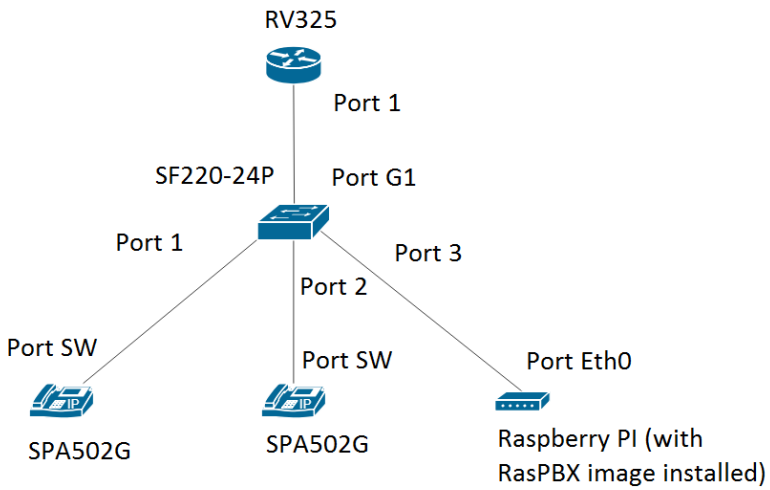
- Router
- Switch Power over Ethernet (PoE)
- Lampone Pi (modelli Pi 3 B+, Pi 3, Pi 3, B+, B e A)
- 2 o più telefoni IP Cisco SPA/MPP

Versione del software

- 14.0.1.20 (FreePBX)
- 13.20.0 (asterisco)
- 1.1.1.06 (RV325 Router)
- 1.1.4.1 (SF220-24P)
- 7.1.3 (SPA502G)

Per configurare Basic Voice Network con Raspberry Pi, attenersi alle seguenti linee guida:

Topologia:



Qui è possibile trovare l'immagine del RasPBX. Questa immagine deve essere installata sul Raspberry Pi.

Nota: in questo documento l'immagine Raspberry Pi con l'immagine RasPBX è già configurata. Per accedere alla GUI di Raspberry Pi, digitare http://raspbx.local o l'indirizzo IP di Raspberry Pi nel browser per configurare il PBX. Il login predefinito di FreePBX è utente: **admin** password: **admin**.

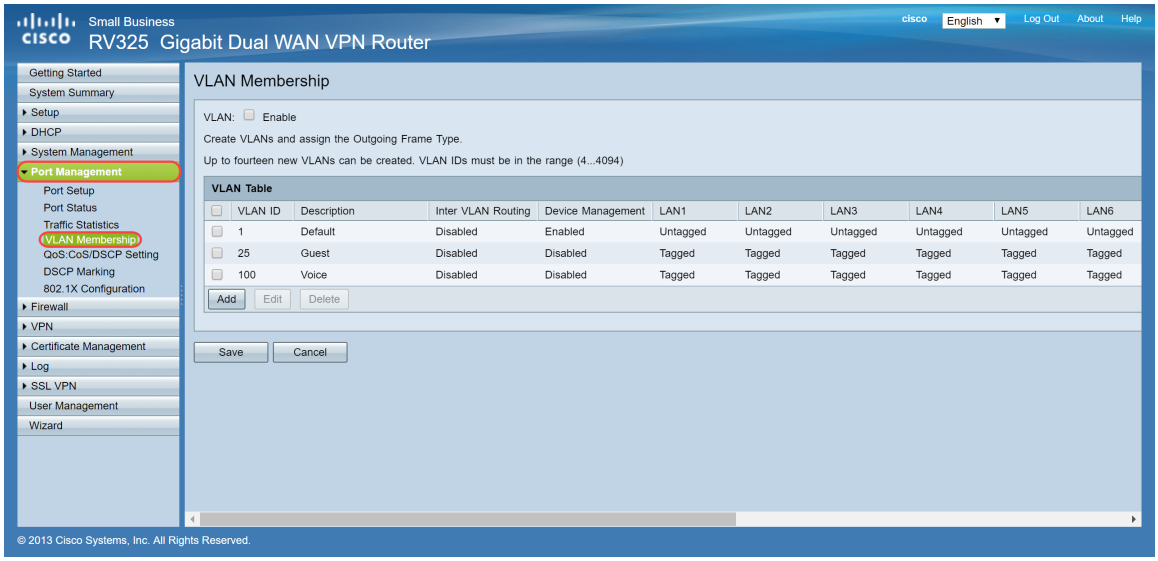
Inoltre, il Raspberry Pi è stato preconfigurato per avere un indirizzo IP statico.

Sommario

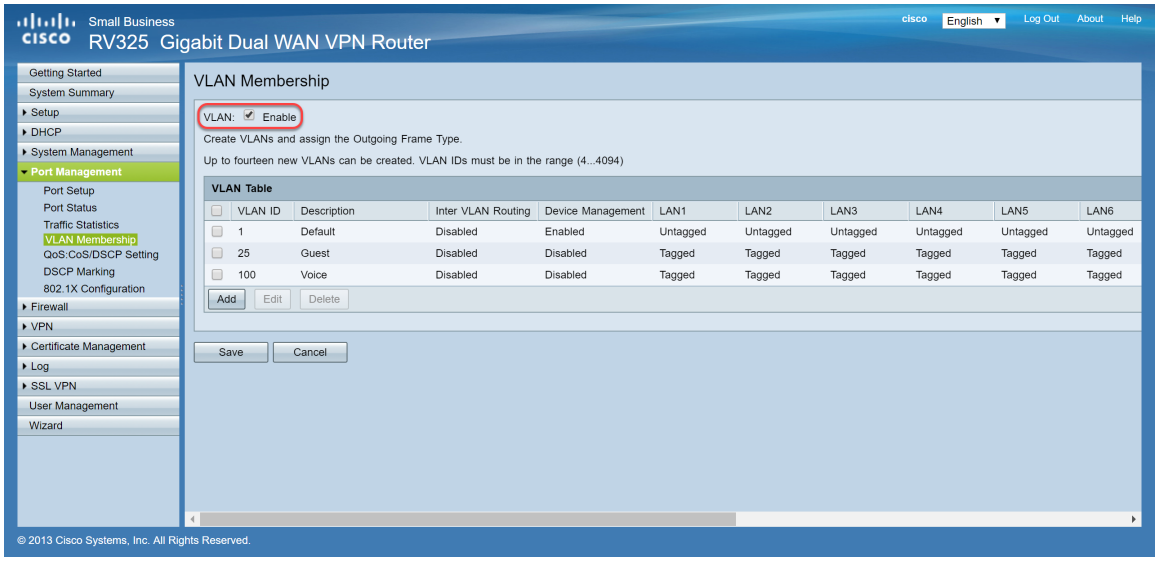
Configurazione delle VLAN sul router

Passaggio 1. Accedere all'utility basata sul Web e selezionare **Port Management > VLAN Membership** (Gestione porte > Appartenenza VLAN).

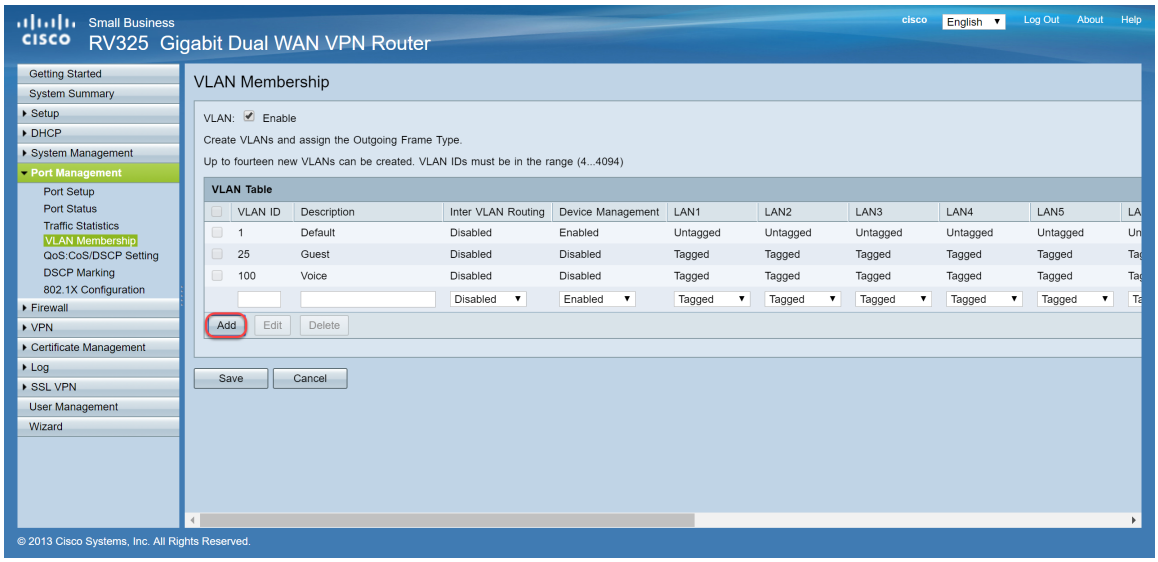
Nota: questa condizione può variare a seconda del modello. Nell'esempio viene usata la RV325. Per ulteriori informazioni sull'accesso alla pagina di installazione basata sul Web, fare clic qui.



Passaggio 2. Selezionare la casella di controllo **Enable** per abilitare la VLAN sul router.

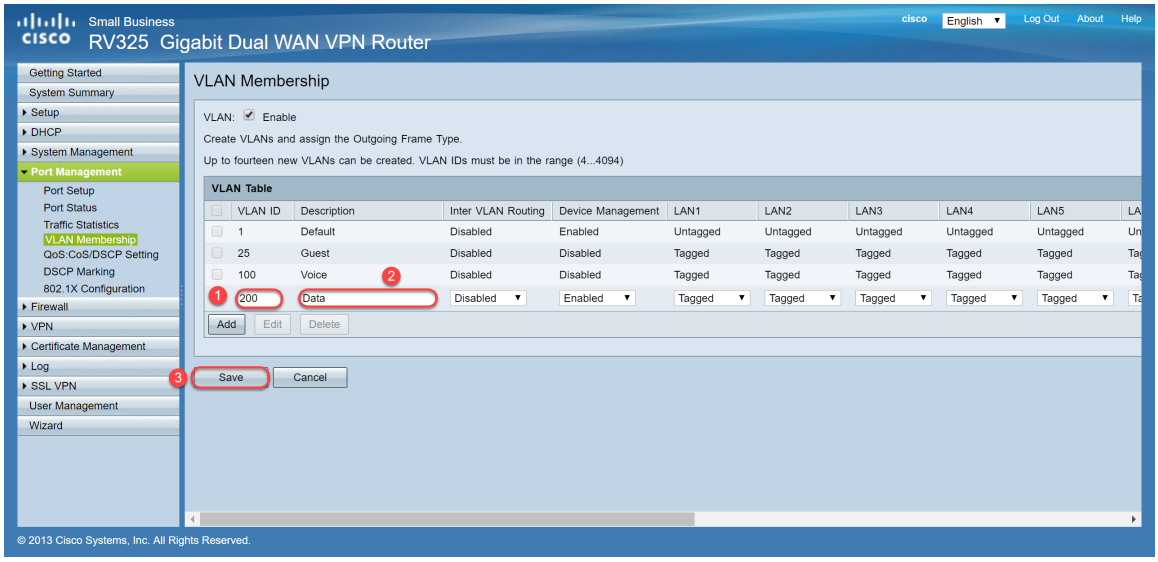


Passaggio 3. Nella sezione *Tabella VLAN*, fare clic su **Add** (Aggiungi) per creare un nuovo ID VLAN.

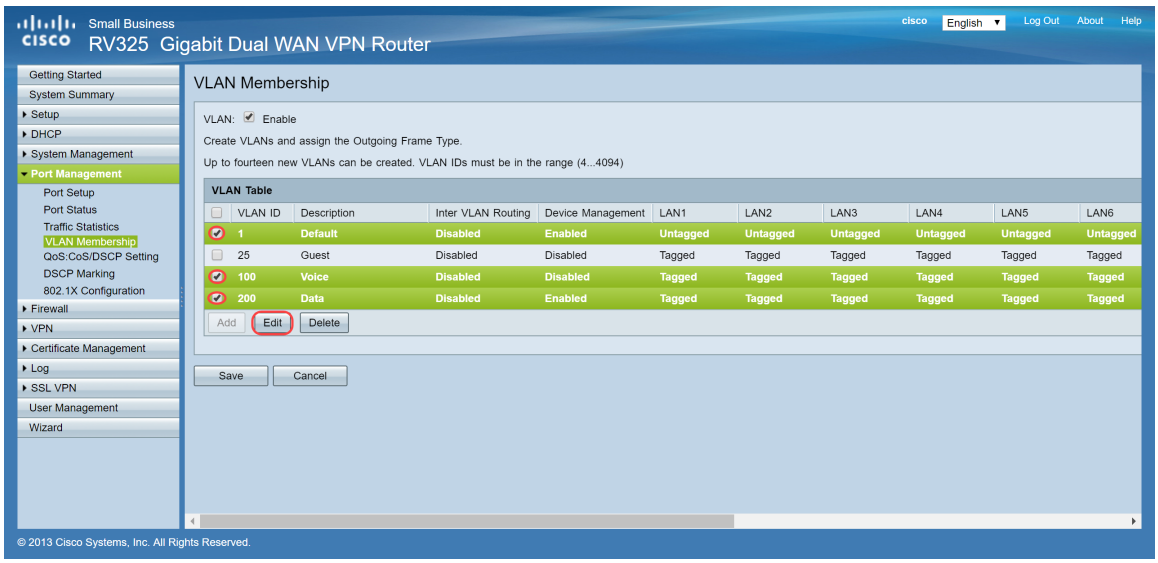


Passaggio 4. Immettere un numero VLAN nel campo *VLAN ID*. Gli ID VLAN devono essere compresi tra 4 e 4094. nell'esempio, il valore 200 viene usato per i dati come ID VLAN. Quindi, immettere una descrizione per la VLAN nel campo *Description* (Descrizione). I dati vengono immessi come esempio per la descrizione. Quindi fare clic su **Salva**.

Nota: la VLAN 100 per la voce è stata creata per impostazione predefinita su questo router. È possibile creare fino a quattordici nuove VLAN.



