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 <u>http://raspbx.local</u> 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

- 1. Configurazione delle VLAN sul router
- 2. Configurazione dei telefoni SPA/MPP
- 3. Configurazione delle VLAN su uno switch
- 4. Configurazione di VLAN voce su uno switch
- 5. Configurazione delle impostazioni dell'interfaccia su uno switch
- 6. Configurazione dell'appartenenza della porta VLAN su uno switch
- 7. Modifica dell'indirizzo IP di Raspberry Pi in modo che si trovi su una subnet diversa
- 8. Conclusioni

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 <u>qui</u>.

Small Business								cisco English	 Log Out 		
CISCO RV325 Gi	gabit Dual W	AN VPN Route	r								
Getting Started	VI AN Membe	ershin									
System Summary	VEAN Membe										
▶ Setup	VLAN: DEnable	VI AN: Enable									
► DHCP	Create VI ANs and	Create Vise and assign the Outgoing Frame Type									
System Management	Up to fourteen new	w VI ANE can be created a	(LAN IDe muet he in th	e range (4 - 4094)							
Port Management	op to lourteen ner	w vering can be created. v	EAN IDS INdst be In an	e range (44054)							
Port Setup	VLAN Table										
Port Status	ULAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6	
Traffic Statistics	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged	
DSCP Marking	0 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged	
802.1X Configuration	Add Edit	Delete									
Firewall		Delete									
▶ VPN											
 Certificate Management 	Save	Cancel									
▶ Log											
SSL VPN											
User Management											
Wizard											
	•									•	
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

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

CISCO RV325 Gi	gabit Dual W	/AN VPN Route	r					isco English	▼ Log Out	
Getting Started System Summary	VLAN Membership									
Setup DHCP System Management Port Management	VLAN: Create VLANs an Up to fourteen ne	VLAN: Create VLANs and assign the Outgoing Frame Type. Up to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)								
Port Setup	VLAN Table									
Port Status	VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
Traffic Statistics	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
DSCP Marking	100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
802.1X Configuration	Add Edit	Delete								
Firewall										_
 VPN Cortificate Management 										
Certificate Management	Save	Cancel								
▶ SSL VPN										
User Management										
Wizard										
	4									•

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

cisco RV325 Gig	gabit Dual V	/AN VPN Router					cisco	English V	Log Out Abo	ut Help	
Getting Started System Summary	VLAN Memb	/LAN Membership									
Setup DHCP System Management Port Management	VLAN: Create VLANs ar Up to fourteen ne	VLAN: Contract State Contract State									
Port Setup	VLAN Table					1					
Port Status Traffic Statistics	VLAN ID	Description Default	Inter VLAN Routing Disabled	Device Management Enabled	LAN1 Untagged	LAN2 Untagged	LAN3 Untagged	LAN4 Untagged	LAN5 Untagged	LA Un	
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Тар	
DSCP Marking	0 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Та	
► Firewall			Disabled v	Enabled v	Tagged V	Tagged 🔻	Tagged V	Tagged •	Tagged	▼ Ta	
▶ VPN	Add Edit	Delete									
 Certificate Management 											
 Log SSL VPN 	Save	Cancel									
User Management											
Wizard											
	4									•	
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

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.

cisco RV325 Gi	gabit Dual V	/AN VPN Router					cisco	English v			
Getting Started System Summary	VLAN Memb	AN Membership									
DHCP System Management Port Management	VLAN: Create VLANs ar Up to fourteen no	LAN:									
Port Setup	VLAN Table										
Port Status	VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5		LA
VLAN Membership	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagge	d	Un
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Та
DSCP Marking	0 100	Voice 2	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Тас
Eirewall	0 200	Data	Disabled *	Enabled V	Tagged V	Tagged V	Tagged 🔻	Tagged 🔻	Tagged	•	Та
▶ VPN	Add Edit	Delete									
Certificate Management											
▶ Log											
SSL VPN	Save	Cancel									
User Management											
Wizard											
	4										•
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

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.

