## **Comment créer un réseau vocal de base avec Raspberry Pi**

## Objectif

Ce document fournit des instructions sur la façon de configurer un réseau vocal de base avec Raspberry Pi comme serveur de communication en utilisant Asterisks. Le réseau local virtuel (VLAN) et la qualité de service (QoS) seront utilisés pour aider à hiérarchiser le trafic en séparant le trafic voix et le trafic données. L'objectif de ce réseau est de mettre en place des tests internes. Ces tests vous aideront à faire évoluer votre réseau de manière appropriée, à déterminer si vous disposez d'une bande passante suffisante pour le volume vocal attendu et à détecter tout autre conflit possible entre les équipements. Il peut également vous aider à déterminer si vous souhaitez l'héberger localement ou dans le cloud. Une fois qu'une entreprise a atteint une certaine taille, elle peut préférer disposer de son propre contrôleur d'appels local, tel qu'un PBX ou un PBX IP. Cela rendrait les appels internes plus efficaces puisque les appels entre les téléphones à l'intérieur de l'entreprise n'auraient pas besoin d'être acheminés hors de l'immeuble, puis de nouveau vers l'intérieur.

**Remarque importante :** le Raspberry Pi n'est pas un produit pris en charge par Cisco, ce document est uniquement destiné à l'assistance et n'est pas un document de solution.

#### Introduction

Pour qu'une entreprise puisse mener ses activités efficacement, ses employés doivent avoir accès à un réseau vocal. Cela facilite la communication entre les employés et leurs clients et permet aux employés de communiquer en interne. Chaque employé peut disposer d'une ligne téléphonique fixe et/ou d'un téléphone portable, mais cela peut s'avérer très coûteux. Les entreprises choisissent souvent de configurer un réseau vocal qui utilise plutôt la voix sur IP (VoIP).

La technologie VoIP vous permet d'utiliser Internet pour passer et recevoir des appels téléphoniques depuis n'importe quel endroit, vers n'importe quel endroit dans le monde, avec des frais d'interurbain minimes, voire inexistants. Cela peut être utilisé sur n'importe quel périphérique qui utilise Internet.

La VoIP permet à une entreprise de réaliser des économies tout en augmentant la productivité, la communication et la satisfaction client. Les employés peuvent utiliser différentes fonctionnalités telles que le routage des appels, la musique d'attente et la messagerie vocale intégrée.

Le routage d'appels, également appelé distributeur automatique d'appels, est une fonctionnalité courante de la VoIP utilisée par de nombreuses entreprises. Le routage des appels distribue les appels entrants à l'agent disponible suivant au lieu de les envoyer à la messagerie vocale. Cela garantit que les appels des clients seront traités aussi efficacement que possible. En dehors des heures de bureau, les appels peuvent être envoyés directement vers la messagerie vocale.

L'ajout d'utilisateurs et la mise à niveau de fonctionnalités sont des processus simples, utiles lorsque votre entreprise se développe ou que vos besoins évoluent. Contrairement à un système téléphonique traditionnel, aucun câblage coûteux n'est nécessaire.

Pour configurer un réseau VoIP, vous devez prendre en compte plusieurs options. Vous pouvez héberger un service VoIP pour votre propre système téléphonique à l'aide de KSU, sans KSU, d'un autocommutateur privé (PBX) ou d'un autre système VoIP.

Votre budget, le nombre d'employés et de sites, les services disponibles dans votre région et la

croissance de l'entreprise doivent tous être pris en compte. Des formations et des équipements supplémentaires, tels que des casques, peuvent également être nécessaires. La VoIP peut augmenter l'utilisation de vos données et vous devrez peut-être augmenter votre bande passante pour prendre en compte le trafic du réseau vocal.

Vous devez également planifier une sauvegarde, « Plan B », au cas où votre réseau tomberait en panne. Si vous perdez l'alimentation, votre système VoIP ne se connectera pas. Cette redondance doit être implémentée pour restaurer immédiatement vos services téléphoniques et empêcher toute interruption de la productivité de votre entreprise.

Dans cet article, nous allons déployer notre propre système téléphonique en utilisant Asterisk, un PBX sur un Raspberry Pi.

**Remarque** : une fois ces étapes terminées et que vous souhaitez également pouvoir appeler à partir de votre réseau interne, vous devez choisir un fournisseur de services de téléphonie Internet (ITSP).

#### Définitions

Un **réseau local virtuel (VLAN)** vous permet de segmenter logiquement un réseau local (LAN) en différents domaines de diffusion. Dans les scénarios où des données sensibles peuvent être diffusées sur un réseau, des VLAN peuvent être créés pour améliorer la sécurité en désignant une diffusion sur un VLAN spécifique. Les utilisateurs dâ€<sup>TM</sup>un VLAN spécifique sont les seuls à pouvoir accéder aux données de ce VLAN et les manipuler. Les VLAN peuvent également être utilisés pour améliorer les performances en réduisant le besoin dâ€<sup>TM</sup>envoyer des diffusions et des multidiffusions vers des destinations inutiles.

Par défaut, tous les ports sont affectés au VLAN 1. Par conséquent, une fois que vous avez configuré différents VLAN, vous devez affecter manuellement chaque port au VLAN approprié.

Chaque VLAN doit être configuré avec un ID de VLAN (VID) unique dont la valeur est comprise entre 1 et 4 094. Le périphérique réserve le VID 4095 comme VLAN de rejet. Tous les paquets classés dans le VLAN de rejet sont rejetés en entrée et ne sont pas transférés vers un port.

La qualité de service (QoS) vous permet de hiérarchiser le trafic pour différentes applications, différents utilisateurs ou différents flux de données. Il peut également être utilisé pour garantir des performances à un niveau spécifié, affectant ainsi la QoS pour le client. La qualité de service est généralement affectée par les facteurs suivants : gigue, latence et perte de paquets. Le plus souvent, la vidéo ou la VoIP sont prioritaires, car elles sont les plus affectées par la QoS.

Le PBX (Private Branch Exchange) est un système de commutation téléphonique qui gère les appels entrants et sortants pour les utilisateurs internes d'une entreprise. Un PBX est connecté au système téléphonique public et achemine automatiquement les appels entrants vers des postes spécifiques. Il partage et gère également plusieurs lignes. Un système PBX type pour petites entreprises comprend des lignes téléphoniques externes et internes, un serveur informatique qui gère la commutation et le routage des appels et une console pour le contrôle manuel.

Un **PBX IP** peut faire tout ce qu'un PBX traditionnel pour petites entreprises peut faire et bien plus encore. Il assure la commutation et la connexion des appels VoIP et des appels vers les lignes terrestres. Un système PBX IP fonctionne sur un réseau de données IP, ce qui permet de réduire les coûts et de réduire la gestion du réseau. Vous pouvez utiliser des téléphones IP, des téléphones logiciels (qui ne nécessitent aucun matériel téléphonique autre qu'un ordinateur et un casque de microphone) et des téléphones fixes sur un système téléphonique PBX IP.

Un Raspberry Pi est un petit ordinateur portable peu coûteux qui fonctionne comme un ordinateur de

bureau.