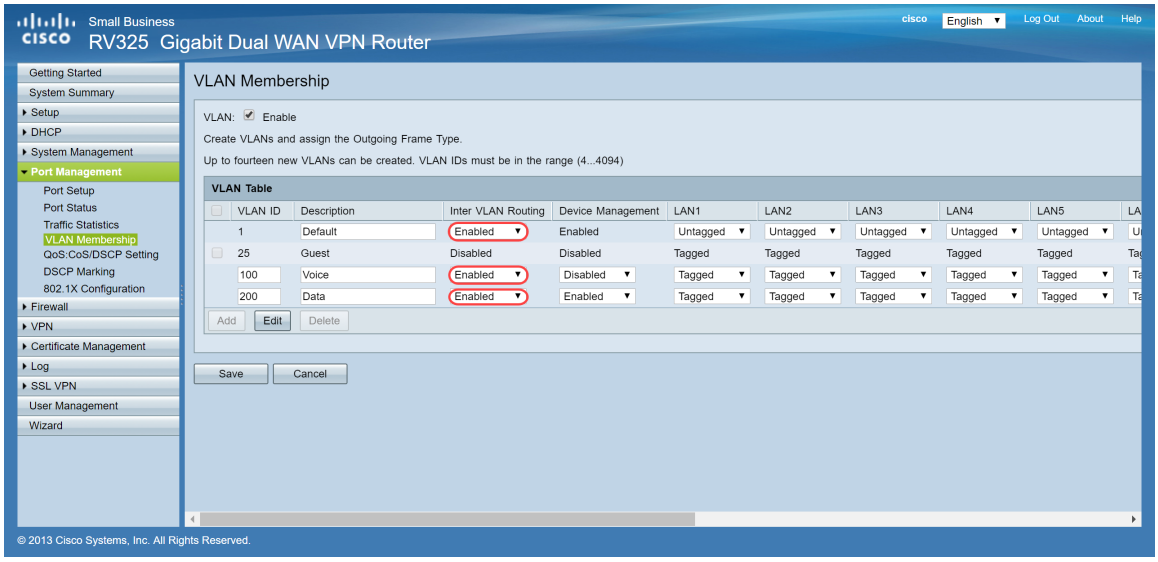
Passaggio 5. Per modificare una VLAN, selezionare la casella di controllo della VLAN appropriata. nell'esempio, verranno modificate le VLAN 1, 100 e 200. Quindi, fare clic su **Edit** (Modifica) per modificare le VLAN.



Passaggio 6. (Facoltativo) Nell'elenco a discesa *Routing tra VLAN*, selezionare **Enabled** (Abilitato) o **Disabled** (Disabilitato) per instradare i pacchetti da una VLAN a un'altra. L'abilitazione di questa funzionalità è utile perché gli amministratori della rete interna potranno accedere in remoto ai dispositivi per risolvere i problemi. In questo modo si riduce il tempo necessario per commutare continuamente le VLAN e accedere ai dispositivi.

- Disabilitato: indica che il routing tra VLAN è inattivo
- Enabled: indica che il routing tra VLAN è attivo su questa VLAN. Il routing tra VLAN indirizza i pacchetti solo tra le VLAN per cui è stato abilitato.

Nota: nell'esempio, verrà abilitato il routing tra VLAN per le VLAN con ID 1, 100 e 200.



Passaggio 7. Selezionare l'opzione desiderata dall'elenco a discesa relativo alla porta LAN con cui si è connessi e l'impostazione deve corrispondere alla porta connessa. Se si è connessi a più porte, è necessario scegliere le stesse impostazioni per ogni porta connessa. L'impostazione predefinita è tagged, ma per la VLAN 1 non è tagged.

Nota: se si abilita il routing tra VLAN nel passaggio 6, è necessario contrassegnare la VLAN per distinguere il traffico.

Con tag

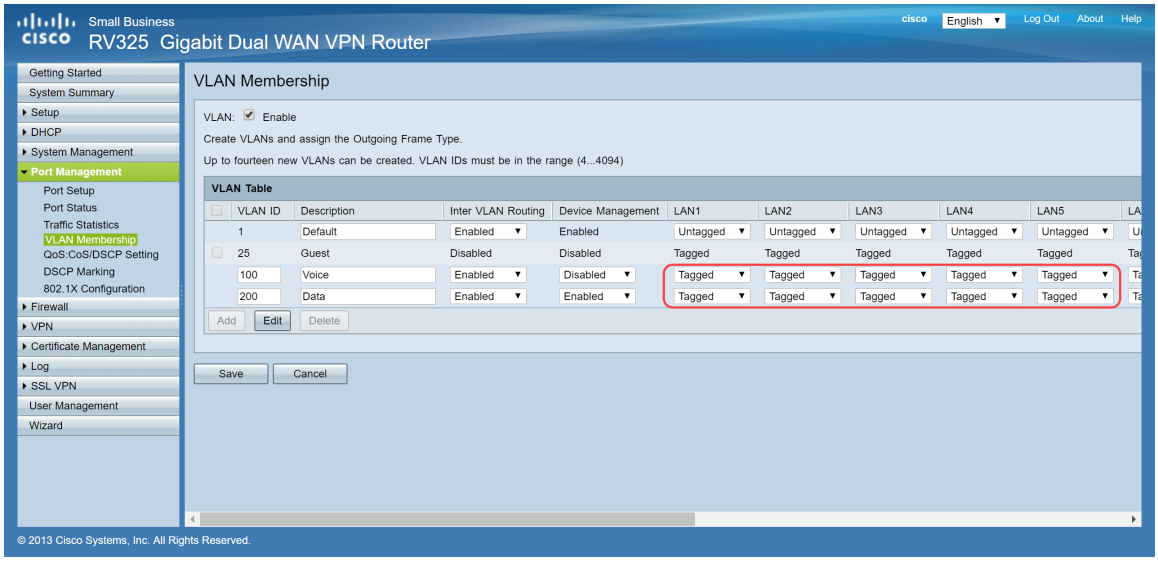
- Indica che l'associazione tra la porta e la VLAN è contrassegnata.
- L'opzione Tagged (Contrassegnata) viene usata per determinare la VLAN a cui appartiene il traffico tramite l'ID VLAN univoco quando si creano più VLAN per la stessa porta.

Senza tag

- Indica che l'associazione tra la porta e la VLAN è senza tag.
- Viene usata quando si crea una sola VLAN e il traffico riconosce la VLAN. Solo una VLAN può essere contrassegnata come senza tag per ciascuna porta LAN.
- Se la VLAN predefinita è sulla porta, deve essere sempre senza tag anche se la porta ha più VLAN.

Escluso

- Indica che l'interfaccia non è un membro della VLAN.
- Se si sceglie questa opzione, il traffico tra la VLAN e la porta viene disabilitato.



Passaggio 8. Fare clic su **Save** (Salva) per salvare le impostazioni.

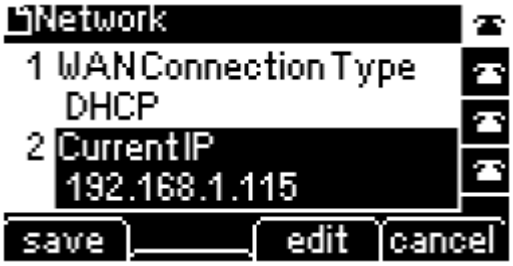
Nota: sul router, è possibile accedere all'utility basata sul Web e selezionare **DHCP > DHCP Setup** per configurare le VLAN su una subnet specifica. Per impostazione predefinita, le VLAN sono configurate per essere su una subnet diversa.

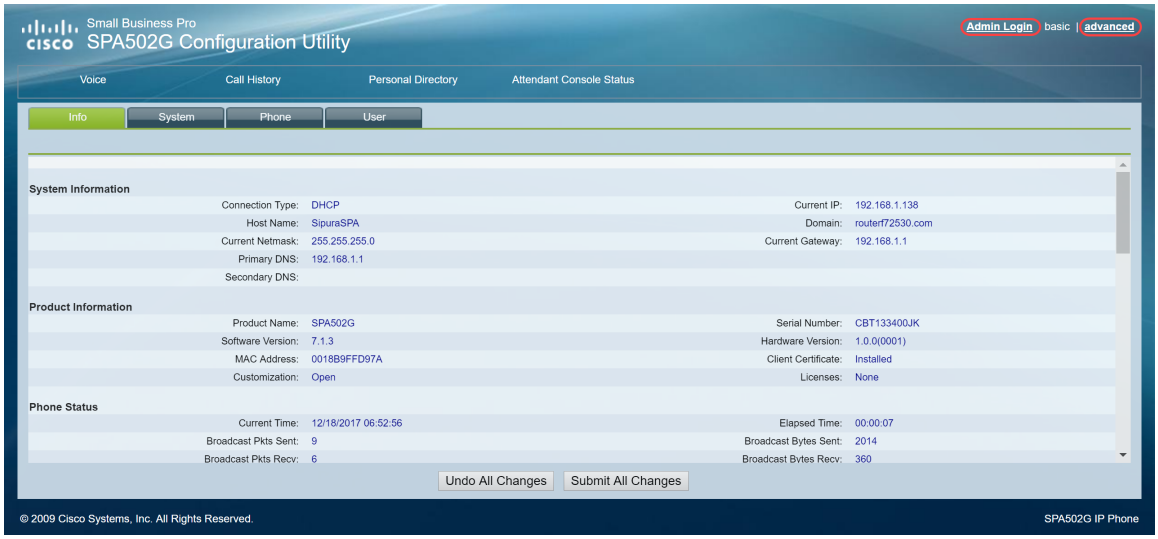
Configurazione dei telefoni SPA/MPP

Gli utenti possono anche configurare i telefoni in modo da estrarre un profilo da una posizione configurata manualmente, una posizione trovata tramite l'opzione DHCP 150 o da un server Cisco EDOS. Di seguito è riportato un esempio di configurazione manuale.

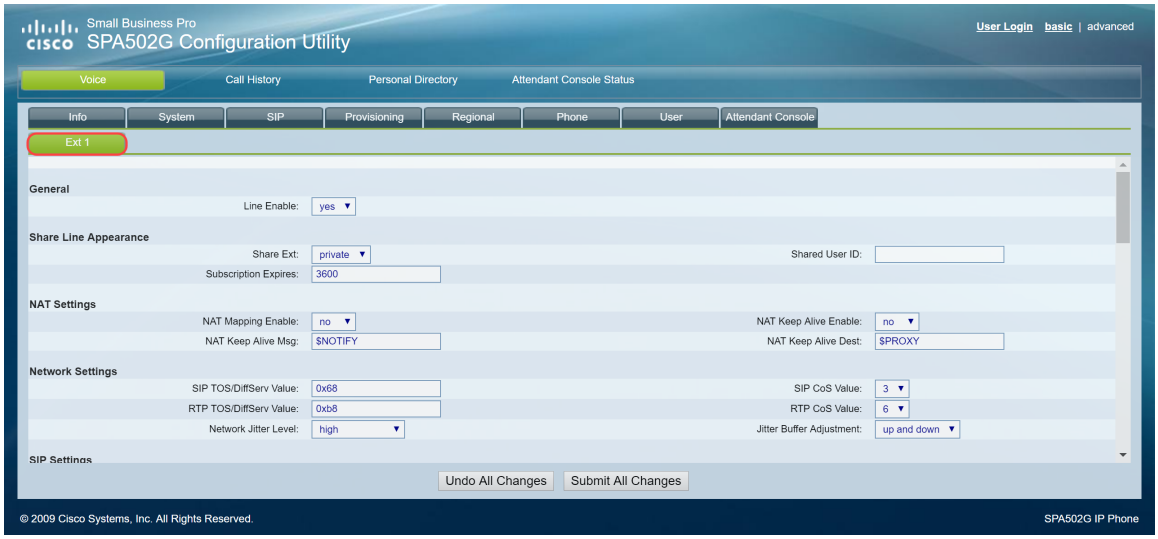
Passaggio 1. Immettere l'indirizzo IP dell'SPA/MPP sul browser e selezionare **Admin Login** (Accesso amministratore), quindi **Advanced** (Avanzate).

Nota: la configurazione del telefono SPA/MPP può variare a seconda del modello. Nell'esempio riportato viene utilizzato SPA502G. Per trovare l'indirizzo IP del telefono IP, selezionare **DHCP > DHCP Status** (DHCP > Stato DHCP) sul router (varia a seconda del modello). In alternativa, è possibile premere il pulsante **Setup** (Imposta) e selezionare **Network** (Rete) sul telefono Cisco (i menu e le opzioni possono variare a seconda del modello di telefono).



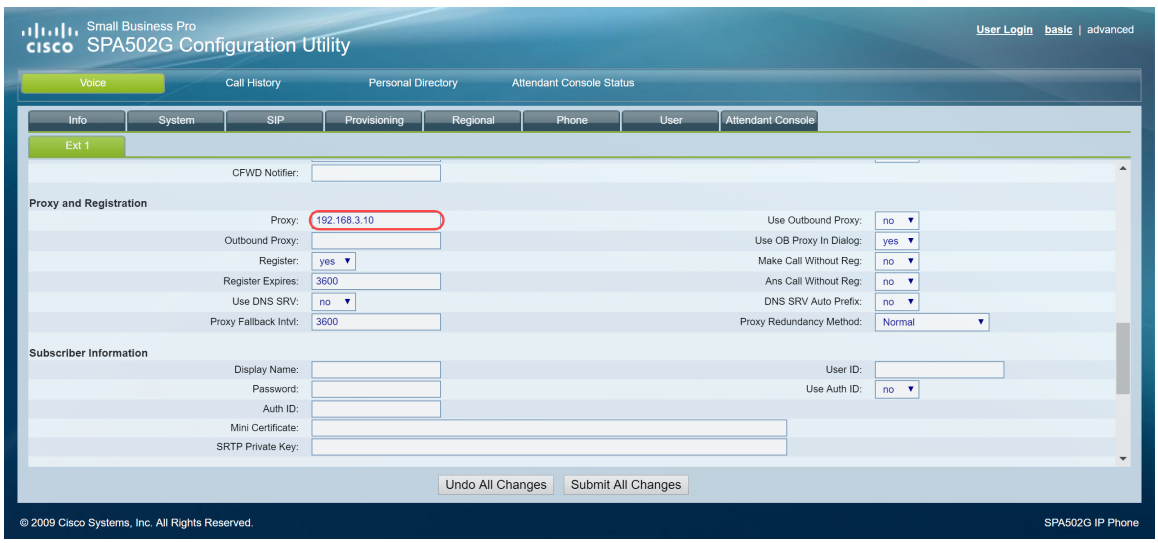


Passaggio 2. Passare a **Voce > Est 1**. Viene visualizzata la pagina di estensione.



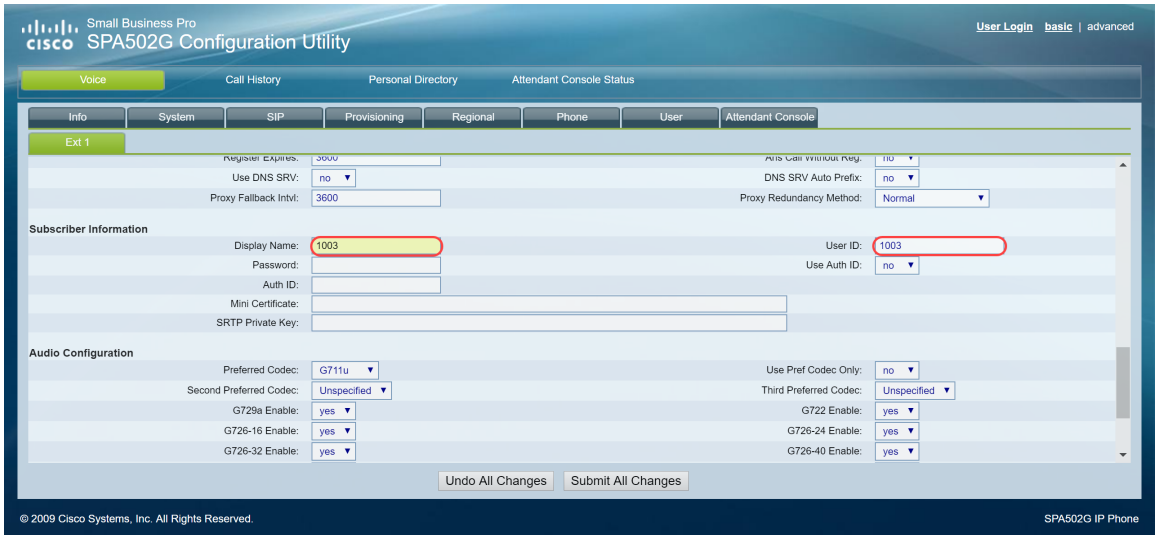
Passaggio 3. Nella sezione *Proxy e registrazione*, digitare il server proxy nel campo *Proxy*. Nell'esempio, l'indirizzo del Raspberry Pi (192.168.3.10) verrà utilizzato come server proxy. La VLAN 100 è sulla subnet con 192.168.3.x.