cisco RV325 Gi	gabit Dual V	VAN VPN Router					cisco	English T	Log Out Abou	t Help	
Getting Started System Summary	VLAN Memb	LAN Membership									
 Setup DHCP System Management Port Management 	VLAN: Create VLANs a Up to fourteen n	LAN: C Enable 2reate VLANs and assign the Outgoing Frame Type. Jp to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)									
Port Setup Port Status	VLAN Table VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LA	
VLAN Membership QoS:CoS/DSCP Setting	1 25	Default Guest	Enabled Disabled	Enabled Disabled	Untagged T agged	Untagged • Tagged	Untagged v Tagged	Untagged v Tagged	Untagged Tagged	▼ U Taç	
DSCP Marking 802.1X Configuration	100	Voice Data	Enabled V	Disabled T Enabled	Tagged V	Tagged ▼ Tagged ▼	Tagged Tagged Tagged	Tagged •	Tagged	▼ Ta ▼ Ta	
Firewall VPN	Add Edit	Delete									
Certificate Management Log SSL VPN User Management	Save Cancel										
Wizard											
	4										
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

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.

cisco RV325 Gi	gabit Dual W	AN VPN Router					cisco	English 🔻	Log Out Abou	t Help
Getting Started System Summary	VLAN Membe	AN Membership								
Setup DHCP System Management Port Management	VLAN: Create VLANs and Create VLANs and Up to fourteen new	VLAN: C Enable Create VLANs and assign the Outgoing Frame Type. Up to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)								
Port Setup Port Status	VLAN Table	Description	Inter VI AN Routing	Device Management	LAN1	LAN2	LAN3	I AN4	LAN5	LA
Traffic Statistics VLAN Membership	1	Default	Enabled V	Enabled	Untagged V	Untagged V	Untagged V	Untagged V	Untagged	▼ U
QoS:CoS/DSCP Setting DSCP Marking	25	Guest Voice	Disabled Enabled	Disabled	Tagged Tagged •	Tagged Tagged •	Tagged Tagged v	Tagged Tagged •	Tagged Tagged	Tag Ta
802.1X Configuration Firewall	200	Data	Enabled •	Enabled V	Tagged V	Tagged V	Tagged V	Tagged V	Tagged	• •
► VPN	Add Edit	Delete								
Log SSL VPN User Management	Save Cancel									
Wizard										
	4									•
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.									

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).



cisco SPA5020	S Pro Configuration	Utility					Admin Login basic advanced
Voice	Call History	Personal Directory	Attendant	Console Status			
Info	ystem Phone	User					
							A
System Information							
	Connection Type:	DHCP			Current IP:	192.168.1.138	
	Host Name:	SipuraSPA			Domain:	routerf72530.com	
	Current Netmask:	255.255.255.0			Current Gateway:	192.168.1.1	
	Primary DNS:	192.168.1.1					
	Secondary DNS:						
Product Information							
	Product Name:	SPA502G			Serial Number:	CBT133400JK	
	Software Version:	7.1.3			Hardware Version:	1.0.0(0001)	
	MAC Address:	0018B9FFD97A			Client Certificate:	Installed	
	Customization:	Open			Licenses:	None	
Phone Status							and the second
	Current Time:	12/18/2017 06:52:56			Elapsed Time:	00:00:07	
	Broadcast Pkts Sent:	9			Broadcast Bytes Sent:	2014	
	Broadcast Pkts Recv:	6			Broadcast Bytes Recv:	360	•
		Und	io All Changes	Submit All Changes			
© 2009 Cisco Systems, Inc. Al	I Rights Reserved.						SPA502G IP Phone

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

cisco SPA502G Co	IIII Small Business Pro SISCO SPA502G Configuration Utility								
Voice	Call History	Personal Dire	ctory Attenda	int Console Status					
Info System	SIP	Provisioning	Regional	Phone U:	ser Attendant Console				
Ext 1									
General							^		
	Line Enable:	yes 🔻							
Share Line Appearance									
	Share Ext:	private 🔻			Shared U	Jser ID:			
	Subscription Expires:	3600							
NAT Settings									
,	NAT Mapping Enable:	no 🔻			NAT Keep Alive B	Enable: no 🔻			
	NAT Keep Alive Msg:	\$NOTIFY			NAT Keep Aliv	re Dest: \$PROXY			
Network Settings									
SIF	P TOS/DiffServ Value:	0x68			SIP CoS	S Value: 3 🔻			
RTF	P TOS/DiffServ Value:	0xb8			RTP CoS	S Value: 6 🔻			
	Network Jitter Level:	high 🔻			Jitter Buffer Adju	stment: up and down	•		
SIP Settings							-		
			Undo All Changes	Submit All Chang	es				
© 2009 Cisco Systems, Inc. All Rights	Reserved.			i La ¹¹			SPA502G IP Phone		