Asterisk est un framework open source qui peut transformer un ordinateur, tel qu'un Raspberry Pi, en serveur de communication. Cela vous permet de créer votre propre système téléphonique PBX professionnel. Dans cet article, Asterisk utilise FreePBX comme interface graphique utilisateur (GUI) qui contrôle et gère Asterisk où vous pouvez configurer les extensions, les utilisateurs, etc.

### Périphériques pertinents

- Routeur
- Commutateur PoE (Power over Ethernet)
- Raspberry Pi (modèles Pi 3 B+, Pi 3, Pi 3, B+, B et A)
- 2 téléphones IP Cisco SPA/MPP ou plus

## Version du logiciel

- 14.0.1.20 (PBX gratuit)
- 13.20.0 (Astérisque)
- 1.1.1.06 (routeur RV325)
- 1.1.4.1 (SF220-24P)
- 7.1.3 (SPA502G)

Pour configurer le réseau vocal de base avec Raspberry Pi, suivez les instructions ci-dessous :

**Topologie:** 



L'image du RasPBX est disponible ici. Cette image doit être installée sur le Raspberry Pi.

**Remarque :** dans ce document, le Raspberry Pi avec l'image RasPBX est déjà configuré. Pour accéder à l'interface graphique utilisateur du Raspberry Pi, tapez <u>http://raspbx.local</u> ou l'adresse IP du Raspberry Pi dans votre navigateur pour configurer le PBX. La connexion FreePBX par défaut est user: **admin** password: **admin**. En outre, le Raspberry Pi a été préconfiguré pour avoir une adresse IP

statique.

#### Table des matières

- 1. Configuration de réseaux locaux virtuels sur le routeur
- 2. Configuration des téléphones SPA/MPP
- 3. Configuration de VLAN sur un commutateur
- 4. Configuration de VLAN voix sur un commutateur
- 5. Configuration des paramètres d'interface sur un commutateur
- 6. Configuration de l'appartenance VLAN à un port sur un commutateur
- 7. Modification de l'adresse IP de Raspberry Pi sur un sous-réseau différent
- 8. Conclusion

#### Configuration de réseaux locaux virtuels sur le routeur

Étape 1. Connectez-vous à l'utilitaire Web et accédez à **Port Management > VLAN Membership**.

**Remarque :** cela peut varier en fonction du modèle. Dans cet exemple, RV325 est utilisé. Pour plus d'informations sur l'accès à la page de configuration Web, cliquez <u>ici</u>.

						ci	sco English '	Log Out			
CISCO RV325 Gi	gabit Dual WAN	VPN Router									
Getting Started	VI AN Membershi	n									
System Summary		P									
Setup	VLAN: DEnable	LAN: Enable									
► DHCP	Create VLANs and assid	cale VI Als and assign the Outgoing Frame Type									
<ul> <li>System Management</li> </ul>	Un to fourteen new VLA	Greate VLANS and assign the Outgoing Franker type.									
Port Management			be in the range (44004)						_		
Port Setup	VLAN Table										
Port Status	VLAN ID Des	cription Inter VLAN F	Routing Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6		
Traffic Statistics	🔲 1 Defa	ault Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged		
QoS:CoS/DSCP Setting	🔲 25 Gue	st Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged		
DSCP Marking	🔲 100 Voic	e Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged		
802.1X Configuration	Add Edit De	lete									
Firewall		1010									
► VPN											
<ul> <li>Certificate Management</li> </ul>	Save Cance	el									
▶ Log											
SSL VPN											
User Management											
Wizard											
									•		
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

Étape 2. Cochez la case Enable pour activer le VLAN sur le routeur.

cisco RV325 Gi	gabit Dual W	/AN VPN Route	:r					cisco English	Log Out	About Help		
Getting Started System Summary > Setup > DHCP > System Management - Port Management	VLAN Member VLAN: C Enab Create VLANs and Up to fourteen ne	LAN Membership         vLAN: ✓ Enable         Create VLANs and assign the Outgoing Frame Type.         Up to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)										
Port Setup Port Status	VLAN Table	Description	Inter 1/1 Abl Douting	Device Menorement	1.4514	1.4112	1 4 1 2	1.4514	LANE	LANC		
Traffic Statistics VLAN Membership	U VLAN ID	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged		
QoS:CoS/DSCP Setting DSCP Marking	25	Guest Voice	Disabled Disabled	Disabled Disabled	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged		
802.1X Configuration ► Firewall	Add Edit	Delete										
VPN     Certificate Management	Save	Cancel										
Log     SSL VPN												
User Management Wizard												
© 2013 Cisco Systems, Inc. All Rig	ts Reserved.									•		

Étape 3. Dans la section VLAN Table, cliquez sur Add pour créer un nouvel ID de VLAN.

CISCO RV325 G	igabit Du	al W	AN VPN Router							ci	sco	English <b>v</b>			Help
Getting Started System Summary	VLAN M	embe	ership												
Setup     DHCP     System Management     Port Management	VLAN: Create VL Up to four	Enabl ANs an een ne	le Id assign the Outgoing Frame T w VLANs can be created. VLA	ype. N IDs must be in the ra	ange (44094)										
Port Setup	VLAN T	ble													
Traffic Statistics		AN ID	Description	Disabled	Device Management Enabled	LAN1 Untagged		LAN2 Untagged		LAN3 Untagged		LAN4 Untagged	LAN5 Untag	red	Un
VLAN Membership QoS:CoS/DSCP Setting	25		Guest	Disabled	Disabled	Tagged		Tagged		Tagged		Tagged	Tagged	4 1	Та
DSCP Marking	100		Voice	Disabled	Disabled	Tagged		Tagged		Tagged		Tagged	Taggeo	d	Тас
<ul> <li>802.1X Configuration</li> <li>Firewall</li> </ul>				Disabled •	Enabled •	Tagged	۲	Tagged	۲	Tagged	۲	Tagged 🔻	Tagge	ed 🔻	Ta
▶ VPN	Add	Edit	Delete												
<ul> <li>Certificate Management</li> </ul>															
► Log	Save		Cancel												
User Management															
Wizard															
	4														Þ

Étape 4. Entrez un numéro de VLAN dans le champ *VLAN ID*. Les ID de VLAN doivent être compris entre 4 et 4 094. Dans cet exemple, 200 est utilisé pour les données comme ID de VLAN. Entrez ensuite une description pour le VLAN dans le champ *Description*. Les données sont entrées comme exemple de description. Cliquez ensuite sur **Enregistrer**.

