Cómo crear una red de voz básica con Raspberry Pi

Objetivo

Este documento proporciona instrucciones sobre cómo configurar una red de voz básica con Raspberry Pi como el servidor de comunicación mediante Asterisks. La red de área local virtual (VLAN) y la calidad de servicio (QoS) se utilizarán para ayudar a priorizar el tráfico mediante la separación del tráfico de voz y de datos. El objetivo de esta red es establecer pruebas internas. Estas pruebas le ayudarán a escalar la red de forma adecuada, ver si tiene suficiente ancho de banda para el volumen de voz que espera y encontrar cualquier otra posible contención entre los equipos. También puede ayudar a determinar si desea alojarlo localmente o en la nube. Una vez que una empresa ha alcanzado un determinado tamaño, es posible que prefiera tener su propio controlador de llamadas local, como PBX o PBX IP. Esto haría que las llamadas internas fueran más eficientes, ya que las llamadas entre teléfonos dentro de la empresa no tendrían que enrutarse fuera del edificio y luego volver a conectarse.

Nota importante: Raspberry Pi no es un producto compatible con Cisco. Este documento se ofrece solo como soporte y no es una solución.

Introducción

Para que una empresa pueda desarrollar una actividad comercial eficaz, los empleados deben tener acceso a una red de voz. Esto facilita la comunicación entre los empleados y sus clientes, además de permitirles la posibilidad de comunicarse internamente. Se puede proporcionar a cada empleado un teléfono fijo y/o un teléfono celular, pero esto puede llegar a ser bastante caro. Las empresas suelen optar por configurar una red de voz que, en su lugar, utilice el protocolo de voz sobre IP (VoIP).

La tecnología VoIP le permite utilizar Internet para hacer y recibir llamadas telefónicas desde cualquier ubicación, a cualquier ubicación en el mundo con cargos mínimos, si los hay, de larga distancia. Esto se puede utilizar en cualquier dispositivo que utiliza Internet.

VoIP puede ahorrar dinero a la empresa a la vez que aumenta la productividad, la comunicación y la satisfacción del cliente. Los empleados pueden utilizar diferentes funciones, como enrutamiento de llamadas, música en espera y correo de voz integrado.

Una característica común de VoIP que utilizan muchas empresas es el enrutamiento de llamadas, también conocido como distribuidor automático de llamadas. El enrutamiento de llamadas distribuye las llamadas entrantes al siguiente agente disponible en lugar de enviarlas al buzón de voz. Esto garantiza que las llamadas de los clientes se responderán de la forma más eficaz posible. Después del horario laboral, las llamadas se pueden enviar directamente al correo de voz.

Agregar usuarios y actualizar funciones es un proceso sencillo, que resulta útil cuando su empresa está en expansión o sus necesidades cambian. A diferencia de un sistema telefónico tradicional, no es necesario realizar un cableado costoso.

Para configurar una red VoIP, tiene opciones que considerar. Puede alojar un servicio VoIP para su propio sistema telefónico mediante KSU, sin KSU, centralita privada (PBX) u otro sistema VoIP.

Debe tener en cuenta su presupuesto, el número de empleados y ubicaciones, los servicios disponibles en su zona y el crecimiento de la empresa. Es posible que sea necesario disponer también de formación y equipo adicional, como auriculares. VoIP puede aumentar el uso de datos y es posible que necesite aumentar el ancho de banda para dar cuenta del tráfico de red de voz.

También debe planificar una copia de seguridad, "Plan B", en caso de que la red se caiga alguna vez. Si pierde la alimentación, el sistema VoIP no se conectará. Esta redundancia debe implementarse para restaurar inmediatamente los servicios telefónicos y evitar la interrupción de la productividad empresarial.

En este artículo, implementaremos nuestro propio sistema telefónico con Asterisk, un PBX en un Raspberry Pi.

Nota: una vez completados estos pasos y si desea poder llamar desde su red interna, debe elegir un distribuidor de servicios de telefonía por Internet (ITSP).

Definiciones

Una red de área local virtual (VLAN) permite segmentar lógicamente una red de área local (LAN) en diferentes dominios de difusión. En situaciones en las que se pueden transmitir datos confidenciales en una red, se puede crear una VLAN para mejorar la seguridad mediante la designación de una transmisión a una VLAN específica. Los usuarios en una VLAN específica son los únicos que pueden acceder y manipular los datos en esa VLAN. Las VLAN también pueden utilizarse para mejorar el rendimiento al reducir la necesidad de enviar difusiones y multidifusiones a destinos innecesarios.