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: <u>Modifica</u> <u>dell'indirizzo del Raspberry Pi per essere su una subnet diversa</u>.

small Busi cisco SPA50	ness Pro 2G Configuration U	Jtility					<u>User Login</u> <u>basic</u> adv	ranced
Voice	Call History	Personal Direct	tory Attenda	nt Console Status				
Info	System SIP	Provisioning	Regional	Phone User	Attendant Console			
Ext 1								
	CFWD Notifier:							-
Proxy and Registration								
i rexy and regionation	Proxy:	(192.168.3.10)		Use Outbound Proxy	no 🔻		
	Outbound Proxy:				Use OB Proxy In Dialog	yes 🔻		
	Register:	yes 🔻			Make Call Without Reg	no 🔻		
	Register Expires:	3600			Ans Call Without Reg	no 🔻		
	Use DNS SRV:	no 🔻			DNS SRV Auto Prefix	no 🔻		
	Proxy Fallback Intvl:	3600			Proxy Redundancy Method	Normal	•	
Subscriber Information	1							
	Display Name:				User ID			
	Password:				Use Auth ID	no 🔻		
	Auth ID:							
	Mini Certificate:							
	SRTP Private Key:							
			Undo All Changes	Submit All Changes				
© 2009 Cisco Systems, In	c. All Rights Reserved.			in an			SPA502G IP	Phone

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.

Voice	Call History	Personal D	irectory A	Attendant Console Statu					
Info	System SIP	Provisioning	Regional	Phone	User	Attendant Console			
Ext 1									
	rtegister Expires.	3000				Alls Gall Williout Reg.	10 •		_
	Use DNS SRV:	no 🔻				DNS SRV Auto Prefix:	no 🔻		
	Proxy Fallback Intvi:	3600				Proxy Redundancy Method:	Normal	•	
scriber Informatio	n	(m)	_						
	Display Name:	1003				User ID:	1003		
	Password:					Use Auth ID:	no 🔻		
	Auth ID:								
	Mini Certificate:								
	SRTP Private Key:								
lio Configuration									
	Preferred Codec:	G711u 🔻				Use Pref Codec Only:	no 🔻		
	Second Preferred Codec:	Unspecified V				Third Preferred Codec:	Unspecified V		
	G729a Enable:	yes 🔻				G722 Enable:	yes 🔻		
	G726-16 Enable:	yes V				G726-24 Enable:	yes 🔻		
	G726-32 Enable:	yes 🔻				G726-40 Enable:	yes 🔻		
				Submit All	Changes				

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.

uluulu Small Business Pro cisco SPA502G Configuration	Utility	<u>User Login</u> <u>basic</u> advanced						
Voice Call History	Personal Directory Attendant Console Status							
Info System SIP	Provisioning Regional Phone User Attendant Console							
Ext 1								
Register Expires	3000 Alls Gall Williout Reg.	• •						
Use DNS SRV	no 🔻 DNS SRV Auto Prefix: ni	0 🔻						
Proxy Fallback Intvl	3600 Proxy Redundancy Method: N	iormal 🔻						
Subscriber Information								
Display Name	1003 User ID: 10	03						
Password	(12345 Use Auth ID: n	0 •						
Auth ID								
Mini Certificate								
SRTP Private Key								
Audio Configuration								
Preferred Codec	G711u VUse Pref Codec Only: n	0 🔻						
Second Preferred Codec	Unspecified Third Preferred Codec: U	Inspecified T						
G729a Enable	yes 🔻 G722 Enable: ye	es 🔻						
G726-16 Enable	yes T G726-24 Enable: ye	es 🔻						
G726-32 Enable	yes 🔻 G726-40 Enable: ye	es 🔻 👻						
	Undo All Changes Submit All Changes							
© 2009 Cisco Systems, Inc. All Rights Reserved.	2009 Cisco Systems, Inc. All Rights Reserved. SPA502G IP Phone							

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).