Nota: più avanti in questo articolo, sarà possibile configurare l'indirizzo IP del Raspberry Pi, per ulteriori informazioni fare clic sul collegamento per essere reindirizzati a quella sezione: Modifica dell'indirizzo del Raspberry Pi per essere su una subnet diversa.



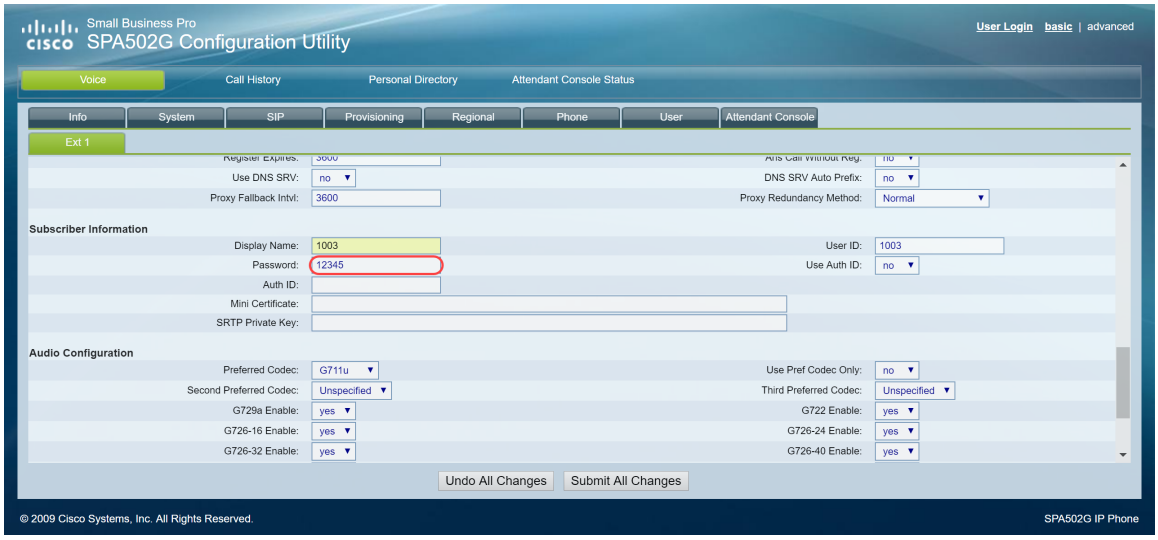
Passaggio 4. In *Informazioni sottoscrittore*, immettere il nome visualizzato e l'ID utente (numero di estensione) per l'estensione condivisa. In questo esempio verrà utilizzata l'estensione 1003.

Nota: l'estensione 1003 è già stata creata e configurata sul Raspberry Pi.

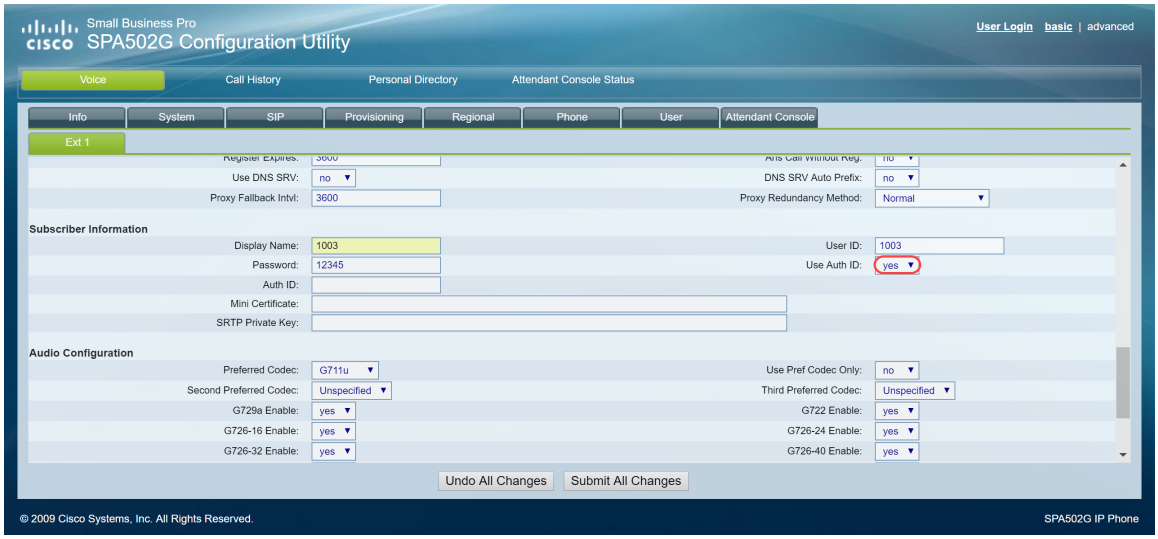


Passaggio 5. Immettere la password dell'estensione configurata nella sezione Estensione Raspberry Pi. Questo è anche noto come *Secret* nella *Modifica Estensione* sezione in Raspberry Pi. Nell'esempio è stata utilizzata la password **12345**.

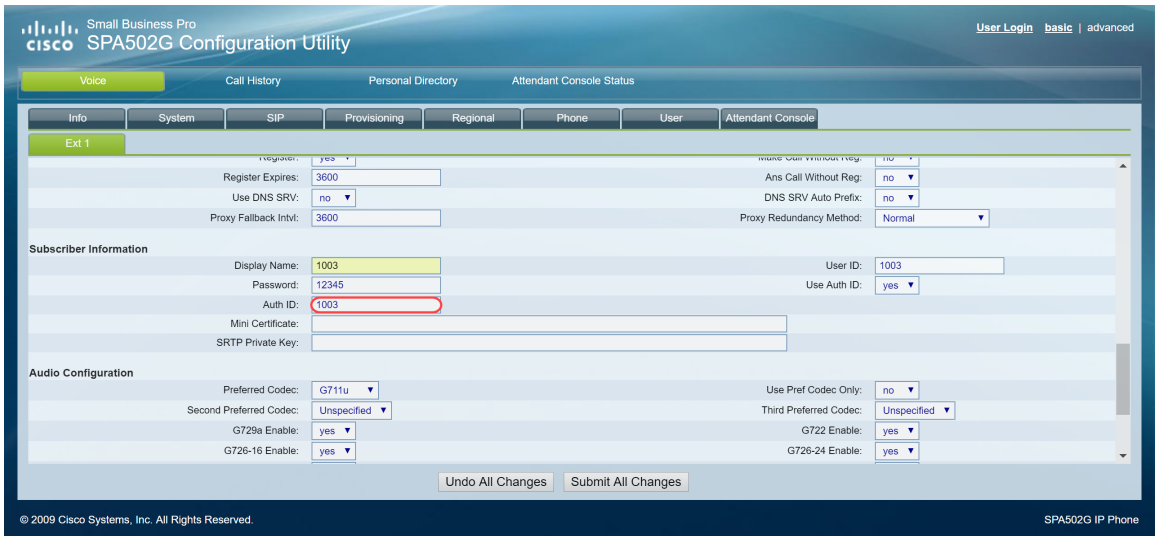
Nota: la password **12345** è stata utilizzata solo come esempio; si consiglia una password più complessa.



Passaggio 6. Selezionare l'opzione desiderata dall'elenco a discesa *Usa ID autenticazione*. Le opzioni sono **Sì** e **No**. Per abilitare l'autenticazione SIP (Session Initiation Protocol), in cui i messaggi SIP possono essere contestati per determinare se sono autorizzati prima della trasmissione, scegliere **Sì** dall'elenco a discesa *ID autenticazione*. Nell'esempio riportato di seguito è stato scelto **Sì** (Yes).



Passaggio 7. Immettere l'interno che si sta tentando di configurare per questo telefono nel campo *ID autenticazione*. ID di autenticazione per l'autenticazione SIP.



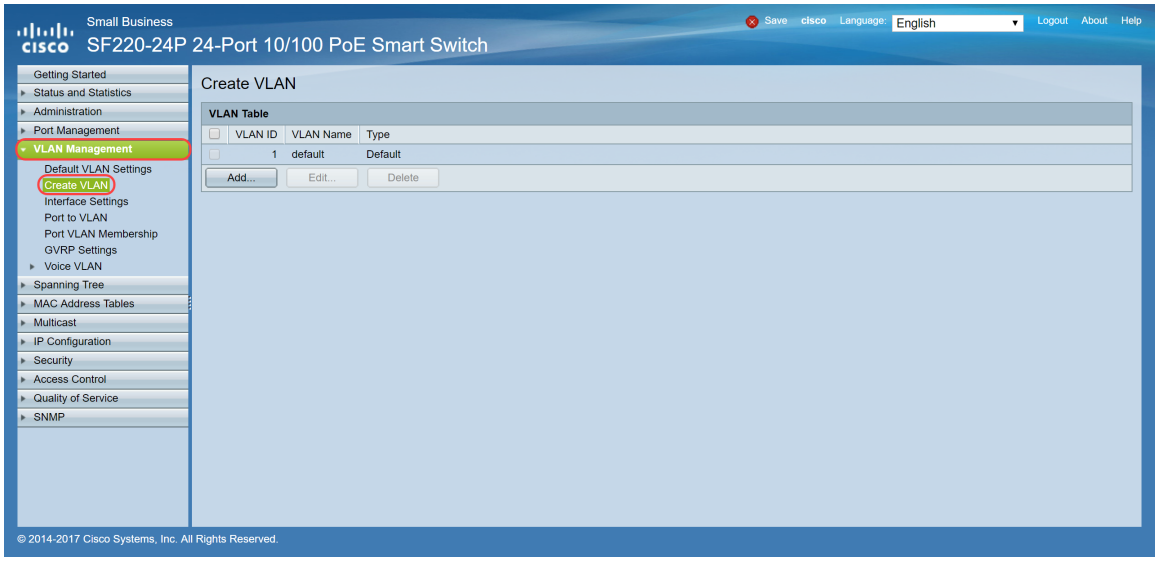
Passaggio 8. Quindi fare clic su **Invia tutte le modifiche.**

Nota: tornare al passo 1 della sezione Configurazione dei telefoni SPA/MPP se si hanno più telefoni SPA/MPP da configurare.

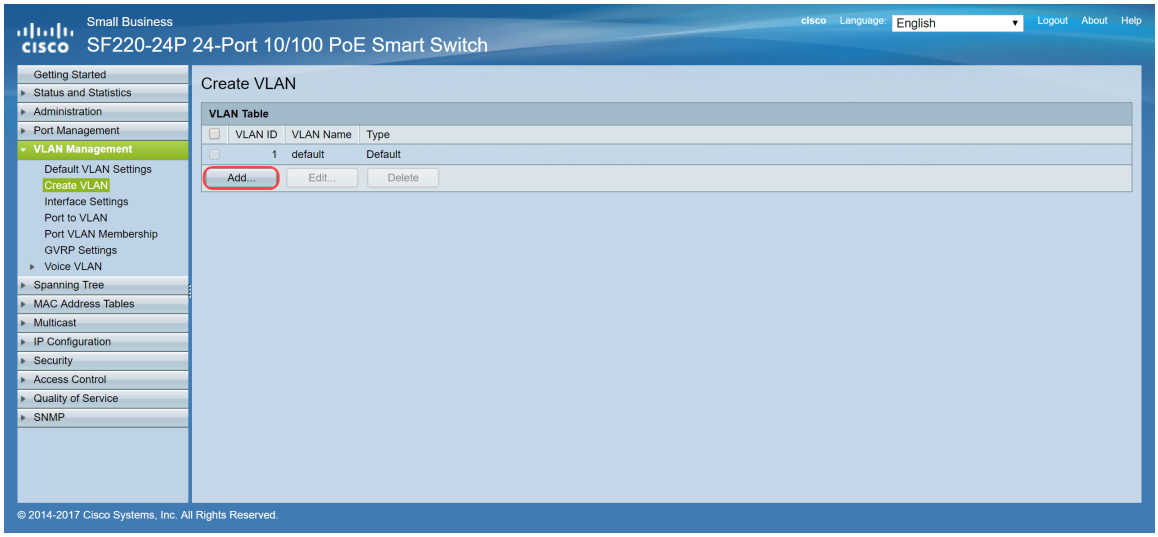
Configurazione delle VLAN sullo switch

Passaggio 1. Accedere all'utility basata sul Web e selezionare **Gestione VLAN > Crea VLAN**.

Nota: la configurazione può variare a seconda del dispositivo. Nell'esempio, viene usato l'SF220-24P per configurare le VLAN.

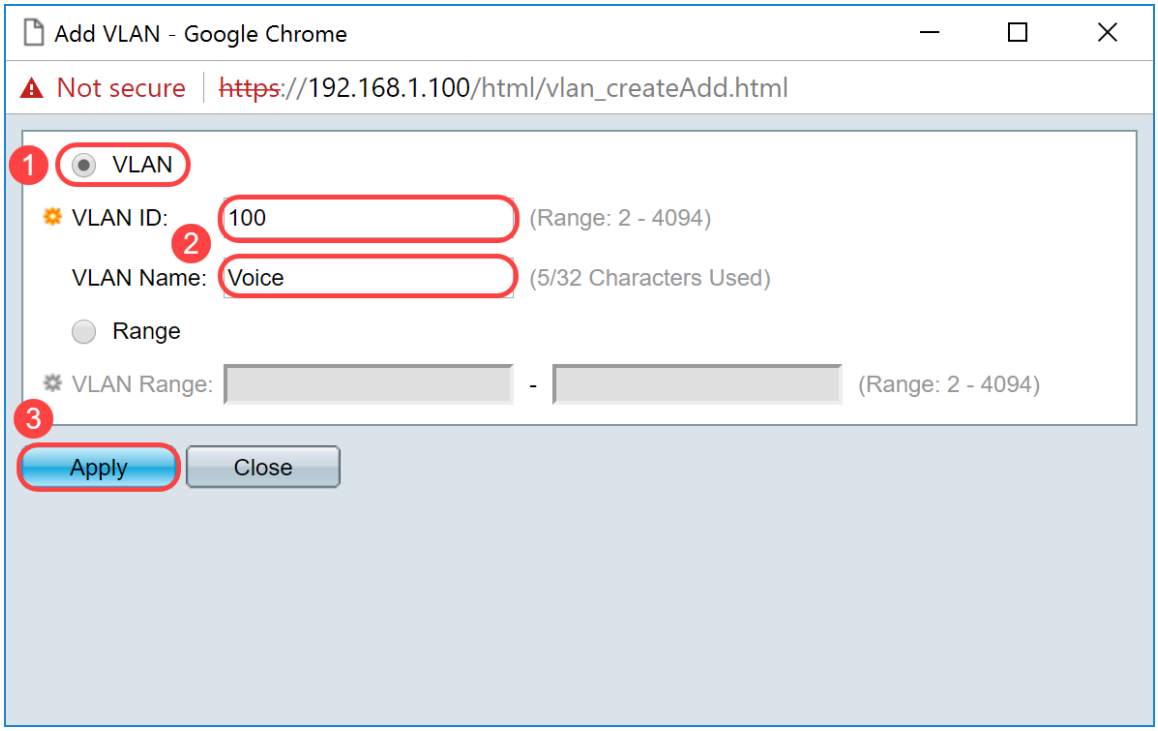


Passaggio 2. Fare clic su **Aggiungi...** per creare una nuova VLAN.