**Remarque :** le VLAN 100 pour la voix a été créé par défaut sur ce routeur. Il est possible de créer jusquâ€<sup>™</sup>à quatorze nouveaux VLAN.

cisco RV325 Gi	gabit Dual V	/AN VPN Router					cisco	English 🔻				
Getting Started System Summary	VLAN Memb	N Membership										
Setup     DHCP     System Management     Port Management	VLAN: Create VLANs ar Up to fourteen ne	LAN: D Enable reate VLANs and assign the Outgoing Frame Type. p to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)										
Port Setup Port Status	VLAN Table	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5		LA	
Traffic Statistics VLAN Membership	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagg	ed	Un	
QoS:CoS/DSCP Setting DSCP Marking	25	Voice 2	Disabled	Disabled	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged		Тас Тас	
802.1X Configuration Firewall	0 200	Data	Disabled <b>T</b>	Enabled <b>T</b>	Tagged 🔻	Tagged <b>T</b>	Tagged <b>T</b>	Tagged	Tagger	d 🔻	Ta	
VPN     Certificate Management	Add Edit	Delete										
► Log ► SSL VPN	Save	Cancel										
User Management												
Wizard	4										•	
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.											

Étape 5. Pour modifier un VLAN, cochez la case du VLAN approprié. Dans cet exemple, VLAN 1, 100 et 200 seront modifiés. Cliquez ensuite sur **Edit** pour modifier les VLAN.

cisco RV325 Gi	gabit Dual V	/AN VPN Route	er					cisco English	Log Out	About Help	
Getting Started System Summary	VLAN Memb	AN Membership									
Setup     DHCP     System Management     Port Management	VLAN: Create VLANs ar Up to fourteen ne	LAN: C Enable reate VLANs and assign the Outgoing Frame Type. p to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)									
Port Setup Port Status	VLAN Table	Description		Derive Management		1 4110	1 4 1 10		1.415	1.410	
Traffic Statistics	VLAN ID	Description	Disabled	Enabled	LAN1 Untagged	Untagged	Untagged	Untagged	Untagged	Untagged	
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged	
802.1X Configuration	<ul> <li>100</li> <li>100</li> </ul>	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged	
Firewall     VPN	Add Edit	Delete	Disabled	Enabled	lagged	lagged	lagged	lagged	lagged	lagged	
Certificate Management     Log     SSL VEN	Save	Cancel									
User Management Wizard											
	4									Þ	
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

Étape 6. (Facultatif) Dans la liste déroulante *Inter VLAN Routing*, sélectionnez **Enabled** ou **Disabled** pour acheminer les paquets dâ€<sup>TM</sup>un VLAN à un autre VLAN. Cette activation est utile, car les administrateurs réseau internes peuvent accéder à distance à vos périphériques pour vous aider à résoudre vos problèmes. Cela réduit le temps nécessaire pour commuter constamment les VLAN afin d'accéder aux périphériques.

- Disabled : indique que le routage inter-VLAN est inactif.
- Enabled : indique que le routage inter-VLAN est actif sur ce VLAN. Le routage inter-VLAN achemine les paquets uniquement entre les VLAN pour lesquels il est activé.

**Remarque :** dans cet exemple, nous allons activer le routage inter-VLAN pour les ID de VLAN 1, 100 et 200.

cisco RV325 Gig	gabit Dual W	/AN VPN Router					cisco	English 🔻	Log Out	About	Help
Getting Started System Summary	VLAN Membe	ership									
Setup     DHCP     System Management     Port Management	VLAN: Create VLANs and Up to fourteen net	/LAN: Ø Enable Steate 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 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 Tagged	Untagged Tagged	Untagged V Tagged	Untagged • Tagged	Untagg Tagged	ed 🔻	U Taş
DSCP Marking 802.1X Configuration	100	Voice Data	Enabled V Enabled V	Disabled T Enabled T	Tagged Tagged	Tagged Tagged	Tagged ▼ Tagged ▼	Tagged <b>v</b> Tagged <b>v</b>	Tagged Tagged	• •	Ta Ta
Firewall     VPN	Add Edit	Delete									
Certificate Management     Log     SSL VPN	Save	Cancel									
User Management Wizard											
© 2013 Cisco Systems, Inc. All Rig	flats Reserved.										•

Étape 7. Choisissez l'option souhaitée dans la liste déroulante pour le port LAN avec lequel vous êtes connecté et le paramètre doit correspondre au port connecté. Si vous êtes connecté avec plusieurs ports, vous devez choisir les mêmes paramètres pour chaque port que vous êtes connecté. La valeur par défaut est tagged, mais le VLAN 1 est untagged.

**Remarque :** si vous activez le routage inter-VLAN à l'étape 6, vous devez marquer le VLAN pour distinguer le trafic.

Étiqueté

- Représente l'association entre le port et le VLAN comme étant balisé.
- Le marquage est utilisé pour déterminer le VLAN auquel le trafic appartient via l'ID de VLAN unique lorsque plusieurs VLAN sont créés pour le même port.

#### Non Étiqueté

- Représente que l'association entre le port et le VLAN n'est pas balisée.
- Il est utilisé lorsqu'un seul VLAN est créé et que le trafic connaît le VLAN. Un seul VLAN peut être marqué comme non balisé pour chaque port LAN.
- Si le VLAN par défaut se trouve sur le port, il doit toujours être non balisé, même si le port comporte plusieurs VLAN.

#### Exclus

- Représente que lâ€<sup>TM</sup>interface nâ€<sup>TM</sup>est pas membre du VLAN.
- Si vous choisissez cette option, le trafic est désactivé entre le VLAN et le port.

cisco RV325 Gi	gabit Dual W	/AN VPN Router					cisco	English 🔻			
Getting Started System Summary	VLAN Memb	ership									
Setup     DHCP     System Management     Port Management	VLAN: Create VLANs ar Up to fourteen ne	AN: Senable eate VLANs and assign the Outgoing Frame Type. 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	LA	
Traffic Statistics	1	Default	Enabled T	Enabled	Untagged V	Untagged V	Untagged T	Untagged V	Untagged	▼ U	
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Та	
DSCP Marking	100	Voice	Enabled T	Disabled 🔻	Tagged 🔻	Tagged 🔻	Tagged T	Tagged •	Tagged	• Ta	
802.1X Configuration	200	Data	Enabled T	Enabled V	Tagged V	Tagged V	Tagged V	Tagged V	Tagged	V Ta	
Firewall	Add Edit	Delete								_	
▶ VPN		Detete									
<ul> <li>Certificate Management</li> </ul>											
▶ Log	Save	Cancel									
SSL VPN											
User Management											
Wizard											
	4									•	
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.										

Étape 8. Cliquez sur Save pour enregistrer les paramètres.

**Remarque :** sur le routeur, vous pouvez vous connecter à l'utilitaire Web et accéder à **DHCP** > **DHCP Setup** pour configurer les VLAN sur un sous-réseau spécifique que vous souhaitez. Par défaut, les VLAN sont configurés pour se trouver sur un sous-réseau différent.

#### Configuration des téléphones SPA/MPP

Les utilisateurs peuvent également configurer les téléphones pour extraire un profil d'un emplacement de profil configuré manuellement, d'un emplacement trouvé via l'option DHCP 150 ou d'un serveur Cisco EDOS. L'exemple suivant est un exemple de configuration manuelle.

Étape 1. Saisissez l'adresse IP du SPA/MPP dans votre navigateur et accédez à Admin Login puis à advanced.