cisco SPA5	siness Pro 02G Configuration l	tility	<u>User Login</u> <u>basic</u> advanced
Voice	Call History	Personal Directory Attendant Console Status	
Info	System SIP	Provisioning Regional Phone User Attendant Console	
Ext 1			
	register Expires.	2000 MIS Gall Without Key. 10	A
	Use DNS SRV:	no 🔻 DNS SRV Auto Prefix: no 🔻	
	Proxy Fallback Intvl:	3600 Proxy Redundancy Method: Normal	Y
Subscriber Information	on		
	Display Name:	1003 User ID: 1003	
	Password:	12345 Use Auth ID: Ves 🔨	
	Auth ID:		
	Mini Certificate:		
	SRTP Private Key:		
Audio Configuration			
	Preferred Codec:	G711u 🔻 Use Pref Codec Only: no 🔻	
	Second Preferred Codec:	Unspecified Third Preferred Codec: Unspecified	fied 🔻
	G729a Enable:	yes 🔻 G722 Enable: yes 🔻	
	G726-16 Enable:	yes T G726-24 Enable: yes T	
	G726-32 Enable:	yes 🔻 G726-40 Enable: yes 🔻	-
		Undo All Changes Submit All Changes	
© 2009 Cisco Systems, I	nc. All Rights Reserved.		SPA502G IP Phone

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.

cisco SPA50	siness Pro D2G Configuration l	tility	<u>User Login</u> basic advanced
Voice	Call History	Personal Directory Attendant Console Status	
Info	System SIP	Provisioning Regional Phone User Attendant Console	
Ext 1			
	r regiorer.	yes	
	Register Expires:	3600 Ans Call Without Reg: no 🔻	
	Use DNS SRV:	no 🔻 DNS SRV Auto Prefix: no 🔻	
	Proxy Fallback Intvi:	3600 Proxy Redundancy Method: Normal	T
Subscriber Informatio	'n		
	Display Name:	1003 User ID: 1003	
	Password:	12345 Use Auth ID: yes 🔻	
	Auth ID:	1003	
	Mini Certificate:		
	SRTP Private Key:		
Audio Configuration			
	Preferred Codec:	G711u 🔻 Use Pref Codec Only: no 🔻	
	Second Preferred Codec:	Unspecified Third Preferred Codec: Unspecified	•
	G729a Enable:	yes T G722 Enable: yes T	
	G726-16 Enable:	yes ▼ G726-24 Enable: yes ▼	-
		Undo All Changes Submit All Changes	
© 2009 Cisco Systems, Ir	nc. All Rights Reserved.		SPA502G IP Phone

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.

🗋 Add VLAN - Google Chrome	_		×
A Not secure https://192.168.1.100/html/vlan_createAdd.html			
VLAN ID: 100 (Range: 2 - 4094)			
VLAN Name: Voice (5/32 Characters Used)			
Range			
VLAN Range: -	(Range: 2 -	4094)	
Apply Close			

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.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch € Logout About 1	lelp
Getting Started Status and Statistics Administration Det Magazement	Properties CoS/802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.	
VI AN Management	Voice VLAN Settings:	
Default VLAN Settings Create VLAN	Administrative Status: Operational Status:	
Interface Settings Port to VLAN	Voice VLAN ID: 1 (Range: 1 - 4094, Default: 1) Voice VLAN ID: 1	
Port VLAN Membership	CoS/802.1p: 5 ▼ (Default: 5) CoS/802.1p: 5	
GVRP Settings Voice VLAN Properties	DSCP: 46 (Default: 46) DSCP: 46	
Telephony OUI Telephony OUI Interface	Dynamic Voice VLAN Settings:	
Spanning Tree	Dynamic Voice VLAN: Enable Auto Voice VLAN Enable Auto Voice VLAN	
 MAC Address Tables 	Disable	
Multicast		
 P Conliguration Security 	Apply Cancel	
Access Control		
Quality of Service		
▶ SNMP		
© 2014-2017 Cisco Systems, Inc. A	I Rights Reserved.	

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.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started Status and Statistics Administration Port Management	Properties Cos/802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.
VLAN Management Default VLAN Settings Create VLAN Interface Settings Default VLN	Voice VLAN Settings: Operational Status: Administrative Status: 0 Voice VLAN ID: 100 (Range: 1 - 4094, Default: 1) Voice VLAN ID:
Port to VLAN Port VLAN Membership GVRP Settings Voice VLAN Properties	CoSi802.1p: 5 • (Default 5) CoSi802.1p: 5 DSCP: 46 • (Default 46) DSCP: 46
Telephony OUI Telephony OUI Interface Spanning Tree MAC Address Tables	Dynamic Volce VLAN Settings: Dynamic Volce VLAN: Enable Auto Volce VLAN Enable Telephony OUI Deable
Multicast IP Configuration Security	Apply Cancel
Access Control Quality of Service SNMP	
© 2014-2017 Cisco Systems, Inc. A	I Rights Reserved.