Passaggio 3. Per creare una singola VLAN, selezionare il pulsante di opzione **VLAN**. Immettere l'**ID** e il **nome della VLAN**. Quindi, fare clic su **Apply** (Applica) per salvare la VLAN. In questo esempio, verrà creata la VLAN 100 per la voce e la VLAN 200 per i dati.

Nota: alcune VLAN sono necessarie al sistema per l'utilizzo interno e non possono essere create immettendo i valori VID iniziale e finale, inclusi. Quando si utilizza la funzione **Range**, il numero massimo di VLAN che è possibile creare contemporaneamente è 100.

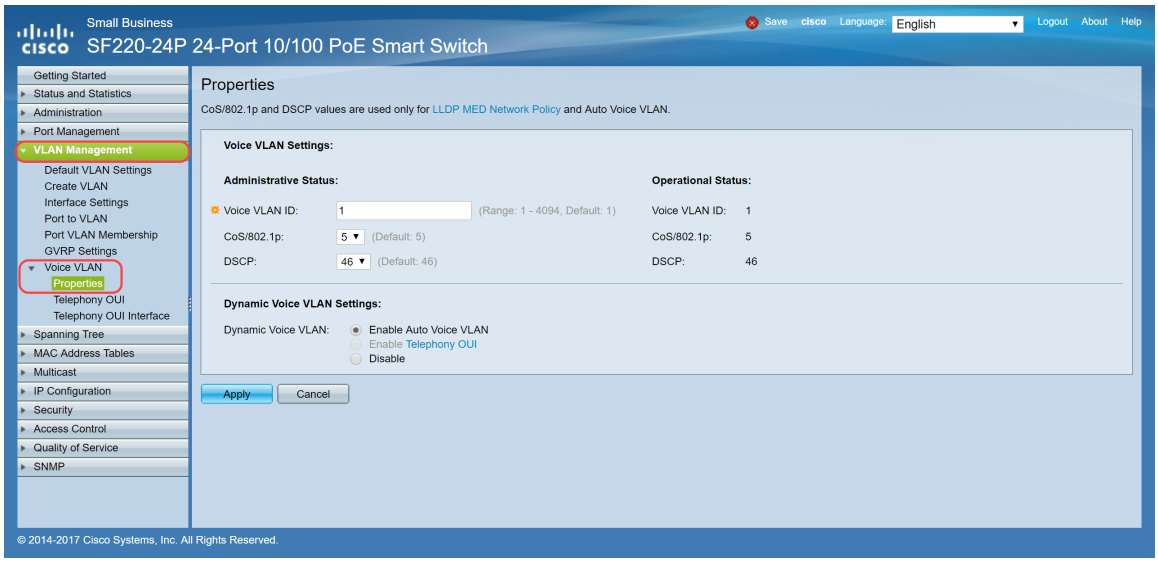


Nota: ripetere il passaggio 2 se è necessario creare un'altra singola VLAN.

Configurazione della VLAN vocale sullo switch

Passaggio 1. Accedere alla configurazione Web e selezionare **Gestione VLAN > Voice VLAN > Proprietà**.

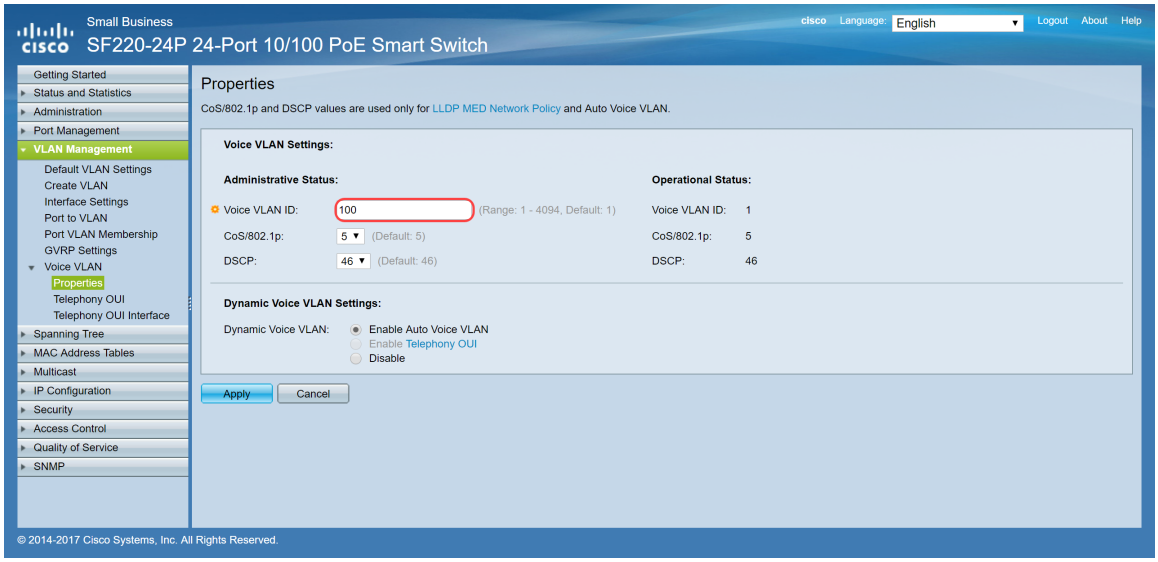
Nota: la configurazione della VLAN voce automatica applica automaticamente le impostazioni QoS della VLAN voce e assegna la priorità al traffico vocale.



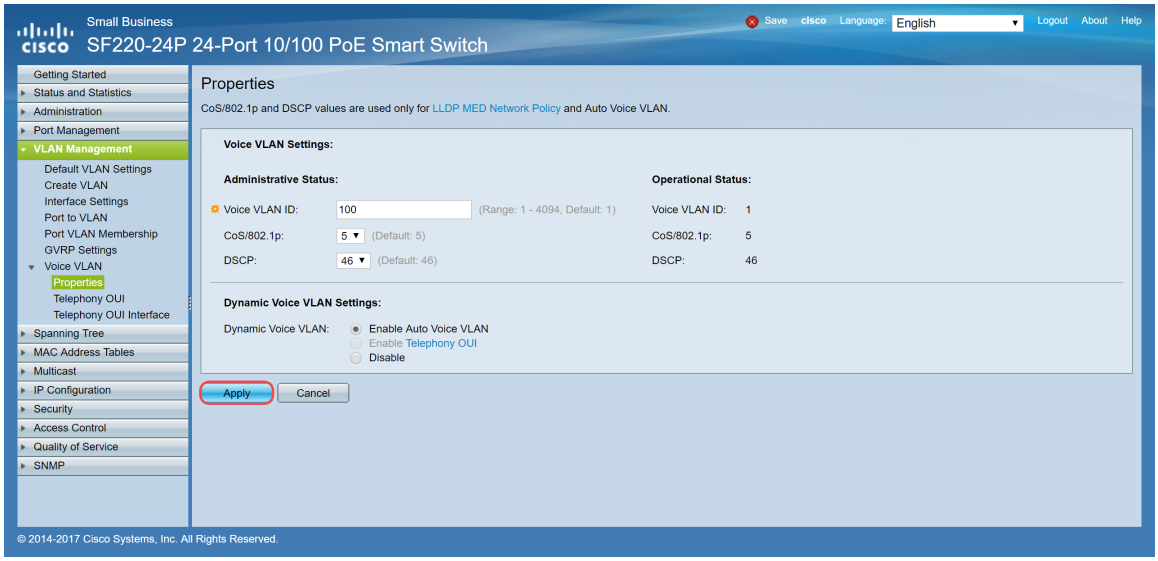
Passaggio 2. In *Stato amministrativo*, immettere la VLAN che deve essere la VLAN voce nel campo *ID VLAN voce*. nell'esempio, la VLAN 100 viene immessa come VLAN voce.

Nota: le modifiche all'ID della VLAN voce, alla classe di servizio (CoS)/802.1p e/o al DSCP (Differentiated Service Code Point) fanno in modo che il dispositivo annunci la VLAN voce amministrativa come VLAN voce statica. Se si seleziona l'opzione *Auto Voice VLAN activation* attivata da VLAN voce esterna, è necessario mantenere i valori predefiniti. Nell'esempio, CoS/802.1p

viene lasciato come valore predefinito 5 e DSCP come valore predefinito 46.



Passaggio 3. Fare clic su **Apply** (Applica) per salvare le impostazioni.

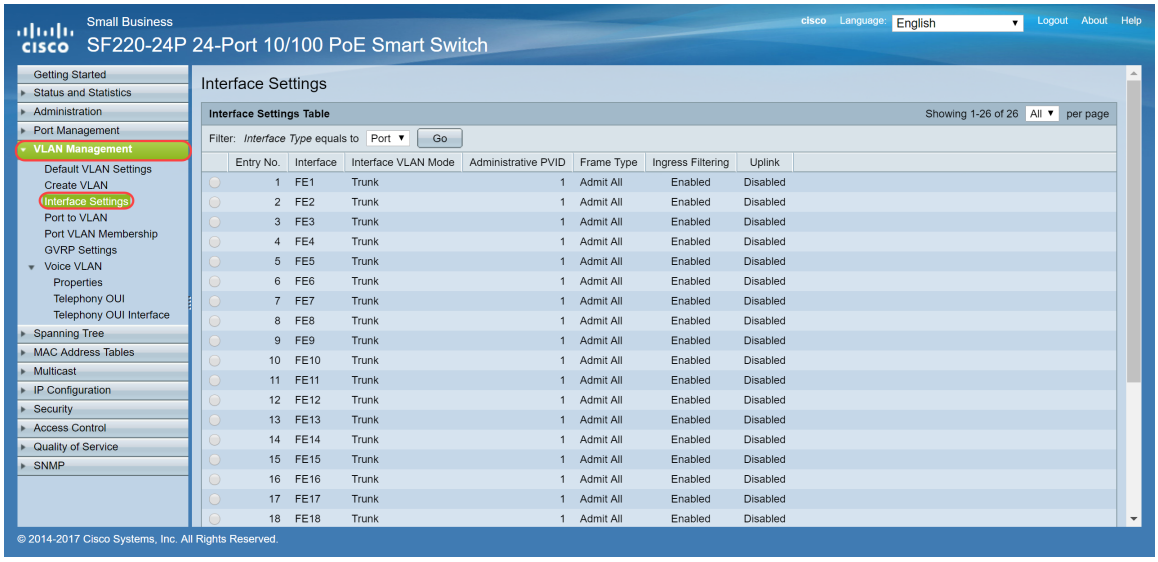


Configurazione delle impostazioni dell'interfaccia sullo switch

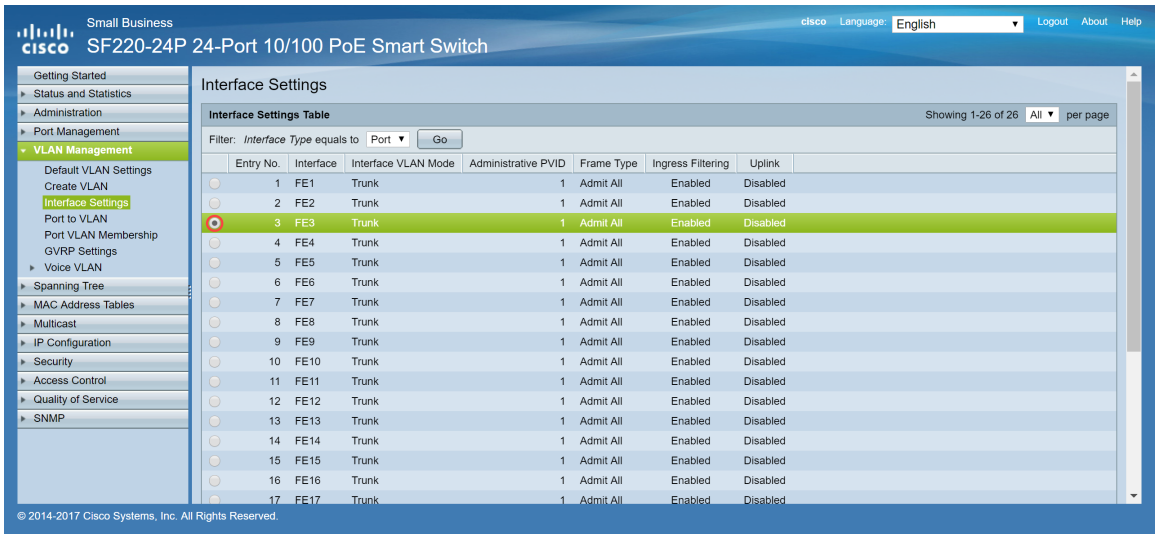
Le interfacce, le porte fisiche sullo switch, possono essere assegnate a una delle seguenti impostazioni:

- Generale: la porta può supportare tutte le funzioni definite nella specifica IEEE 802.1q. L'interfaccia può essere un membro con o senza tag di una o più VLAN.
- Accesso: può avere solo una VLAN configurata sull'interfaccia e può avere solo una VLAN.
- Trunk: può trasportare il traffico di più VLAN su un singolo collegamento e consente di estendere le VLAN sulla rete.
- Dot1p-Tunnel: attiva la modalità QinQ per l'interfaccia. Ciò consente all'utente di usare le proprie disposizioni VLAN (PVID) sull'intera rete del provider. Lo switch sarà in modalità QinQ quando dispone di una o più porte del tunnel dot1p.

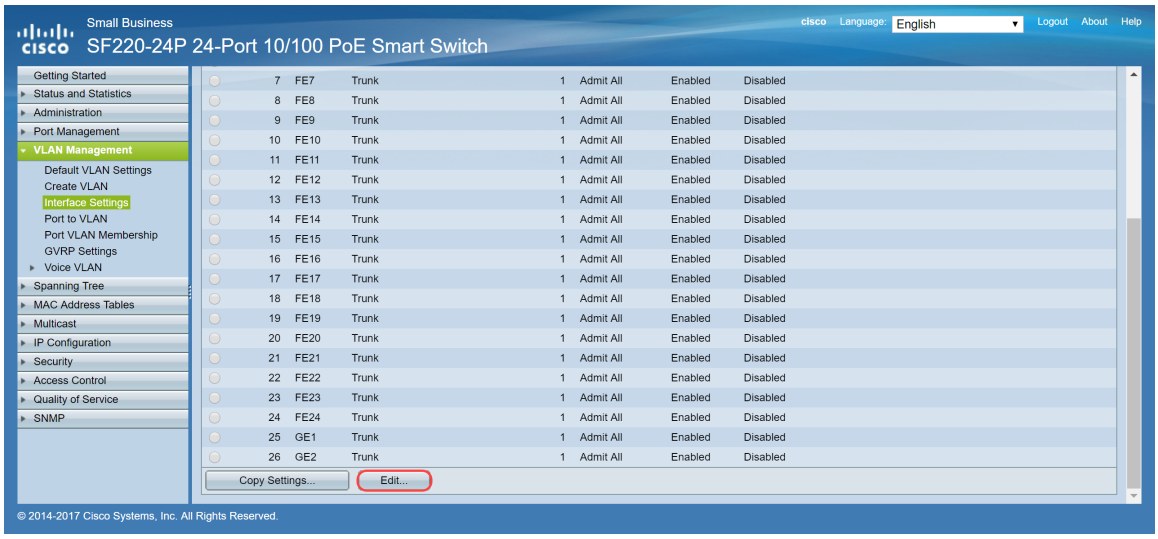
Passaggio 1. Accedere alla configurazione Web e selezionare **Gestione VLAN > Impostazioni interfaccia**.