Todos los puertos, de forma predeterminada, se asignan a la VLAN 1, por lo que una vez configuradas diferentes VLAN, debe asignar manualmente cada puerto a la VLAN adecuada.

Cada VLAN debe configurarse con un ID de VLAN (VID) único con un valor entre 1 y 4094. El dispositivo reserva VID 4095 como la VLAN de descarte. Todos los paquetes clasificados en la VLAN de descarte se descartan en el ingreso y no se reenvían a un puerto.

La calidad de servicio (QoS) permite dar prioridad al tráfico de las diferentes aplicaciones, usuarios o flujos de datos. También se puede utilizar para garantizar el rendimiento a un nivel especificado, lo que afecta a la QoS del cliente. QoS se ve generalmente afectada por los siguientes factores: fluctuación, latencia y pérdida de paquetes. En la mayoría de los casos, se da prioridad al vídeo o a la VoIP, ya que son los más afectados por QoS.

La centralita privada (PBX) es un sistema de conmutación telefónica que administra las llamadas entrantes y salientes de los usuarios internos de una empresa. Un PBX está conectado al sistema de telefonía pública y enruta automáticamente las llamadas entrantes a extensiones específicas. También comparte y gestiona varias líneas. Un sistema PBX típico para pequeñas empresas incluye líneas telefónicas externas e internas, un servidor informático que administra el switching y el enrutamiento de llamadas, y una consola para el control manual.

Una PBX IP puede hacer todo lo que una PBX tradicional para pequeñas empresas puede hacer y mucho más. Realiza la conmutación y la conexión de VoIP, así como las llamadas de línea fija. Un sistema PBX IP se ejecuta en una red de datos IP, lo que ahorra costes y minimiza la gestión de la red. Puede utilizar teléfonos IP, softphones (que no requieren ningún hardware telefónico más allá de un ordenador y auriculares de micrófono) y teléfonos fijos en un sistema telefónico PBX IP.

Un Raspberry Pi es un equipo pequeño, portátil y económico que funciona como un equipo de escritorio.

Asterisk es un marco de código abierto que puede convertir un equipo, como un Raspberry Pi, en un servidor de comunicaciones. Esto le permite crear su propio sistema telefónico PBX empresarial. En este artículo, Asterisk utiliza FreePBX como una interfaz gráfica de usuario (GUI) que controla y gestiona Asterisk donde puede configurar extensiones, usuarios, etc.

Dispositivos aplicables

Router

- Switch Power over Ethernet (PoE)
- Raspberry Pi (modelos Pi 3 B+, Pi 3, Pi 3, B+, B y A)
- 2 o más teléfonos Cisco SPA/MPP IP Phones

Versión del software

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

Para configurar la red de voz básica con Raspberry Pi, siga estas instrucciones:

Topología:



La imagen para el RasPBX se puede encontrar <u>aquí</u>. Esta imagen debe instalarse en el Raspberry Pi.

Nota: En este documento, el Raspberry Pi con la imagen RasPBX ya está configurado. Para

acceder a la GUI del Raspberry Pi, escriba <u>http://raspbx.local</u> o la dirección IP del Raspberry Pi en su navegador para configurar el PBX. El inicio de sesión predeterminado de FreePBX es user: admin password: admin. Además, Raspberry Pi estaba preconfigurado para tener una dirección IP estática.

Table Of Contents

- 1. Configuración de VLAN en el router
- 2. Configuración de teléfonos SPA/MPP
- 3. Configuración de VLAN en un Switch
- 4. Configuración de VLAN de voz en un switch
- 5. Configuración de los Parámetros de la Interfaz en un Switch
- 6. Configuración de la Pertenencia a VLAN de Puerto en un Switch
- 7. Cambiar la dirección IP de Raspberry Pi para que esté en una subred diferente
- 8. Conclusión

Configuración de VLAN en el router

Paso 1. Inicie sesión en la utilidad basada en web y navegue hasta Administración de puertos > Pertenencia a VLAN.