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

Small Business SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started Status and Statistics Administration	Properties CoS/802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.
 Port Management VI AN Management 	Voice VLAN Settings:
Default VLAN Settings Create VLAN	Administrative Status: Operational Status:
Port to VLAN	Ø Voice VLAN ID: 100 (Range: 1 - 4094, Default: 1) Voice VLAN ID: 1
Port VLAN Membership	CoS/802.1p: 5 (Default 5) CoS/802.1p: 5
GVRP Settings Voice VLAN	DSCP: 46 (Default: 46) DSCP: 46
Properties Telephony OUI Telephony OUI Interface	Dynamic Voice VLAN Settings:
Spanning Tree	Dynamic Voice VLAN: Enable Auto Voice VLAN
 MAC Address Tables 	Disable
 Multicast ID Configuration 	
 Recurity 	Apply Cancel
 Access Control 	
 Quality of Service 	
▶ SNMP	
© 2014-2017 Cisco Systems, Inc. Al	I Rights Reserved.

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.

Small Business SF220-24P	24-Pc	ort 10/	100 P	oE Smart Swi	tch				cisco Languag	e: English	۲			
Getting Started Status and Statistics	Interfa	ace Se	ttings											^
 Administration 	Interfa	ice Setting	gs Table					Showing 1	26 of 26	All 🔻 p	er page			
 Port Management 	Filter	Interface	Type equals	sto Port V Go								1		
 VLAN Management 				Interface MI Abl Maria	Administrative DV//D	France Truck	In succes Filtering	Unlink						
Default VLAN Settings		nury NO.	Internace	Truel	Administrative PVID	Prame Type	Eachlad	Disabled						-
Create VLAN		2	FE 1	Trunk	1	Admit All	Enabled	Disabled						
Port to VLAN		2	FE2	Trunk	1	Admit All	Enabled	Disabled						
Port VLAN Membership		3	FE3	Trunk	1	Admit All	Enabled	Disabled						
GVRP Settings		4	FE4	Trunk	1	Admit All	Enabled	Disabled						
 Voice VLAN 		5	FED	Trunk	1	Admit Ali	Enabled	Disabled						
Properties Telephony OUI		6	FE6	Trunk	1	Admit All	Enabled	Disabled						
Telephony OUI Interface		(FE/	Irunk	1	Admit All	Enabled	Disabled						
 Spanning Tree 		8	FE8	Trunk	1	Admit All	Enabled	Disabled						
MAC Address Tables		9	FE9	Trunk	1	Admit All	Enabled	Disabled						
Multicast	$\overline{\mathbf{O}}$	10	FE10	Trunk	1	Admit All	Enabled	Disabled						
IP Configuration		11	FE11	Trunk	1	Admit All	Enabled	Disabled						
Security		12	FE12	Trunk	1	Admit All	Enabled	Disabled						
Access Control		13	FE13	Trunk	1	Admit All	Enabled	Disabled						
Quality of Service		14	FE14	Trunk	1	Admit All	Enabled	Disabled						
▶ SNMP		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						-
© 2014-2017 Cisco Systems, Inc. A	II Rights Re	eserved.												