**Remarque :** la configuration du téléphone SPA/MPP peut varier en fonction du modèle. Dans cet exemple, nous utilisons le SPA502G. Pour trouver l'adresse IP de votre téléphone IP, accédez à **DHCP > DHCP Status** sur votre routeur (peut varier selon le modèle). Vous pouvez également appuyer sur le bouton **Setup** et accéder à **Network** sur votre téléphone Cisco (les menus et options peuvent varier selon le modèle de téléphone).



cisco SPA50	ness Pro 2G Configuration	Utility					Admin Login basic (advanced)
Voice	Call History	Personal Direc	tory Attendant	Console Status			
Info	System 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							
	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	·
			Undo All Changes	Submit All Changes			
© 2009 Cisco Systems, Inc	c. All Rights Reserved.						SPA502G IP Phone

Étape 2. Accédez à **Voice > Ext 1**, la page d'extension s'ouvre.

cisco SPA50	siness Pro 02G Configuration (	Jtility				User Login basic   advanced
Voice	Call History	Personal Dire	ctory Attendan	t Console Status		
Info	System SIP	Provisioning	Regional	Phone User	Attendant Console	
Ext 1						
General	Line Enable:	Ves V				
Share Line Appearance	ce	100 1				
	Share Ext:	private 🔻			Shared User ID:	
	Subscription Expires:	3600				
NAT Settings						
	NAT Mapping Enable:	no 🔻	_		NAT Keep Alive Enable:	no 🔻
	NAT Keep Alive Msg:	\$NOTIFY			NAT Keep Alive Dest:	SPROXY
Network Settings						
	SIP TOS/DiffServ Value:	0x68			SIP CoS Value:	3 🔻
	RTP TOS/DiffServ Value:	0xb8			RTP CoS Value:	6 🔻
	Network Jitter Level:	high 🔻			Jitter Buffer Adjustment:	up and down 🔻
SIP Settings						<b>•</b>
			Undo All Changes	Submit All Changes		
© 2009 Cisco Systems, I	nc. All Rights Reserved.					SPA502G IP Phone

Étape 3. Dans la section *Proxy et enregistrement*, saisissez le serveur proxy dans le champ *Proxy*. Dans cet exemple, l'adresse du Raspberry Pi (192.168.3.10) sera utilisée comme serveur proxy. Le VLAN 100 se trouve sur le sous-réseau avec 192.168.3.x.

**Remarque :** vous configurerez l'adresse IP du Raspberry Pi plus loin dans cet article, si vous voulez en savoir plus, cliquez sur le lien à rediriger vers cette section : <u>Modification de l'adresse du</u> <u>Raspberry Pi pour être sur un sous-réseau différent</u>.

،،ا،،،ا،، <sup>Small</sup> Business Pro cisco SPA502G Cor	figuration l	Jtility						<u>User Login</u>	basic   advanced
Voice	Call History	Personal Direct	tory Atten	dant Console Status					
Info System	SIP	Provisioning	Regional	Phone	User Attendan	t Console			
Ext 1									
	CFWD Notifier:								-
Proxy and Registration									
	Proxy:	192.168.3.10	)		1	Jse Outbound Proxy:	no 🔻		
	Outbound Proxy:				Use	e OB Proxy In Dialog:	yes 🔻		
	Register:	yes 🔻			Ma	ike Call Without Reg:	no 🔻		
	Register Expires:	3600			A	ins Call Without Reg:	no 🔻		
	Use DNS SRV:	no 🔻			0	INS SRV Auto Prefix:	no 🔻		
	Proxy Fallback Intvl:	3600			Proxy	Redundancy Method:	Normal	•	
Subscriber Information									
	Display Name:					User ID:			
	Password:					Use Auth ID:	no 🔻		
	Auth ID:								
	Mini Certificate:								
	SRTP Private Key:								
			Undo All Change	Submit All Cha	nges				
© 2009 Cisco Systems, Inc. All Rights R	eserved.								SPA502G IP Phone

Étape 4. Sous *Subscriber Information*, saisissez le nom d'affichage et l'ID utilisateur (numéro de poste) du poste partagé. Dans cet exemple, nous allons utiliser le poste 1003.

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 ALIS CAIL WILLIOUL KEY. 10 Y	
	Use DNS SRV:	no 🔻 DNS SRV Auto Prefix: no 🔻	
	Proxy Fallback Intvl:	3600 Proxy Redundancy Method: Normal	T
Subscriber Informatio	n		
	Display Name:	1003 User ID: (1003	
	Password:	Use Auth ID: no 🔻	
	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	•
	G729a Enable:	yes T G722 Enable: yes T	
	G726-16 Enable:	yes T G726-24 Enable: yes T	
	G726-32 Enable:	yes V G726-40 Enable: yes V	-
		Undo All Changes Submit All Changes	
© 2009 Cisco Systems, I	inc. All Rights Reserved.		SPA502G IP Phone

Remarque : le poste 1003 a déjà été créé et configuré sur le Raspberry Pi.

Étape 5. Saisissez le mot de passe du poste que vous avez configuré dans la section Raspberry Pi extension. Ce nom est également connu sous le nom *Secret* sous la section *Edit Extension* dans le Raspberry Pi. Dans cet exemple, le mot de passe **12345** a été utilisé.

**Remarque :** le mot de passe **12345** n'a été utilisé qu'à titre d'exemple ; un mot de passe plus complexe est recommandé.

CISCO SPA502G Configuration	Jtility	<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.	Alls Call Williou Keg. 10	A
Use DNS SRV:	no 🔻 DNS SRV Auto Prefix: no 🔻	
Proxy Fallback Intvl:	3600 Proxy Redundancy Method: Normal	<b>v</b>
Subscriber Information		
Display Name:	1003 User ID: 1003	
Password:	(12345 Use Auth ID: no 🔻	
Auth ID:		
Mini Certificate:		
SRTP Private Key:		
Audio Configuration		
Preferred Codec:	G711u ▼ Use Pref Codec Only: no ▼	
Second Preferred Codec:	Unspecified  Third Preferred Codec: Unspecifie	d 🔻
G729a Enable:	yes T G722 Enable: yes T	
G726-16 Enable:	yes 🔻 G726-24 Enable: yes 🔻	
G726-32 Enable:	yes 🔻 G726-40 Enable: yes 🔻	•
	Undo All Changes Submit All Changes	
© 2009 Cisco Systems, Inc. All Rights Reserved.		SPA502G IP Phone

Étape 6. Choisissez l'option souhaitée dans la liste déroulante *Use Auth ID*. Les options sont **Yes** et **No**. Pour activer l'authentification SIP (Session Initiation Protocol), où les messages SIP peuvent être remis en question pour déterminer s'ils sont autorisés avant de pouvoir transmettre, choisissez **Yes** dans la liste déroulante *Auth ID*. Dans cet exemple, nous avons choisi **Yes**.