Nota: Esto puede variar en función del modelo. En este ejemplo, se utiliza RV325. Para obtener más información sobre cómo acceder a la página de configuración basada en Web, haga clic <u>aquí</u>.

cisco RV325 Gig	gabit Dual V	VAN VPN Route	er					cisco English	▼ Log Out	About Help
Getting Started System Summary	VLAN Memb	pership								
Setup DHCP System Management Port Management	VLAN: Create VLANs a Up to fourteen n	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	VLAN Table									
Traffic Statistics	VLAN ID	Description	Disabled	Device Management Enabled	LAN1 Untagged	LAN2 Untagged	LAN3 Untagged	LAN4 Untagged	LAN5 Untagged	LAN6 Untagged
(VLAN Membership) QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
DSCP Marking 802.1X Configuration	100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
▶ Firewall	Add Edit	Delete								
VPN										_
Certificate Management	Save	Cancel								
SSL VPN										
User Management										
Wizard										
	4									•

Paso 2. Marque la casilla de verificación Enable para habilitar la VLAN en el router.

CISCO RV325 Gi	gabit Dual V	/AN VPN Route	er					cisco English	▼ Log Out	About Help
Getting Started System Summary > Setup > DHCP > System Management - Port Management	VLAN Memb	ership Ie Id assign the Outgoing Fran ew VLANs can be created. 1	ne Type. VLAN IDs must be in th	e range (44094)						
Port Setup	VLAN Table									
Traffic Statistics	VLAN ID	Description Default	Inter VLAN Routing Disabled	Device Management Enabled	LAN1 Untagged	LAN2 Untagged	LAN3 Untagged	LAN4 Untagged	LAN5 Untagged	LAN6 Untagged
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
DSCP Marking 802 1X Configuration	100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
▶ Firewall	Add Edit	Delete								
► VPN										
Certificate Management	Save	Cancel								
► SSL VPN										
User Management										
Wizard										
	4									
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.									

Paso 3. En la sección VLAN Table, haga clic en Add para crear un nuevo ID de VLAN.

Getting Started VLr System Summary VLr > Setup VLr > DHCP Cr > System Management Up Port Management V Port Setup N Port Status N	AN Membe	rship assign the Outgoing Frame Ty VLANs can be created. VLAN Description	ype. 4 IDs must be in the ra	ange (44094)													
Setup VL DHCP Cr System Management Up Port Management Port Setup Port Status	LAN: C Enable treate VLANs and p to fourteen new VLAN Table	assign the Outgoing Frame Ty VLANs can be created. VLAN Description	ype. I IDs must be in the ra	ange (44094)													
Port Setup Port Status	VLAN Table	Description								/LAN:							
Port Status	VLAN ID	Description															
			Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	1	_A						
VLAN Membership	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged		Jn						
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Гас						
DSCP Marking	100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Гас						
802.1X Configuration			Disabled V	Enabled V	Tagged 🔻	Tagged V	Tagged 🔻	Tagged 🔻	Tagged	•	Та						
VPN	Add Edit	Delete															
Certificate Management																	
▶ Log																	
▶ SSL VPN	Save	Cancel															
User Management																	
Wizard																	
											•						

Paso 4. Ingrese un número de VLAN en el campo VLAN ID. Los ID de VLAN deben estar en el rango de 4 a 4094. En este ejemplo, 200 se utiliza para datos como ID de VLAN. A continuación, introduzca una descripción para la VLAN en el campo Description. Los datos se introducen como ejemplo para la descripción. A continuación, haga clic en Guardar.

Nota: VLAN 100 para voz se creó de forma predeterminada en este router. Se pueden crear hasta catorce nuevas VLAN.

Getting Started System Summary Setup	VLAN Member	ership									
Setup	VLAN: 🗹 Enable										
System Management Port Management	Create VLANs and Up to fourteen new	e d assign the Outgoing Frame T w VLANs can be created. VLAt	ype. N IDs must be in the ra	ange (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	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged		Un
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Тас
DSCP Marking	100	Voice 2	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Та
802.1X Configuration	(1 (200))	Data	Disabled •	Enabled •	Tagged 🔻	Tagged 🔻	Tagged 🔻	Tagged 🔻	Tagged	T	Та
Firewall	Add Edit	Delete									
 VPN Cortificate Management 		Delete									
SSI VPN 3	Save	Cancel									
User Management											
Wizard											
	4										Þ