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

Small Business SF220-24P	24-1	Port 10	/100 P	oE Smart Swi	tch					English		Logo		Help
Getting Started Status and Statistics	Inte	erface Se	ettings											^
 Administration 	Inte	erface Settin	ngs Table					Sho	owing 1-26 of 2	All 🔻	per page			
 Port Management 	Filt	er: Interface	Type equa	s to Port 🔻 Go)									
 VLAN Management 		Entry No	Interface	Interface VI AN Mode	Administrative P\/ID	Erame Tune	Ingrase Eiltering	Linlink						-
Default VLAN Settings		1	FE1	Trunk	Administrative 1 VID	Admit All	Enabled	Disabled						6
Create VLAN		2	FEI	Trunk	1	Admit All	Enabled	Disabled						
Port to VLAN		2	FE3	Trunk	1	Admit All	Enabled	Disabled						
Port VLAN Membership		4	FE4	Trunk	1	Admit All	Enabled	Disabled						1 1
GVRP Settings		- 5	FE5	Trunk	1	Admit All	Enabled	Disabled						
Voice VLAN		6	FEG	Trunk	1	Admit All	Enabled	Disabled						
Spanning Tree		7	FE7	Trunk	1	Admit All	Enabled	Disabled						
MAC Address Tables		,	FE8	Trunk	1	Admit All	Enabled	Disabled						
 ID Configuration 		0	FEO	Trunk	1	Admit All	Enabled	Disabled						
 F Configuration Security 		10	FE10	Trunk	1	Admit All	Enabled	Disabled						
Access Control		11	FE11	Trunk	1	Admit All	Enabled	Disabled						
Quality of Service		12	FE12	Trunk	1	Admit All	Enabled	Disabled						
▶ SNMP		12	EE 12	Trunk	1	Admit All	Enabled	Disabled						
		14	FE14	Trunk	1	Admit All	Enabled	Disabled						
		14	EE15	Trunk	1	Admit All	Enabled	Disabled						
		10	EE 16	Trunk	1	Admit All	Enabled	Disabled						
	H	10	FE 10	Truck	1	Admit All	Enabled	Disabled						-
© 2014-2017 Cisco Systems, Inc. A	II Rights	Reserved.	FE1/	TUIN		Agrine All	Enabled	Disabled						

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

Small Business cisco SF220-24P	24-Poi	rt 10/	100 P	oE Smart Switch						English	•	_ogout		Help
Getting Started													-	
Status and Statistics		7	FE7	Trunk	1	Admit All	Enabled	Disabled						
Administration		8	FE8	Trunk	1	Admit All	Enabled	Disabled						
Port Management	\odot	9	FE9	Trunk	1	Admit All	Enabled	Disabled						
 VI AN Management 		10	FE10	Trunk	1	Admit All	Enabled	Disabled						
Default VII AN Cettings		11	FE11	Trunk	1	Admit All	Enabled	Disabled						
Create VLAN		12	FE12	Trunk	1	Admit All	Enabled	Disabled						
Interface Settings		13	FE13	Trunk	1	Admit All	Enabled	Disabled						
Port to VLAN	0	14	FE14	Trunk	1	Admit All	Enabled	Disabled						
Port VLAN Membership		15	FE15	Trunk	1	Admit All	Enabled	Disabled						
GVRP Settings		16	FE16	Trunk	1	Admit All	Enabled	Disabled						
Voice VLAN		17	FE17	Trunk	1	Admit All	Enabled	Disabled						
Spanning Tree		18	FE18	Trunk	1	Admit All	Enabled	Disabled						
MAC Address Tables		19	FE19	Trunk	1	Admit All	Enabled	Disabled						
Multicast		20	EE20	Trunk	1	Admit All	Enabled	Disabled						
 IP Configuration 		20	FE20	Truek	1	Admit All	Enabled	Disabled						
 Security 		21	FE21	Trunk	1	Admit All	Enabled	Disabled						
 Access Control 		22	FE22	Irunk	1	Admit All	Enabled	Disabled						
 Quality of Service 		23	FE23	Trunk	1	Admit All	Enabled	Disabled						
▶ SNMP		24	FE24	Trunk	1	Admit All	Enabled	Disabled						
		25	GE1	Trunk	1	Admit All	Enabled	Disabled						
		26	GE2	Trunk	1	Admit All	Enabled	Disabled						
		opy Setti	ngs	Edit										
© 2014-2017 Cisco Systems, Inc. A	I Rights Res	served.												•

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

🗋 Edit Interface Settings -	Google Chrome	—		×
▲ Not secure https://	/192.168.1.100/html/vlan_intfEdit.html?port=FE3			
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 on	e or more	e Dot1q-T	unnel po
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 V			
Apply Close				ł

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

🖹 Edit Interface Settings -	Google Chrome —		×
▲ Not secure https://	192.168.1.100/html/vlan_intfEdit.html?port=FE3		
Interface:	Port FE3 LAG I		
Interface VLAN Mode:	 General Access Trunk Dot1q-Tunnel (The switch will be in Q-in-Q mode when it has one or more 	Dot1q-T	unnel po
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 V		
Apply Close			

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.