cisco SPA50	<sup>iness Pro</sup> 12G Configuration l	Jtility				<u>User</u>	Login basic   advanced
Voice	Call History	Personal Directo	ory Attendant	Console Status			
Info	System SIP	Provisioning	Regional F	hone User	Attendant Console		
Ext 1							
	register Expires.	3000			Ans Gair Without Reg.	10 1	
	Use DNS SRV:	no 🔻			DNS SRV Auto Prefix:	no 🔻	
	Proxy Fallback Intvl:	3600			Proxy Redundancy Method:	Normal 🔻	
Subscriber Information	n						
	Display Name:	1003			User ID:	1003	
	Password:	12345			Use Auth ID:	yes 🔻	
	Auth ID:						
	Mini Certificate:						
	SRTP Private Key:						
Audio Configuration							
	Preferred Codec:	G711u 🔻			Use Pref Codec Only:	no 🔻	
	Second Preferred Codec:	Unspecified <b>T</b>			Third Preferred Codec:	Unspecified V	
	G729a Enable:	yes 🔻			G722 Enable:	yes 🔻	
	G726-16 Enable:	yes 🔻			G726-24 Enable:	yes 🔻	
	G726-32 Enable:	yes 🔻			G726-40 Enable:	yes 🔻	-
			Undo All Changes	Submit All Changes			
© 2009 Cisco Systems, In	c. All Rights Reserved.						SPA502G IP Phone

Étape 7. Saisissez le poste que vous essayez de configurer pour ce téléphone dans le champ *Auth ID*. L'ID d'authentification est pour l'authentification SIP.

cisco SPA50	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 I	Phone User Attendant	Console	
Ext 1					
	ricgiorer.	yes ·	war	te our vitriout iteg.	
	Register Expires:	3600	Ar	ns Call Without Reg: no 🔻	
	Use DNS SRV:	no 🔻	D	NS SRV Auto Prefix: no 🔻	
	Proxy Fallback Intvl:	3600	Proxy R	edundancy Method: Normal	T
Subscriber Informatio	on				
	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 🔻	U	se Pref Codec Only: no 🔻	
	Second Preferred Codec:	Unspecified V	Thi	rd Preferred Codec: Unspecified V	
	G729a Enable:	yes 🔻		G722 Enable: yes 🔻	
	G726-16 Enable:	yes 🔻		G726-24 Enable: yes 🔻	*
		Undo All Changes	Submit All Changes		
© 2009 Cisco Systems, I	nc. All Rights Reserved.				SPA502G IP Phone

Étape 8. Cliquez ensuite sur Submit All Changes.

**Remarque :** revenez à l'étape 1 de la section Configuration des téléphones SPA/MPP si vous avez d'autres téléphones SPA/MPP à configurer.

#### Configuration des réseaux locaux virtuels sur le commutateur

Étape 1. Connectez-vous à l'utilitaire Web et accédez à VLAN Management > Create VLAN.

**Remarque :** la configuration peut varier en fonction du périphérique. Dans cet exemple, nous utilisons le SF220-24P pour configurer les VLAN.

Small Business cisco SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started  Status and Statistics	Create VLAN
<ul> <li>Administration</li> </ul>	VLAN Table
<ul> <li>Port Management</li> </ul>	VLAN ID VLAN Name Type
<ul> <li>VLAN Management</li> </ul>	1 default Default
Default VLAN Settings Create VLAN	Add Edit Delete
Interface Settings	
Port to VLAN	
Port VLAN Membership	
<ul> <li>Voice VLAN</li> </ul>	
<ul> <li>Spanning Tree</li> </ul>	
<ul> <li>MAC Address Tables</li> </ul>	
<ul> <li>Multicast</li> </ul>	
<ul> <li>IP Configuration</li> </ul>	
<ul> <li>Security</li> </ul>	
<ul> <li>Access Control</li> </ul>	
<ul> <li>Quality of Service</li> </ul>	
▶ SNMP	
© 2014-2017 Cisco Systems, Inc. Al	li Rights Reserved.

Étape 2. Cliquez sur Add... pour créer un nouveau VLAN.

Small Business SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started  Status and Statistics	Create VLAN
<ul> <li>Administration</li> </ul>	VLAN Table
<ul> <li>Port Management</li> </ul>	VLAN ID VLAN Name Type
<ul> <li>VLAN Management</li> </ul>	1 default Default
Default VLAN Settings Create VLAN	Add Edit Delete
Interface Settings	
Port to VLAN	
GVRP Settings	
<ul> <li>Voice VLAN</li> </ul>	
<ul> <li>Spanning Tree</li> </ul>	
MAC Address Tables	
<ul> <li>Multicast</li> </ul>	
<ul> <li>IP Configuration</li> </ul>	
<ul> <li>Security</li> </ul>	
<ul> <li>Access Control</li> </ul>	
<ul> <li>Quality of Service</li> </ul>	
▶ SNMP	
© 2014-2017 Cisco Systems, Inc. Al	I Rights Reserved.

Étape 3. Pour créer un seul VLAN, sélectionnez la case d'option VLAN. Saisissez l'ID et le nom du VLAN. Cliquez ensuite sur Apply pour enregistrer le VLAN. Dans cet exemple, nous allons créer le VLAN 100 pour la voix et le VLAN 200 pour les données.

**Remarque :** certains VLAN sont requis par le système pour une utilisation interne du système et ne peuvent donc pas être créés en entrant le VID de début et le VID de fin inclus. Lors de l'utilisation de la fonction **Range**, le nombre maximal de VLAN que vous pouvez créer simultanément est de 100.

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

Remarque : répétez l'étape 2 si vous devez créer un autre VLAN unique.

#### **Configuration du VLAN voix sur le commutateur**

Étape 1. Connectez-vous à la configuration Web et accédez à VLAN Management > Voice VLAN > Properties.

**Remarque :** la configuration du VLAN voix automatique applique automatiquement les paramètres QoS au VLAN voix et donne la priorité au trafic voix.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch € Logout About Heal										
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	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	DSCP: 46 ▼ (Default: 46) DSCP: 46										
Telephony OUI Telephony OUI Interface	Dynamic Voice VLAN Settings:										
<ul> <li>Spanning Tree</li> </ul>	Dynamic Voice VLAN: • Enable Auto Voice VLAN • Enable Telephony OUI										
MAC Address Tables	Disable										
Multicast     IB Configuration											
Security	Appy Cancel										
<ul> <li>Access Control</li> </ul>											
<ul> <li>Quality of Service</li> </ul>											
SNMP											
© 2014-2017 Cisco Systems, Inc. Al	II Rights Reserved.										

Étape 2. Sous *Administrative Status*, saisissez le VLAN qui doit être le VLAN voix dans le champ *Voice VLAN ID*. Dans cet exemple, le VLAN 100 est saisi comme étant le VLAN voix.