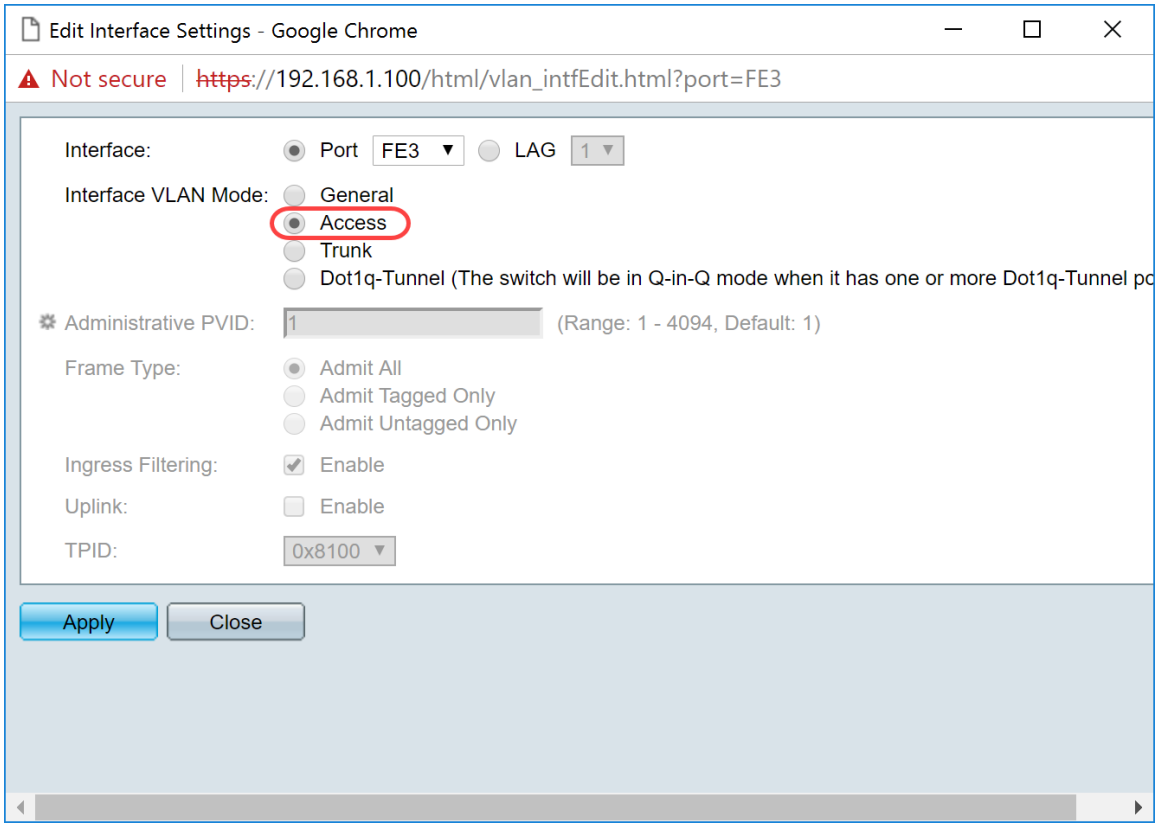
Passaggio 2. Selezionare la modalità interfaccia per la VLAN. In questo esempio, verrà configurata la porta Raspberry Pi (porta FE3) come porta di accesso.



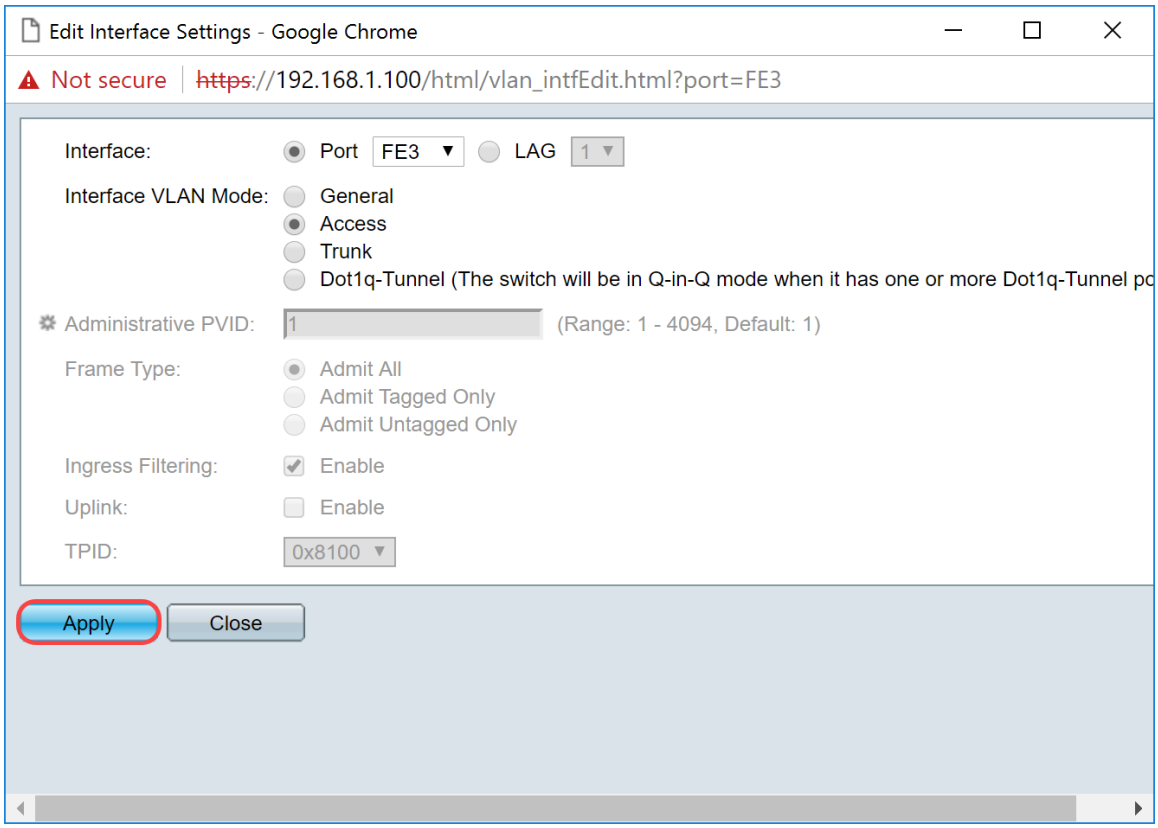
Passaggio 3. Quindi fare clic su **Modifica...** per modificare l'interfaccia.



Passaggio 4. Nel campo *Interface VLAN Mode*, selezionare **Access** per configurare l'interfaccia come membro senza tag di una singola VLAN.



Passaggio 5. Fare clic su **Apply** (Applica) per salvare le impostazioni.

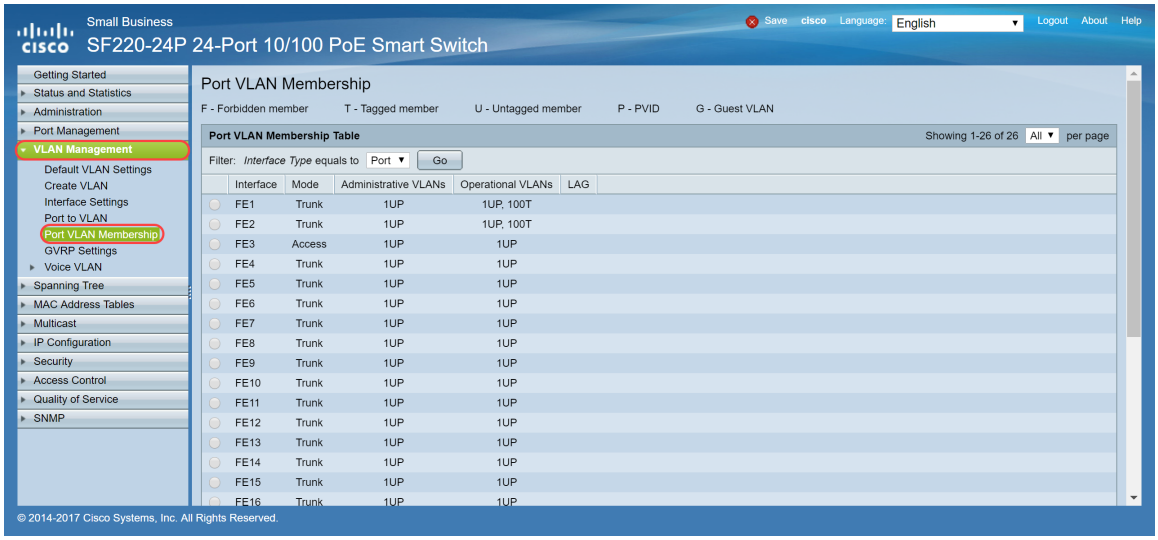


Configurazione dell'appartenenza della porta VLAN sullo switch

Dopo aver creato le VLAN, è necessario assegnare le VLAN alle porte che si desidera collegare.

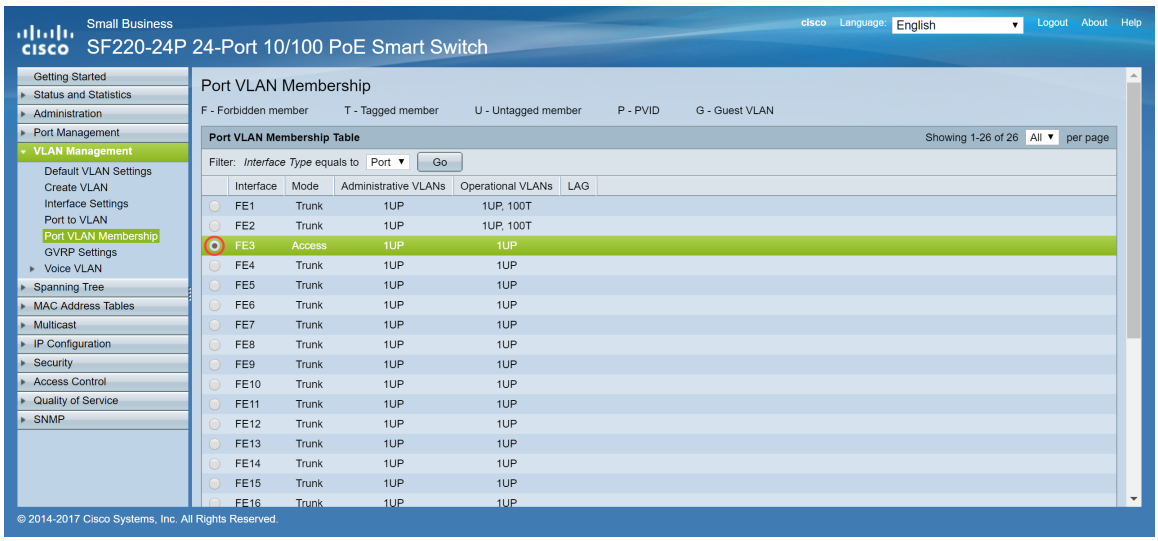
Passaggio 1. Accedere alla configurazione Web e selezionare **Gestione VLAN > Appartenenza alla**

porta VLAN.



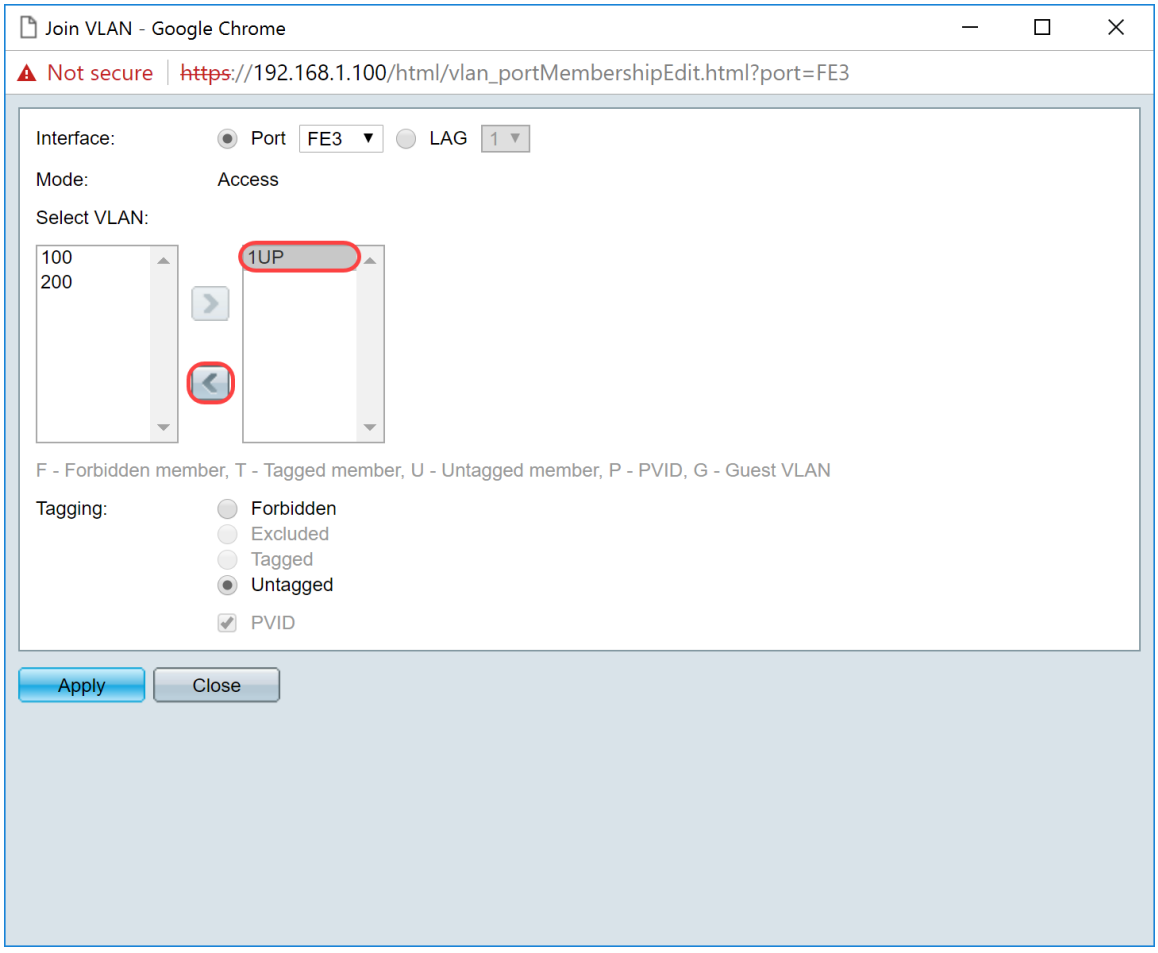
Passaggio 2. Nella *tabella Port VLAN Membership*, selezionare l'interfaccia che si desidera configurare per l'appartenenza della VLAN. In questo esempio, verrà configurato Raspberry Pi (Port: FE3) in modo che si trovi sulla VLAN 100.

Nota: i dispositivi voce verranno già configurati sulla VLAN voce selezionata nella sezione Configurazione della VLAN voce sullo switch.