Small Business cisco SF220-24P	24-	Port 10)/100	PoE Smart Sv	vitch				Save cisco		English		Logo		Help
Getting Started Status and Statistics Administration	Po F-F	rt VLAN ⁼orbidden me	Membe	ership T - Tagged member	U - Untagged mer	nber	P - PVID	G - Guest V	LAN						*
 Port Management 	Po	Port VLAN Membership Table Showing 1-26 of 26 All Y per page													
 VLAN Management 	Fil	ter: Interfac	e Type equ	als to Port V Go									_		
Default VLAN Settings Create VLAN		Interface	Mode	Administrative VLANs	Operational VLANs	LAG									
Interface Settings		FE1	Trunk	1UP	1UP, 100T										
Port to VLAN		FE2	Trunk	1UP	1UP, 100T										
OVEP Settings		FE3	Access	1UP	1UP										
 Voice VLAN 		FE4	Trunk	1UP	1UP										
Spanning Tree		FE5	Trunk	1UP	1UP										
MAC Address Tables		FE6	Trunk	1UP	1UP										
 Multicast 		FE7	Trunk	1UP	1UP										
 IP Configuration 		FE8	Trunk	1UP	1UP										
 Security 		FE9	Trunk	1UP	1UP										
 Access Control 		FE10	Trunk	1UP	1UP										
Quality of Service		FE11	Trunk	1UP	1UP										
► SNMP		FE12	Trunk	1UP	1UP										
		FE13	Trunk	1UP	1UP										
		FE14	Trunk	1UP	1UP										
		FE15	Trunk	1UP	1UP										
© 2014-2017 Cisco Systems, Inc. A	II Right	FE16 s Reserved.	Trunk	1UP	1UP										

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 <u>Configurazione della VLAN voce sullo switch</u>.

Small Business SF220-24P	24-	Port 1(0/100	PoE Smart Sv	vitch				Language	English	Ŧ	Logou		Help
Getting Started Status and Statistics Administration	Po F-F	rt VLAN	Membe	ership T - Tagged member	U - Untagged mer	mber	P - PVID	G - Guest VLAN						*
 Port Management 	Po	rt VLAN Me	mbership	Table			Showing	1-26 of 26	All 🔻	per page				
 VLAN Management 	Fil	er Interfac	e Type equ	uals to Port V Go										1
Default VLAN Settings	-	Interface	Mode	Administrative VI ANs	Operational V/LANe	LAG								
Interface Settings		FE1	Trupk	Authinistrative VEANS	1UP 100T	LAG								
Port to VLAN		FE2	Trunk	101	1UP 100T									
Port VLAN Membership	G	EE3	Access	100	1UP									
GVRP Settings		FE4	Trunk	1UP	1UP									1
Spanning Tree		FE5	Trunk	1UP	1UP									
MAC Address Tables		FE6	Trunk	1UP	1UP									
Multicast		FE7	Trunk	1UP	1UP									
 IP Configuration 		FE8	Trunk	1UP	1UP									
 Security 		FE9	Trunk	1UP	1UP									
 Access Control 		FE10	Trunk	1UP	1UP									
 Quality of Service 		FE11	Trunk	1UP	1UP									
▶ SNMP		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. Al	I Right	s Reserved.												

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

Small Business CISCO SF220-24P	24-	Port 1	0/100 P	oE Smart Sw	itch			cisco Language: English	¥ La	igout Abo	out He	
Getting Started		EEP	Trupk	1110	1118							•
 Status and Statistics 		EEQ	Trunk	111P	111P							
 Administration 		EE10	Trunk	100	100							
 Port Management 		FEIU	Taunk	105	1UP							
 VLAN Management 		FEII	Trunk	TUP	TUP							
Default VLAN Settings		FE12	Trunk	10P	TUP							
Create VLAN		FE13	Trunk	10P	10P							
Interface Settings		FE14	Trunk	1UP	1UP							
Port to VLAN		FE15	Trunk	1UP	1UP							
GVRP Settings		FE16	Trunk	1UP	1UP							
 Voice VLAN 		FE17	Trunk	1UP	1UP							
Spanning Tree		FE18	Trunk	1UP	1UP							
MAC Address Tables		FE19	Trunk	1UP	1UP							
Multicast		FE20	Trunk	1UP	1UP							
IP Configuration		FE21	Trunk	1UP	1UP							
Security		FE22	Trunk	1UP	1UP							
Access Control		FE23	Trunk	1UP	1UP							
Quality of Service		FE24	Trunk	1UP	1UP							
▶ SNMP		GE1	Trunk	1UP	1UP							
		GE2	Trunk	1UP	1UP							
	J	oin VLAN	Details.									
	F - F	Forbidden m	nember	T - Tagged member	U - Untagged member	P - PVID	G - Guest VLAN					•
© 2014-2017 Cisco Systems, Inc. Al	© 2014-2017 Cisco Systems, Inc. All Rights Reserved.											