**Remarque :** les modifications apportées à l'ID VLAN voix, à la classe de service (CoS)/802.1p et/ou au point de code de service différencié (DSCP) entraînent l'annonce du VLAN voix administratif comme VLAN voix statique par le périphérique. Si l'option *Auto Voice VLAN activation* déclenchée par le VLAN voix externe est sélectionnée, alors les valeurs par défaut doivent être conservées. Dans

cet exemple, CoS/802.1p est conservé par défaut sur 5 et DSCP est conservé par défaut sur 46.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started   Status and Statistics  Administration  Port Management	Properties CoSi802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN. Voice VLAN Settings:
VCAN Management     Default VLAN Settings     Create VLAN     Interface Settings     Port to VLAN     Port VLAN Membership     GVRP Settings     Voice VLAN     Port VLAN Membership     GVRP Settings     Voice VLAN     Port VLAN     Por	Administrative Status:     Operational Status:       • Voice VLAN ID:     100       (Range: 1 - 4094, Default: 1)     Voice VLAN ID:       CoS/802.1p:     5       DSCP:     46       Dynamic Voice VLAN Settings:       Dynamic Voice VLAN:     • Enable Auto Voice VLAN       Enable Telephony OUI       Disable
Cuality of service  SNMP  © 2014-2017 Cisco Systems, Inc. A	I Rights Reserved.

Étape 3. Cliquez sur Apply pour enregistrer vos paramètres.

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.
<ul> <li>VLAN Management</li> </ul>	Volce VLAN Settings:
Default VLAN Settings Create VLAN	Administrative Status: Operational Status:
Port to VLAN	O 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	DSCP: 46 V (Default: 46) DSCP: 46
Properties Telephony OUI Telephony OUI Interface	Dynamic Voice VLAN Settings:
<ul> <li>Spanning Tree</li> </ul>	Dynamic Voice VLAN:  Enable Auto Voice VLAN Enable Telephony OUI
<ul> <li>MAC Address Tables</li> </ul>	Disable
<ul> <li>Multicast</li> <li>IB Configuration</li> </ul>	
<ul> <li>P Conliguration</li> <li>Security</li> </ul>	Apply Cancel
Access Control	
Quality of Service	
▶ SNMP	
© 2014-2017 Cisco Systems, Inc. A	II Rights Reserved.

#### Configuration des paramètres d'interface sur le commutateur

Les interfaces, les ports physiques du commutateur, peuvent être affectées à l'un des paramètres suivants :

- Général : le port peut prendre en charge toutes les fonctions définies dans la spécification IEEE 802.1q. L'interface peut être un membre balisé ou non balisé d'un ou plusieurs VLAN.
- Accès : un seul VLAN peut être configuré sur l'interface et ne peut transporter qu'un seul VLAN.
- Trunk : peut transporter le trafic de plusieurs VLAN sur une seule liaison et vous permettre d'étendre les VLAN sur le réseau.
- Dot1p-Tunnel : met l'interface en mode QinQ. Cela permet à l'utilisateur d'utiliser ses propres arrangements VLAN (PVID) sur le réseau du fournisseur. Le commutateur est en mode QinQ lorsqu'il dispose d'un ou de plusieurs ports de tunnel dot1p.

Étape 1. Connectez-vous à la configuration Web et accédez à VLAN Management > Interface Settings.

Small Business cisco SF220-24P	24-Po	ort 10/	100 P	oE Smart Swi	tch				cisco Language:	English	Y		out Help
Getting Started  Status and Statistics	Interfa	ace Set	ttings										^
<ul> <li>Administration</li> </ul>	Interfa	ce Setting	gs Table							Showing 1-26	of 26 Al	<ul> <li>per pa</li> </ul>	ge
<ul> <li>Port Management</li> </ul>	Eilter:	Interface	Type equal:	s to Port V Go									
<ul> <li>VLAN Management</li> </ul>	-				Administrative DV//D	Corner Trans	In succes Filtering	Lindinia					
Default VLAN Settings		nury NO.	Internace	Truela	Administrative PVID	Prame Type	Eachlad	Disabled					
Create VLAN		2	FEI	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					
<ul> <li>Voice VLAN</li> </ul>		5	FED	Trunk	1	Admit All	Enabled	Disabled					
Properties		6	FE6	Trunk	1	Admit All	Enabled	Disabled					
Telephony OUI Interface		/	FE/	Trunk	1	Admit All	Enabled	Disabled					
<ul> <li>Spanning Tree</li> </ul>		8	FE8	Trunk	1	Admit All	Enabled	Disabled					
MAC Address Tables		9	FE9	Trunk	1	Admit All	Enabled	Disabled					
Multicast	$\odot$	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					
	0	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	served.											

Étape 2. Sélectionnez le mode d'interface du VLAN. Dans cet exemple, nous allons configurer le Raspberry Pi (port : FE3) comme port d'accès.

Small Business SF220-24P	24-	Port 10	)/100 F	PoE Smart Swi	itch						English		- Logo	Help
Getting Started  Status and Statistics	Inte	erface S	ettings											*
<ul> <li>Administration</li> </ul>	Int	erface Setti	face Settings Table Showing 1-26 of 26 All ▼ per page											
<ul> <li>Port Management</li> </ul>	Filt	ter: Interfac	e Tvpe equa	Is to Port V Go	]									
<ul> <li>VLAN Management</li> </ul>		Entry No	Interface	Interface VI AN Mode	Administrative P\/ID	Erame Tune	Ingrass Eiltaring	Linlink						4
Default VLAN Settings		Lina y No.	EE1	Trunk	1	Admit All	Enabled	Disabled						4
Unterface Settings		2	FE2	Trunk	1	Admit All	Enabled	Disabled						
Port to VLAN		2	EE3	Trunk	1	Admit All	Enabled	Disabled						
Port VLAN Membership		4	EE4	Trunk	1	Admit All	Enabled	Disabled						1 1
GVRP Settings		- 5	EE5	Trunk	1	Admit All	Enabled	Disabled						
Voice VLAN		6	FE6	Trunk	1	Admit All	Enabled	Disabled						
Spanning Tree		7	FE7	Trunk	1	Admit All	Enabled	Disabled						
Multicost		,	FE8	Trunk	1	Admit All	Enabled	Disabled						
<ul> <li>Multicast</li> <li>IP Configuration</li> </ul>		9	FEQ	Trunk	1	Admit All	Enabled	Disabled						
<ul> <li>F Configuration</li> <li>Security</li> </ul>		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		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						
		10	FE17	Trunk	1	Admit All	Enabled	Disabled						-
© 2014-2017 Cisco Systems, Inc. A	II Rights	s Reserved.	1 = 1/	TUTK	I	Asing All	Linabled	Disabled						

Étape 3. Cliquez ensuite sur Modifier... pour modifier l'interface.