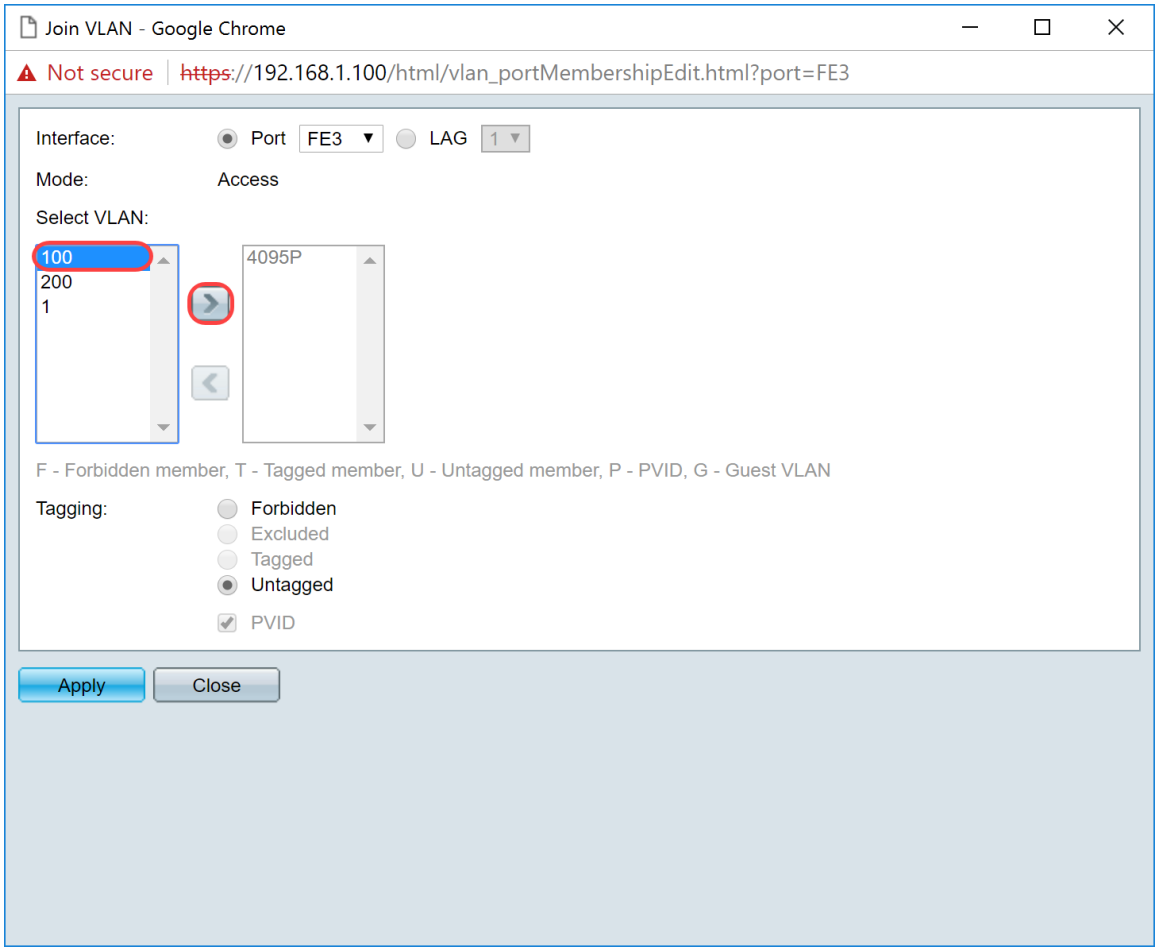


Passaggio 3. Fare clic su **Join VLAN...** per modificare la porta su cui configurare le VLAN.

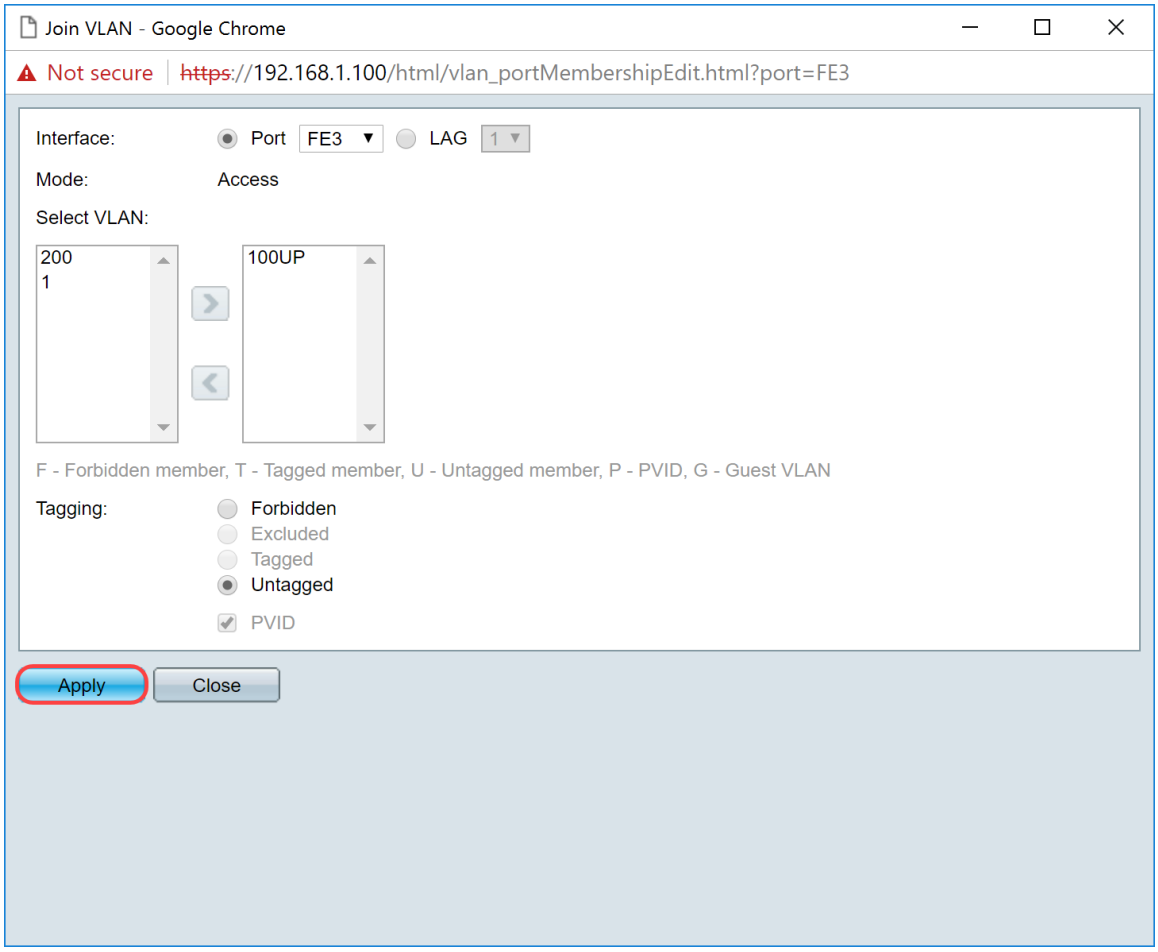
Passaggio 4. Selezionare **1UP** e fare clic su < per rimuovere la VLAN 1 dall'interfaccia nella sezione *Selezione VLAN*. Quando si tratta di una porta di accesso, è possibile aggiungere all'interfaccia solo 1 VLAN senza tag.



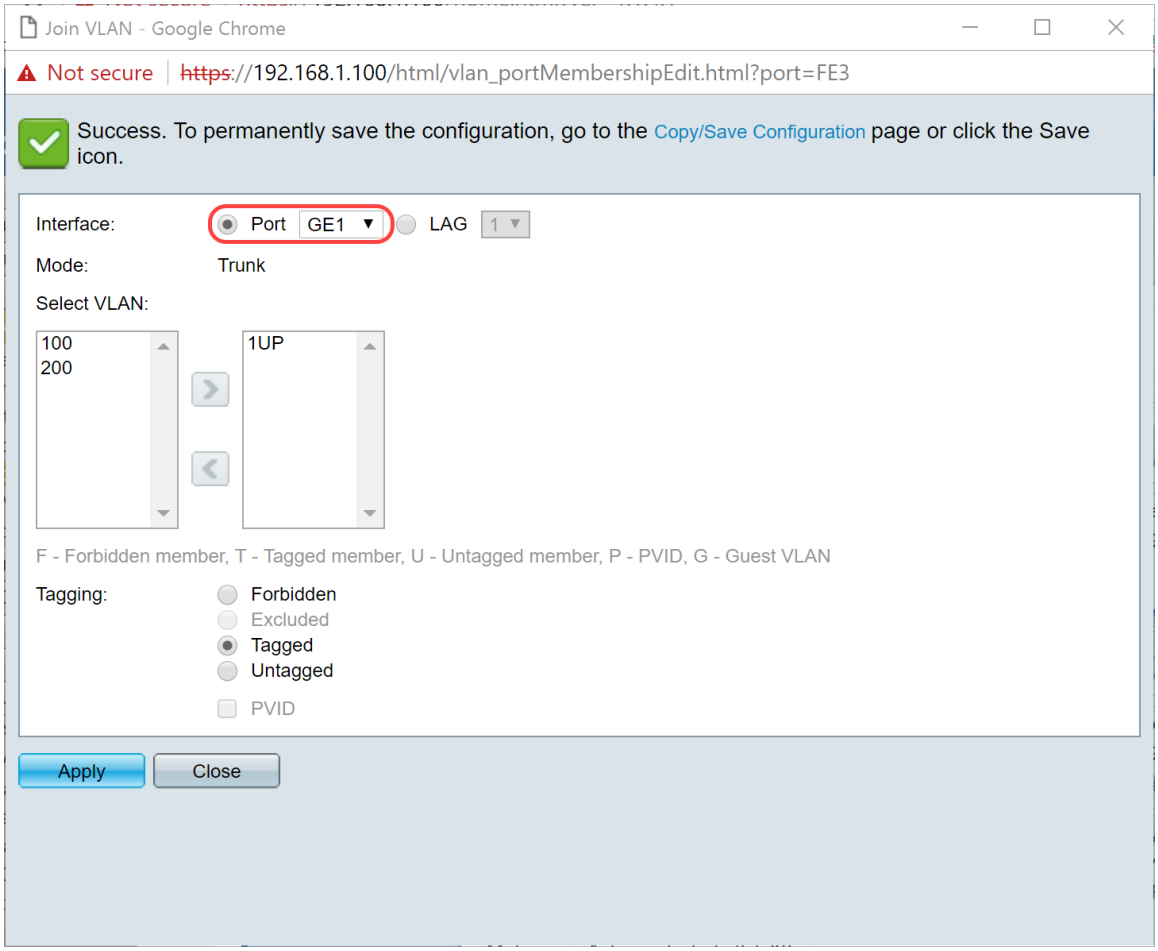
Passaggio 5. Selezionare **100** e fare clic su > per aggiungere la VLAN senza tag all'interfaccia.



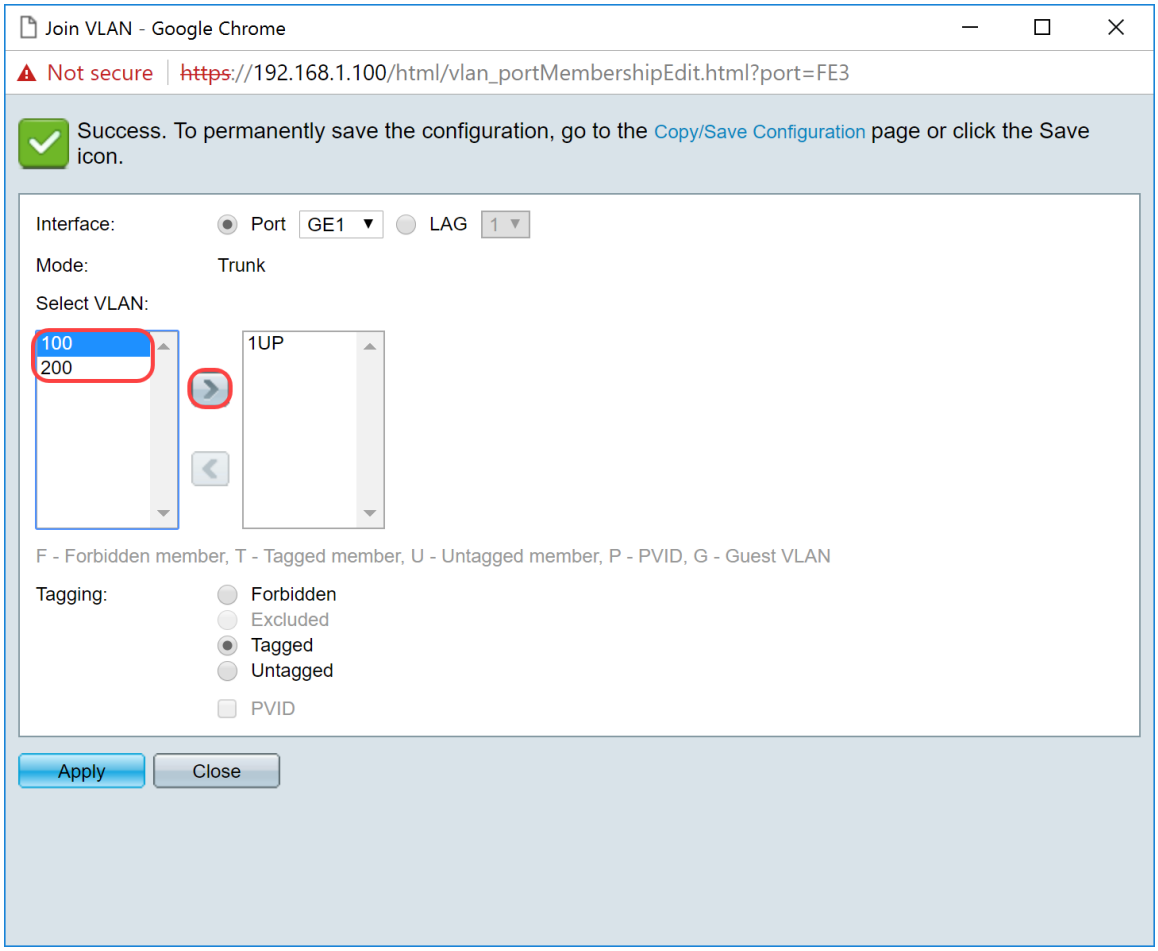
Passaggio 6. Fare clic su **Apply** (Applica) per salvare le impostazioni.



Passaggio 7. Nel campo *Interface* (Interfaccia), selezionare la porta di interfaccia collegata al router. Nell'esempio, la porta GE1 è selezionata.



Passaggio 8. Selezionare la VLAN che verrà aggiunta all'interfaccia selezionata e fare clic su > per aggiungerla nella sezione *Selezione VLAN*. Nell'esempio, verrà selezionata la VLAN **100** e la VLAN **200**.