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.

D Join VLAN - Google Chrome		×
A Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3		
Interface: Port FE3 LAG I		
Mode: Access		
Select VLAN:		
100 200 1 <		
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN		
Tagging: Forbidden Excluded Tagged Intagged		
VID VID		
Apply Close		

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

🖒 Join VLAN - Google Chrome	_	×
A Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3		
Interface: Port FE3 LAG I		
Mode: Access		
Select VLAN:		
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN		
Tagging: Forbidden Excluded Tagged ● Untagged Untagged ✓ PVID PVID		
Apply Close		

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

Doin VLAN - Google Chrome			\times
▲ 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 icon.	or click t	the Save	
Interface: OPort GE1 LAG 1			
Mode: Trunk			
Select VLAN:			
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN			
Tagging: Forbidden Excluded Tagged Untagged PVID			
Apply Close			

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**.

Din VLAN - Google Chrome - X						
▲ 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:						
Mode: Trunk						
Select VLAN:						
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN						
Tagging: Forbidden Excluded Tagged Untagged PVID						
Apply Close						

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 <u>Configurazione delle impostazioni</u> <u>dell'interfaccia su uno switch e Configurazione dell'appartenenza della porta VLAN sullo switch in</u> 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 <u>qui</u>.

PuTTY Configuration		\times			
Category:					
Session	Basic options for your PuTTY session				
	Specify the destination you want to connect	et to			
Keyboard	Host Name (or IP address)	Port			
Bell		22			
- Window - Appearance	Connection type:	H 🔿 Serial			
-Behaviour -Translation -Selection -Colours	Load, save or delete a stored session Saved Sessions				
Data	Default Settings	Load			
- Proxy - Telnet		Save			
-Rlogin		Delete			
Jenar					
	Close window on exit: Always Never Only on c	lean exit			
About	Open	Cancel			

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.

PuTTY Configuration		×
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection 	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port 192.168.1.10 22 Connection type: Raw Telnet Rlogin SSH C Load, save or delete a stored session Saved Sessions) Serial
Colours Connection Data Proxy Telnet Rlogin SSH Serial	Default Settings	_oad Save Delete
	Close window on exit: Always Never Only on clean e	exit
About	Open C	ancel

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

PuTTY Configuration		×
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation 	Basic options for your PuTTY sess Specify the destination you want to connect to Host Name (or IP address) 192.168.1.10 Connection type: O Raw O Telnet O Rlogin O SSH Load, save or delete a stored session Saved Sessions	ion o Port 22 O Serial
- Selection - Colours - Data - Proxy - Telnet - Rlogin - SSH - Serial	Default Settings	Load Save Delete
	Close window on exit: Always Never Only on clear	an exit
About	Open	Cancel

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.

PuTTY Configuration		×
Category:		
-Session Logging	Basic options for your PuTTY se	ession
 Terminal Keyboard Bell Features Window 	Host Name (or IP address) 192.168.1.10 Connection type: Raw Telnet Riogin SSH	Port 22
 Appearance Behaviour Translation Selection Colours 	Load, save or delete a stored session Saved Sessions	
⊂Connection -Data -Proxy -Telnet	Default Settings	Load Save
- Rlogin		Delete
	Close window on exit: Always Never Only on c	lean exit
About	Open	Cancel

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.

PuTTY Configuration		×
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance 	Basic options for your PuTTY ses Specify the destination you want to connect Host Name (or IP address) 192.168.3.10 Connection type: O Raw O Telnet O Rlogin • SSH	sion to Port 22 O Serial
 Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	Load, save or delete a stored session Saved Sessions Default Settings	Load Save Delete
About	Close window on exit: Always Never Only on cle	ean exit

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).