Small Business cisco SF220-24P	24-Po	rt 10	/100	PoE Smart Switch						English	•	Logout	Help
Getting Started		7	EE7	Trunk	1	Admit All	Enabled	Dischlod					-
Status and Statistics		/	FE/	Truck	1	Admit All	Enabled	Disabled					
Administration		0	FEO	Trunk	1	Admit All	Enabled	Disabled					
Port Management		9	FE9	Trunk	1	Admit All	Enabled	Disabled					
✓ VLAN Management		10	FE10	Irunk	1	Admit All	Enabled	Disabled					
Default VLAN Settings		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		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					
Spanning Tree		17	FE17	Trunk	1	Admit All	Enabled	Disabled					
MAC Address Tables		18	FE18	Trunk	1	Admit All	Enabled	Disabled					
Multicast	$\odot$	19	FE19	Trunk	1	Admit All	Enabled	Disabled					
IP Configuration		20	FE20	Trunk	1	Admit All	Enabled	Disabled					
<ul> <li>Security</li> </ul>		21	FE21	Trunk	1	Admit All	Enabled	Disabled					
Access Control		22	FE22	Trunk	1	Admit All	Enabled	Disabled					
Quality of Service	0	23	FE23	Trunk	1	Admit All	Enabled	Disabled					
▶ SNMP		24	FE24	Trunk	1	Admit All	Enabled	Disabled					
	Õ	25	GE1	Trunk	1	Admit All	Enabled	Disabled					
	ŏ	26	GE2	Trunk	1	Admit All	Enabled	Disabled					
		opy Sett	ings										
© 2014-2017 Cisco Systems, Inc. A	I Rights Res	served.											

Étape 4. Dans le champ *Interface VLAN Mode*, choisissez **Access** pour configurer l'interface en tant que membre non balisé d'un VLAN unique.

🗋 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:	<ul> <li>Admit All</li> <li>Admit Tagged Only</li> <li>Admit Untagged Only</li> </ul>			
Ingress Filtering:	Enable			
Uplink:	Enable			
TPID:	0x8100 V			
Apply Close				Þ

Étape 5. Cliquez sur Apply pour enregistrer vos paramètres.

🖹 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:	<ul> <li>General</li> <li>Access</li> <li>Trunk</li> <li>Dot1q-Tunnel (The switch will be in Q-in-Q mode when it has one or more Dot1q</li> </ul>	-Tunnel pc				
Administrative PVID:	1 (Range: 1 - 4094, Default: 1)					
Frame Type:	<ul> <li>Admit All</li> <li>Admit Tagged Only</li> <li>Admit Untagged Only</li> </ul>					
Ingress Filtering:	Enable					
Uplink:	Enable					
TPID:	0x8100 V					
Apply Close						

#### Configuration de l'appartenance VLAN au port sur le commutateur

Une fois les VLAN créés, vous devez les affecter aux ports que vous souhaitez relier.

Étape 1. Connectez-vous à la configuration Web et accédez à VLAN Management > Port VLAN

#### Membership.

Catling Stated			
Status and Statistics     Administration     F - Forbidden member T - Tagged member U - Untagged member P - PVID G - Guest VLAN			^
Port Management Port VLAN Membership Table Showing 1	I-26 of 26 All 🔻	per page	
VLAN Management			
Default VLAN Settings			
Create VLAN Interface Settings EE4 Transk 11/D Official OFFICE OFFICE			
Portio VLAN CE2 Trank 10P 10P, 100T			
Port VLAN Membership			
GVRP Settings OF EF4 Turk 111P 111P			
Volce VLAN     OFFS     Tunk     10			
MAC drifters Tables FF6 Truck 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			
O FE13 Trunk 1UP 1UP			
G FE14 Trunk 1UP 1UP			
O FE15 Trunk 1UP 1UP			
FE16 Trunk 1UP 1UP			-

Étape 2. Dans la *table Port VLAN Membership*, sélectionnez l'interface que vous souhaitez configurer l'appartenance VLAN. Dans cet exemple, nous allons configurer le port Raspberry Pi (Port : FE3) pour qu'il soit sur le VLAN 100.

**Remarque :** tous les périphériques vocaux seront déjà configurés sur le VLAN voix sélectionné dans la section <u>Configuration du VLAN voix sur le commutateur</u>.

Small Business SF220-24P	24-1	Port 10	0/100	PoE Smart Sv	vitch					Language: English	Ŧ	Logou		Help
Getting Started   Status and Statistics  Administration	Por	rt VLAN Membership orbidden member T - Tagged member U - Untagged member P - PVID G - Guest VLAN												
<ul> <li>Port Management</li> </ul>	Po	rt VLAN Me	mbership	Table						Showing 1	-26 of 26	All 🔻	per page	
<ul> <li>VLAN Management</li> </ul>	Eilt.	or: Interfac	o Tuno ogu	ala ta Bart 👅 📿 Ga	7								1 1 5	4
Default VLAN Settings	Filo	ei. Internac	e rype equ		_	1								4
Create VLAN		Interface	Mode	Administrative VLANs	Operational VLANs	LAG								-
Port to VLAN		FEI	Trunk	10P	10P, 1001									
Port VLAN Membership		FE2	Trunk	10P	10P, 1001									
GVRP Settings	$\mathbf{\Theta}$	FE3	Access	10P	10P									
Voice VLAN		FE4	Trunk	10P	10P									
Spanning Tree		FED	Trunk	10P	10P									
MAC Address Tables		FE6	Trunk	10P	10P									
▶ 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	2014-2017 Cisco Systems, Inc. All Rights Reserved.													

Étape 3. Cliquez sur **Joindre un VLAN...** pour modifier le port que vous voulez configurer les VLAN.

Small Business CISCO SF220-24P	24-	Port 1	0/100 P	oE Smart Sw	itch			cisco Language: English	▼ Lo	gout Abo	ut He	
Getting Started		EEP	Trupk	1110	1118							
<ul> <li>Status and Statistics</li> </ul>		FEQ	Trunk	111P	111P							
<ul> <li>Administration</li> </ul>		EE10	Trunk	100	100							
<ul> <li>Port Management</li> </ul>		FEIU	Taunk	105	1UP							
<ul> <li>VLAN Management</li> </ul>		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							
<ul> <li>Voice VLAN</li> </ul>		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. All Rights Reserved.												

Étape 4. Sélectionnez **1UP** et cliquez sur < pour supprimer le VLAN 1 de l'interface dans la section *Select VLAN*. Un seul VLAN non étiqueté peut être ajouté à l'interface lorsqu'il s'agit d'un port d'accès.



Étape 5. Sélectionnez **100** et cliquez sur > pour ajouter le VLAN non balisé à l'interface.

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

Étape 6. Cliquez sur Apply pour enregistrer vos paramètres.

🖒 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:		
200 1		
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN		
Tagging: Forbidden Excluded Tagged Ountagged VID		
Apply Close		

Étape 7. Sélectionnez le port d'interface connecté au routeur dans le champ *Interface*. Dans cet exemple, le port GE1 est sélectionné.

Din VLAN - G	oogle Chrome			$\times$
A Not secure	https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3			
Success icon.	. To permanently save the configuration, go to the Copy/Save Configuration page	or click t	he Save	
Interface:	Port GE1      LAG 1			
Mode:	Trunk			
Select VLAN:				
100 200	nember T - Tagged member U - Untagged member P - PVID G - Guest VI AN			
Tagging:	<ul> <li>Forbidden</li> <li>Excluded</li> <li>Tagged</li> <li>Untagged</li> <li>PVID</li> </ul>			
Apply	Close			

Étape 8. Choisissez le VLAN qui sera ajouté à l'interface sélectionnée, puis cliquez sur > pour les ajouter dans la section *Select VLAN*. Dans cet exemple, nous allons sélectionner VLAN **100** et **200**.