Paso 5. Para editar una VLAN, marque la casilla de verificación de la VLAN correspondiente. En este ejemplo, se editarán las VLAN 1, 100 y 200. A continuación, haga clic en Edit para editar las VLAN.

cisco RV325 Gig	gabit Dual W	/AN VPN Route	er					cisco English	▼ Log Out	About Help
Getting Started System Summary	VLAN Membe	ership								
Setup DHCP System Management Port Management	VLAN: Create VLANs an Up to fourteen ne	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 VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
Traffic Statistics VLAN Membership	 ✓ 1 25 	Default	Disabled	Enabled	Untagged	Untagged	Untagged Tagged	Untagged	Untagged	Untagged
DSCP Marking 802.1X Configuration	⊘ 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
Firewall VPN	Add Edit	Delete	Disabled	Enabled	lagged	lagged	Tagged	Tagged	Tagged	Tagged
Certificate Management Log SSL VPN User Management Wizard	Save	Cancel								
© 2013 Cisco Systems, Inc. All Rid	▲ ahts Reserved.									Þ

Paso 6. (Opcional) En la lista desplegable Inter VLAN Routing, elija Enabled o Disabled para rutear paquetes de una VLAN a otra VLAN. Esta opción es útil porque los administradores de red internos podrán acceder de forma remota a sus dispositivos para ayudar a solucionar sus problemas. Esto reducirá el tiempo de tener que cambiar constantemente las VLAN para acceder a los dispositivos.

- · Deshabilitado: representa que el ruteo entre VLAN está inactivo
- Habilitado: representa que el ruteo entre VLAN está activo en esta VLAN. El ruteo entre VLAN enruta los paquetes solamente entre las VLAN que lo tienen habilitado.

Nota: En este ejemplo, habilitaremos el ruteo Inter VLAN para los ID de VLAN 1, 100 y 200.

cisco RV325 Gig	igabit Dual WAN VPN Router	Help
Getting Started System Summary	VLAN Membership	
Setup DHCP System Management Port Management	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 VLAN ID Description Inter VLAN Routing Device Management LAN1 LAN2 LAN3 LAN4 LAN5	
Traffic Statistics VLAN Membership	Image Control Direction Direction <thdirection< th=""> <thdirect< td=""><td>U</td></thdirect<></thdirection<>	U
QoS:CoS/DSCP Setting DSCP Marking	25 Guest Disabled Disabled Tagged Tagged Tagged Tagged Tagged 100 Voice Enabled Disabled Tagged Tagged Tagged Tagged Tagged Tagged	Ta(Ta
802.1X Configuration Firewall 	200 Data Enabled V Enabled V Tagged V Tagged V Tagged V Tagged V Tagged V	Ta
 VPN Certificate Management 	Add Edit Delete	
► Log ► SSL VPN	Save Cancel	
User Management		
wizard		
	د	•
© 2013 Cisco Systems, Inc. All Rig	lights Reserved.	

Paso 7. Elija la opción que desee en la lista desplegable del puerto LAN al que está conectado y la configuración debe coincidir con el puerto conectado. Si está conectado con más de un puerto, debe seleccionar los mismos parámetros para cada puerto que esté conectado. El valor predeterminado es etiquetado, pero para la VLAN 1 no es etiquetado.

Nota: Si habilita el ruteo entre VLAN en el Paso 6, debe etiquetar la VLAN para distinguir el tráfico.

etiquetado

- Representa que la asociación entre el puerto y la VLAN está etiquetada.
- El etiquetado se utiliza para determinar a qué VLAN pertenece el tráfico a través del ID de VLAN único cuando se crean varias VLAN para el mismo puerto.

Sin etiquetas

- Representa que la asociación entre el puerto y la VLAN no está etiquetado.
- Se utiliza cuando sólo se crea una VLAN y el tráfico es consciente de la VLAN. Solo una VLAN se puede marcar como no etiquetada para cada puerto LAN.
- Si la VLAN predeterminada está en el puerto, siempre debe estar sin etiqueta incluso si el puerto tiene varias VLAN.

Excluido

- Representa que la interfaz no es un miembro de la VLAN.
- Si elige esta opción, el tráfico se inhabilita entre la VLAN y el puerto.