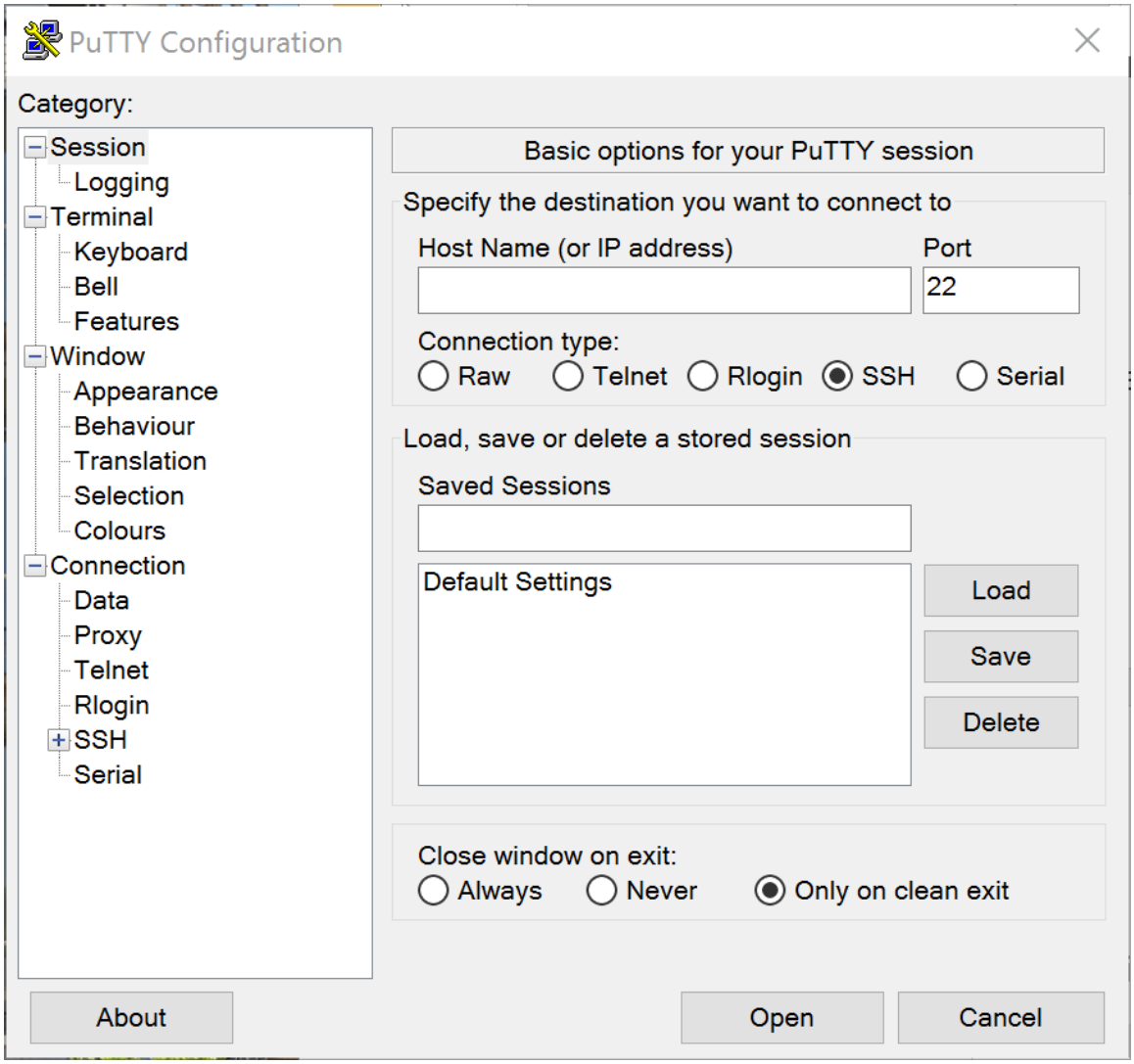
Passaggio 9. Fare clic su **Apply** (Applica) per salvare le impostazioni.

Nota: potrebbe essere necessario riavviare i telefoni IP per modificare l'indirizzo IP nella subnet corretta.

Modifica dell'indirizzo IP di Raspberry Pi in modo che si trovi su una subnet diversa

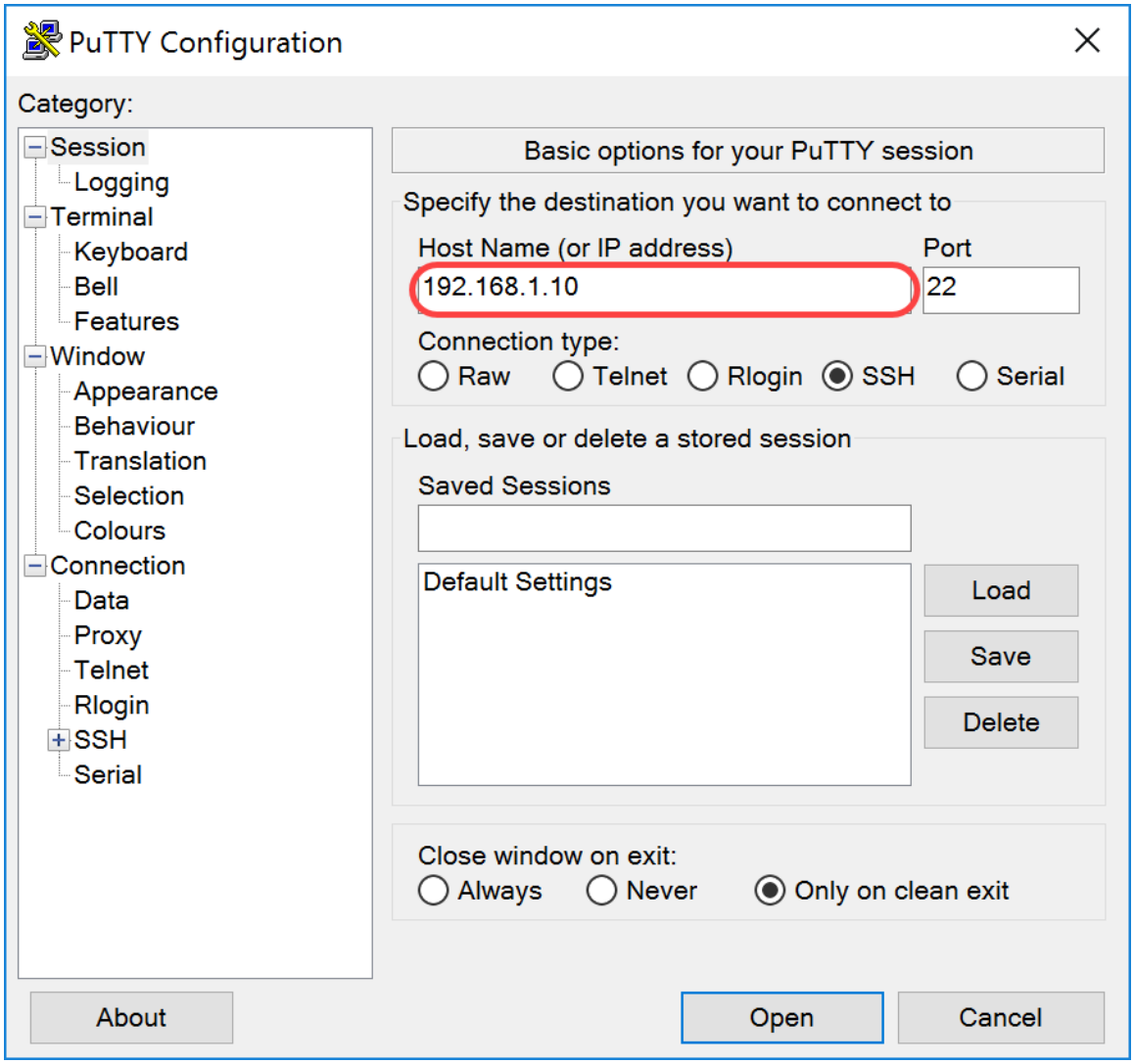
Passaggio 1. Collegare Raspberry Pi tramite Secure Shell (SSH) o collegare Raspberry Pi a un monitor per computer. Nell'esempio, verrà usato il protocollo SSH per configurare l'interfaccia Raspberry Pi.

Nota: la porta dello switch per il computer/notebook deve trovarsi sulla stessa VLAN dell'interfaccia Raspberry Pi e deve essere configurata come porta di accesso quando si configurano le impostazioni dell'interfaccia. Per ulteriori informazioni, vedere la sezione Configurazione delle impostazioni dell'interfaccia su uno switch e Configurazione dell'appartenenza della porta VLAN sullo switch in questo articolo. Per connettersi al protocollo SSH, verificare che l'indirizzo IP sia sulla stessa rete dell'IP del lampone. Se il dispositivo non si trova sulla stessa rete dell'API lampone, utilizzare un indirizzo IP statico e modificare manualmente l'indirizzo IP in modo che si trovi sulla stessa rete oppure digitare il comando **ipconfig /release** e **ipconfig/renew** al prompt dei comandi per ottenere un nuovo indirizzo IP. I client SSH possono variare a seconda del sistema operativo in uso. In questo esempio, PuTTY è stato usato per SSH nel Raspberry Pi. Per ulteriori informazioni sul protocollo SSH, fare clic qui.

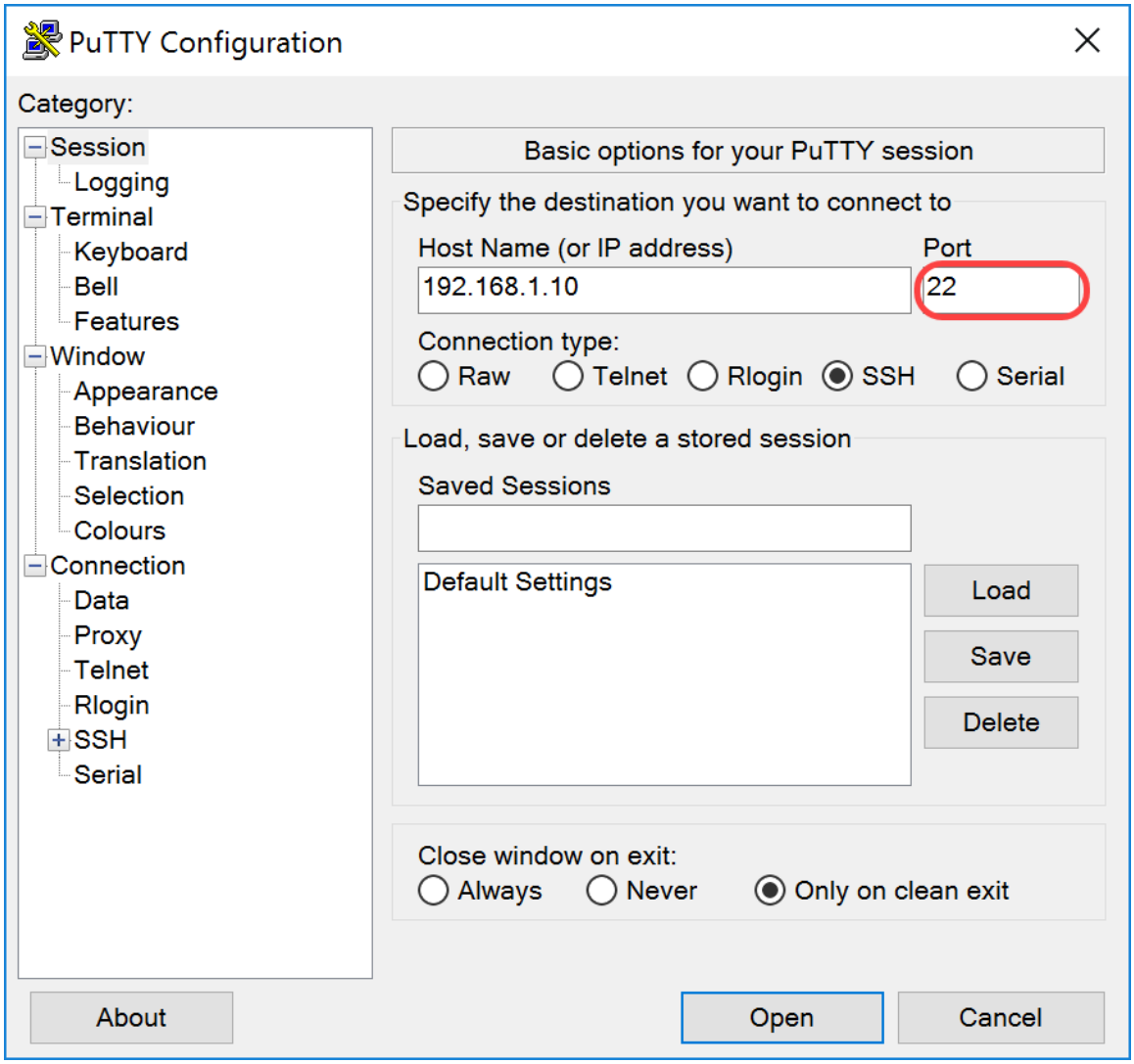


Passaggio 2. Digitare l'indirizzo IP del Raspberry Pi nel campo *Nome host (o indirizzo IP)*. Nell'esempio, viene immesso 192.168.1.10.

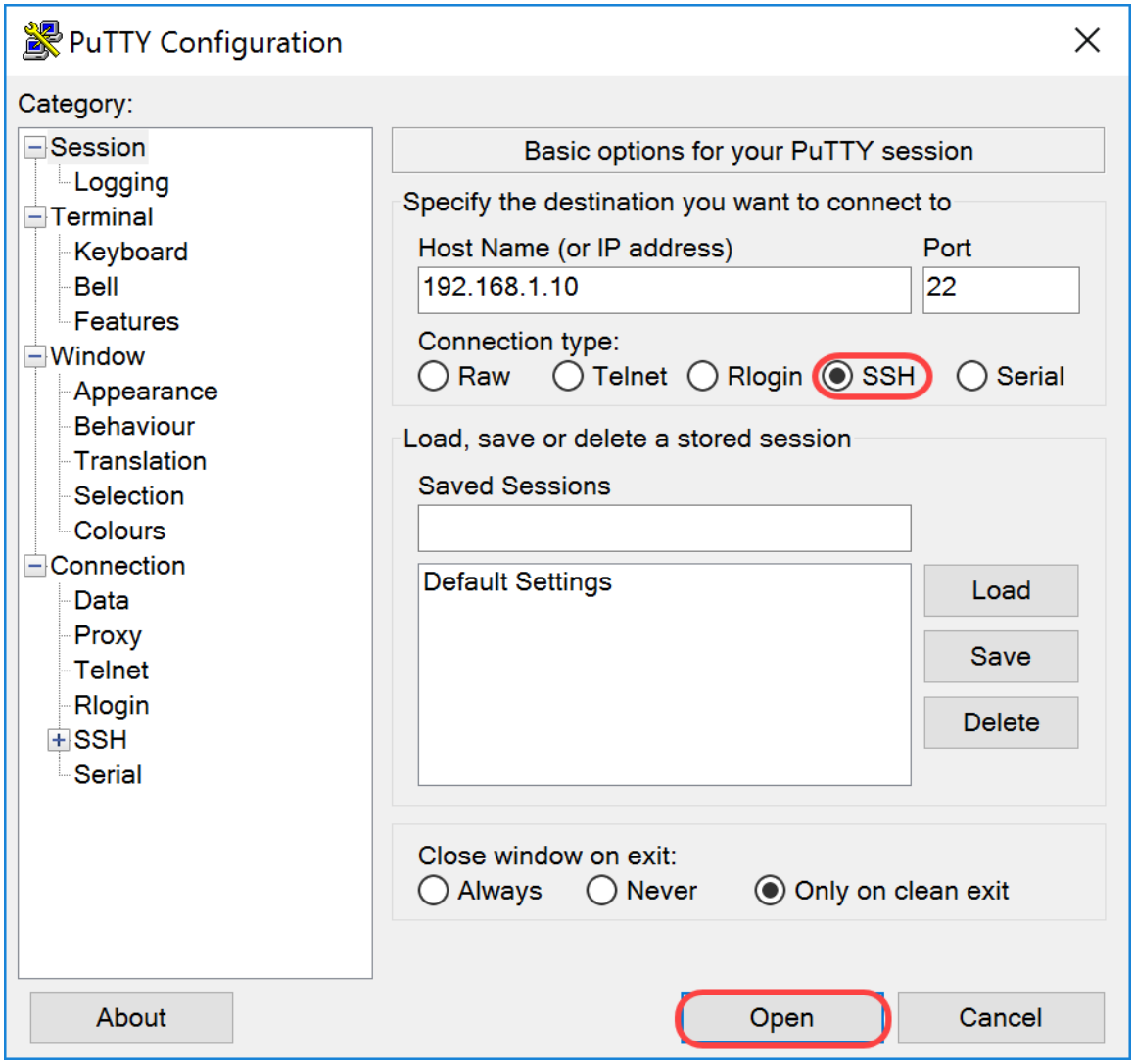
Nota: è possibile utilizzare la tabella DHCP nel router per trovare l'indirizzo del Raspberry Pi. In questo documento, questo Raspberry Pi è stato preconfigurato per avere un indirizzo IP statico.