🖹 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:							
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							

Étape 9. Cliquez sur Apply pour enregistrer vos paramètres.

**Remarque :** un redémarrage des téléphones IP peut être nécessaire pour que l'adresse IP passe au sous-réseau correct.

# Modification de l'adresse IP de Raspberry Pi sur un sous-réseau différent

Étape 1. Connectez-vous à votre Raspberry Pi par Secure Shell (SSH) ou connectez votre Raspberry Pi à un moniteur d'ordinateur. Dans cet exemple, nous allons utiliser SSH pour configurer le Raspberry Pi.

**Remarque :** le port du commutateur de votre ordinateur/ordinateur portable doit se trouver sur le même VLAN que le Raspberry Pi et être configuré en tant que port d'accès lors de la configuration des paramètres d'interface. Consultez la section <u>Configuration des paramètres d'interface sur un</u> commutateur et <u>Configuration de l'appartenance VLAN de port sur le commutateur</u> de cet article pour réviser. Assurez-vous que votre adresse IP est sur le même réseau que votre Raspberry Pi afin de SSH dedans. Si votre périphérique ne se trouve pas sur le même réseau que le Raspberry Pi, utilisez une adresse IP statique et changez manuellement votre adresse IP pour qu'elle soit sur le même réseau ou tapez les commandes **ipconfig/release** et **ipconfig/renew** à l'invite de commandes pour obtenir une nouvelle adresse IP. Les clients SSH peuvent varier selon votre système d'exploitation. Dans cet exemple, PuTTY a été utilisé pour SSH dans le Raspberry Pi. Pour plus d'informations sur SSH, cliquez <u>ici</u>.

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

Étape 2. Saisissez l'adresse IP de votre Raspberry Pi dans le champ *Host Name (or IP address)*. Dans cet exemple, 192.168.1.10 est entré.

**Remarque :** vous pouvez utiliser la table DHCP du routeur pour rechercher l'adresse du Raspberry Pi. Dans ce document, ce Raspberry Pi a été préconfiguré pour avoir une adresse IP statique.

PuTTY Configuration		×
Category:		
<ul> <li>Session</li> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> </ul>	Basic options for your PuTTY ses Specify the destination you want to connect Host Name (or IP address) 192.168.1.10 Connection type:	sion to Port 22
Appearance Behaviour Translation Selection Colours Connection Data Proxy	C Raw C Telnet C Rlogin SSH	Load
-Telnet -Rlogin + SSH -Serial		Delete
	Close window on exit: Always Never Only on cle	ean exit
About	Open	Cancel

Étape 3. Entrez **22** comme numéro de port dans le champ *Port*. Le port 22 est le port standard pour le protocole SSH.

PuTTY Configuration		×
Category:		
<ul> <li>Session</li> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> </ul>	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	ion o Port 22 O Serial
<ul> <li>Iranslation</li> <li>Selection</li> <li>Colours</li> <li>Connection</li> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Serial</li> </ul>	Saved Sessions Default Settings	Load Save Delete
	Close window on exit: Always Never Only on clea	an exit
About	Open	Cancel

Étape 4. Dans la section *Type de connexion :* , cliquez sur la case d'option **SSH** pour choisir SSH comme méthode de connexion avec le commutateur. Cliquez ensuite sur **Open** pour démarrer la session.

PuTTY Configuration		×
Category:		
<ul> <li>Session</li> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> </ul>	Basic options for your PuTTY set Specify the destination you want to connect 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	to Port 22 O Serial
Selection - Colours - Connection - Data - Proxy - Telnet - Rlogin + SSH - Serial	Saved Sessions Default Settings	Load Save Delete
About	Close window on exit: Always Never Only on cle	ean exit Cancel

Étape 5. Saisissez le nom d'utilisateur et le mot de passe du RasPBX dans le champ *login as* et *password*.

**Remarque :** l'utilisateur par défaut : **root** et le mot de passe par défaut : **raspberry** 

P 192.168.1.10 - PuTTY	_	$\times$
login as: root root@192 168 1 10's password• □		$\sim$
		~

Étape 6. Pour modifier l'adresse IP de votre réseau Ethernet en adresse IP statique, tapez ifconfig eth0 [adresse IP] netmask [masque réseau]. Dans cet exemple, nous allons utiliser 192.168.3.10 et le masque de réseau 255.255.255.0

ifconfig eth0 192.168.3.10 masque réseau 255.255.255.0

**Remarque :** vous serez déconnecté de la session lorsque vous modifierez l'adresse IP. Pour vous reconnecter au Raspberry Pi, votre ordinateur/ordinateur portable doit se trouver sur le même sous-réseau que le 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 a	rmv7l			
Welcome to RasPBX -	Asterisk for Raspberry Pi				
RasPBX is based on system are free sof described in the in	Debian. The programs included with the Debian tware; the exact distribution terms for each dividual files in /usr/share/doc/*/copyright.	GNU/Li program	nux are		
RasPBX comes with A applicable law.	BSOLUTELY NO WARRANTY, to the extent permitte	d by			
List of RasPBX spec	ific commands:				
raspbx-upgrade	Keep your system up to date with the latest	add-ons	and		
configure-timezone install-fax	Set timezone for both system and PHP Install HvlaFAX				
add-fax-extension install-fail2ban	Add additional fax extension for use with Hy Install Fail2Ban for additional security	laFAX			
install-dongle raspbx-backup	Install GSM/3G calling capability with chan Backup your complete system to an image file	dongle			
Last login: Mon_Dec	18 19:56:37 2017 from 192.168.1.151				
root@raspbx:~#(ifco	nfig eth0 192.168.3.10 netmask 255.255.255.0			~	1

Étape 7. Reconnectez-vous à votre Raspberry Pi à l'aide de l'adresse IP statique configurée à l'étape 6. Dans cet exemple, nous utilisons 192.168.3.10 pour nous reconnecter.

**Remarque :** assurez-vous que votre ordinateur/ordinateur portable se trouve sur le même sous-réseau que le Raspberry Pi ainsi que le VLAN. Si votre ordinateur/ordinateur portable se trouve sur le même VLAN que le Raspberry Pi et que vous n'avez pas l'adresse IP correcte, vous pouvez accéder à votre invite de commande et taper **ipconfig /release** puis **ipconfig /renew** pour demander une nouvelle adresse IP ou vous pouvez configurer votre périphérique pour qu'il ait une adresse IP statique dans les propriétés Ethernet.

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

Étape 8. Dans la ligne de commande, tapez route add default gw [Adresse IP du routeur du sousréseau] pour ajouter une passerelle par défaut.

Remarque : vous pouvez utiliser la commande route pour afficher la table de routage.

route add default gw 192.168.3.1



## Conclusion

Vous devez maintenant avoir correctement configuré un réseau vocal de base. Pour vérifier cela, décrochez l'un des téléphones SPA/MPP et vous devriez entendre une tonalité. Dans ce document, l'un des téléphones SPA/MPP a le poste 1002 et l'autre le poste 1003. Vous devriez pouvoir appeler le poste 1003 lorsque vous utilisez le téléphone SPA/MPP du poste 1002.

#### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.