Passaggio 3. Immettere **22** come numero di porta nel campo *Porta*. La porta 22 è la porta standard per il protocollo SSH.

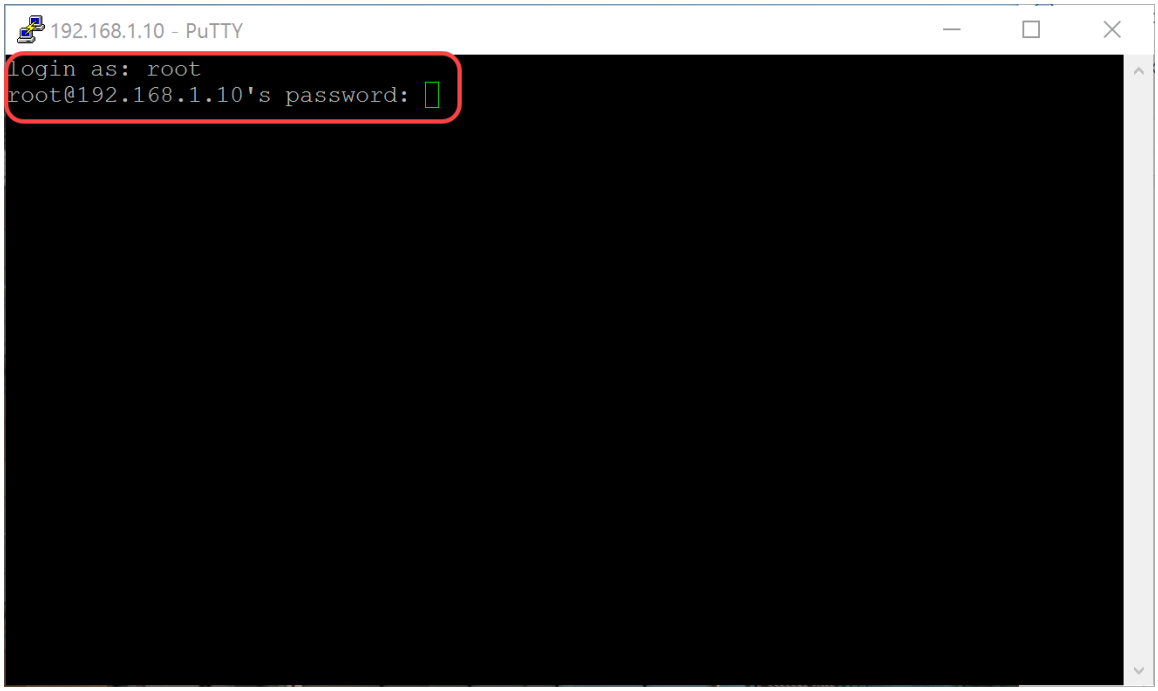


Passaggio 4. Nella sezione *Tipo di connessione:* fare clic sul pulsante di opzione **SSH** per scegliere SSH come metodo di connessione allo switch. Quindi fare clic su **Apri** per avviare la sessione.



Passaggio 5. Immettere il nome utente e la password di RasPBX nel campo *login as* and *password*.

Nota: L'utente predefinito: **root** e la password predefinita: **raspberry**

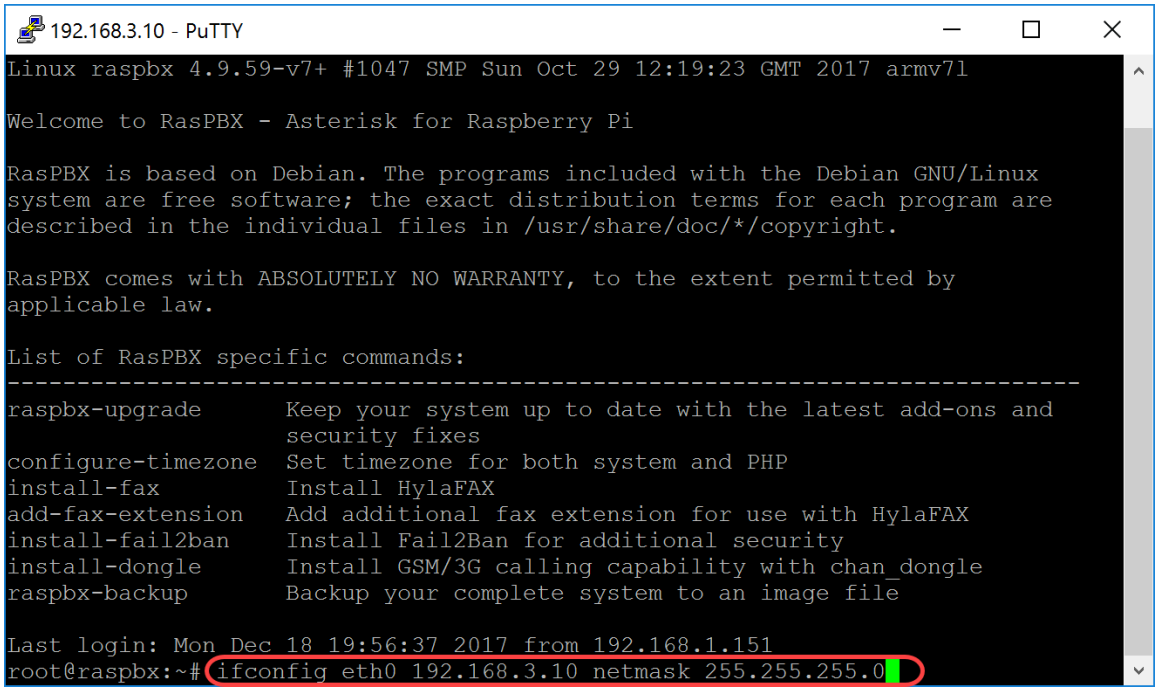


Passaggio 6. Per modificare l'indirizzo IP della rete Ethernet in indirizzo IP statico, digitare ifconfig

eth0 [IP address] netmask [netmask]. Nell'esempio, utilizzeremo 192.168.3.10 e la netmask 255.255.255.0

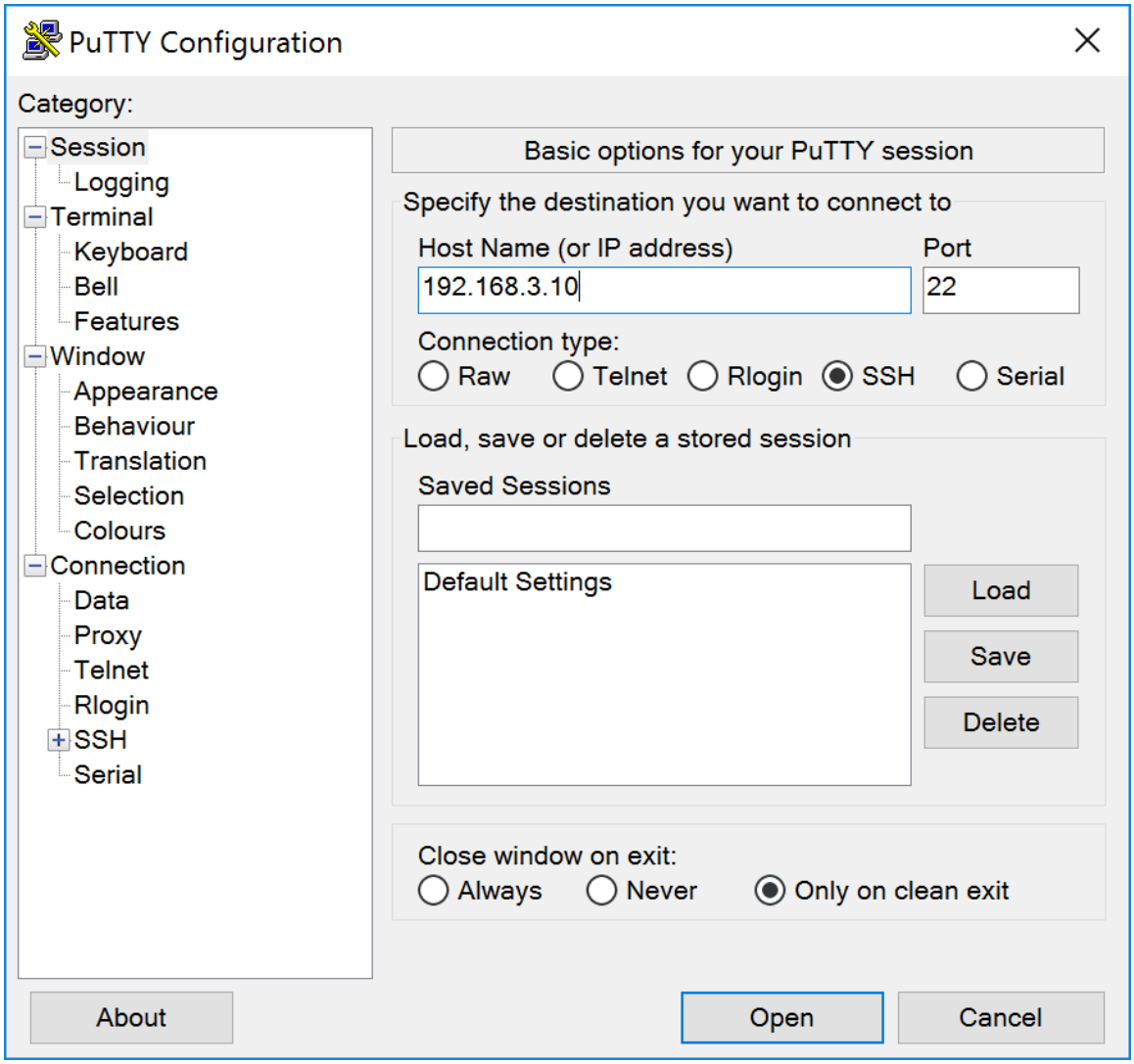
```
ifconfig eth0 192.168.3.10 netmask 255.255.255.0
```

Nota: quando si modifica l'indirizzo IP, si verrà disconnessi dalla sessione. Per collegarsi di nuovo al Raspberry Pi, il computer/laptop deve trovarsi sulla stessa subnet del Raspberry Pi (192.168.3.x).



Passaggio 7. Connettersi nuovamente al Raspberry Pi utilizzando l'indirizzo IP statico configurato nel passaggio 6. Nell'esempio, viene usata la versione 192.168.3.10 per la connessione.

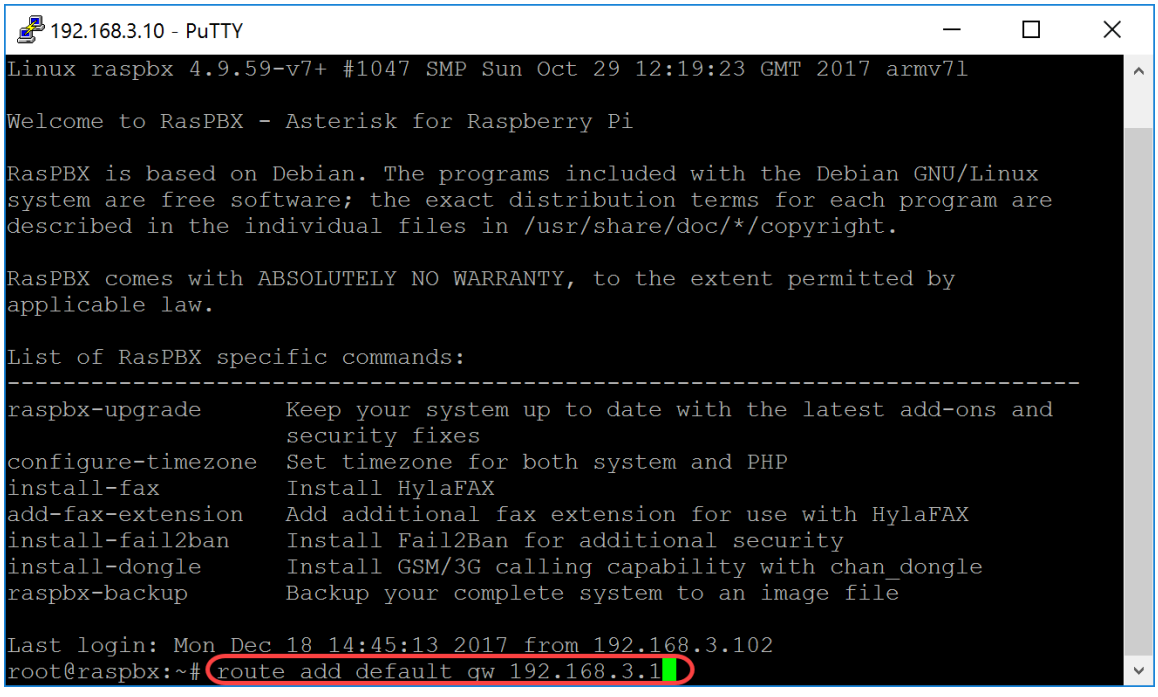
Nota: verificare che il computer/notebook si trovi sulla stessa subnet del lampone Pi e della VLAN. Se il computer/laptop si trova sulla stessa VLAN dell'interfaccia IP del lampone e non si dispone dell'indirizzo IP corretto, è possibile andare al prompt dei comandi e digitare **ipconfig /release** e quindi **ipconfig /renew** per richiedere un nuovo indirizzo IP oppure è possibile configurare il dispositivo in modo che abbia un indirizzo IP statico nelle proprietà Ethernet.



Passaggio 8. Nella riga di comando digitare route add default gw [indirizzo IP router della subnet] per aggiungere un gateway predefinito.

Nota: per **visualizzare** la tabella di routing, è possibile utilizzare il comando **route**.

```
route add default gw 192.168.3.1
```



Conclusioni

La rete vocale di base dovrebbe essere stata configurata correttamente. Per verificare questa condizione, selezionare uno dei telefoni SPA/MPP e si dovrebbe udire un segnale di linea. In questo documento, uno dei telefoni SPA/MPP ha l'estensione 1002 e l'altro ha 1003. Dovrebbe essere possibile chiamare l'interno 1003 quando si utilizza l'interno 1002 SPA/MPP phone.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).