Getting Started VLAN Membership System Summary Setup > Setup VLAN Membership > DHCP Create VLANs and assign the Outgoing Frame Type. > System Management Up to fourteen new VLANs can be created. VLAN IDs must be in the range (44094) Port Status VLAN Table Port Status VLAN ID Description Traffic Statistics 1 VLAN Membership 25 QoS:CoS/DSCP Setting 25 DSCP Marking 100 802.1X Configuration 125 > Firewall Tagged Tagge > VPN Cotificate Management > Log Save Save Cancel	LAN3 gged V Untagg d Tagged	LAN3 ▼ Untagg Tagged	ged V	LAN4 Untagger	▼ t	LAN5 Untage	jed ▼	LA
Setup VLAN: Enable > DHCP Create VLANs and assign the Outgoing Frame Type. > System Management Up to fourteen new VLANs can be created. VLAN IDs must be in the range (44094) Port Status Traffic Statistics VLAN Table VLAN Table OcoS:CoS/DSCP Setting DSCP Marking BOC: Marking 1 Default Enabled Disabled Tagged 25 Guest Disabled Tagged 200 Data Enabled Enabled VPN Certificate Management > Log Save	gged V Untagg td Tagged	LAN3	ged 🔻	LAN4 Untagger	▼ t	LAN5 Untage	jed ▼	LA
Port Setup Port Status Port Status VLAN Table VIAN Memborship VLAN ID CoS:CoS/DSCP Setting DESCP Marking BOCP Marking 25 Guest Disabled Disabled Tagged Tagged Tagged VPN Enabled Cofficate Management Log Save Cancel	LAN3 gged V Untagg ed Tagged	LAN3 Untagg	ged 🔻	LAN4 Untagge	d T	LAN5 Untage	jed ▼	LA
Port Status VLAN ID Description Inter VLAN Routing Device Management LAN1 LAN2 Traffic Statistics VLAN Membership 1 Default Enabled Enabled Untagged Untagged Untagged Untagged Tagged Tag	gged V Untagg d Tagged	 LAN3 Untage Tagged 	ged 🔻	LAN4 Untagge	d 🔻	LAN5 Untage	jed 🔻	LA U
Traffic Statistics 1 Default Enabled Enabled Untagged Untagged Untagged Tagged <	gged v Untagg ed Tagged	 Untagg Tagged 	ged 🔻	Untagge	d▼	Untag	ged ▼	U
Ocs:Cos/DSCP Seting DSCP Marking 802.1X Configuration 25 Guest Disabled Disabled Tagged Tagged 100 Voice Enabled Disabled Tagged Tagged Tagged 200 Data Enabled Enabled Tagged Tagged Tagged VPN Add Edit Delete Enabled Enabled Enabled Enabled Log Save Cancel	d Tagged	Tagged		Transd		Tagged		Tac
DSCP Marking 802.1X Configuration 100 Voice Enabled Tagged				ragged		109900		
802.1X Configuration 200 Data Enabled Tagged Tagged <td< td=""><td>ed 🔻 Tagged</td><td> Tagged </td><td>t ▼</td><td>Tagged</td><td>•</td><td>Tagge</td><td>d 🔻</td><td>Тг</td></td<>	ed 🔻 Tagged	 Tagged 	t ▼	Tagged	•	Tagge	d 🔻	Тг
Firewall Forewall Forewall	ed 🔻 Tagged	 Tagged 	J ▼	Tagged	T	Tagge	d 🔻	Та
VPN Certificate Management Log Save Cancel								
Log Save Cancel					_			
Save Cancel SSLVPN								
SSL VPN								
Liner Management								
User Managenien								
								•

Paso 8. Haga clic en Guardar para guardar la configuración.

Nota: En el router, puede iniciar sesión en la utilidad basada en web y navegar hasta DHCP > DHCP Setup para configurar las VLAN en una subred específica que desee. De forma predeterminada, las VLAN están configuradas para estar en una subred diferente.

Configuración de teléfonos SPA/MPP

Los usuarios también pueden configurar los teléfonos para extraer un perfil desde una ubicación de perfil configurada manualmente, una ubicación encontrada mediante la opción DHCP 150 o desde un servidor EDOS de Cisco. A continuación se muestra un ejemplo de una configuración manual.

Paso 1. Introduzca la dirección IP del SPA/MPP en el navegador, vaya a Admin Login y, a continuación, a advanced.

Nota: La configuración del teléfono SPA/MPP puede variar en función del modelo. En este ejemplo, estamos utilizando el SPA502G. Para buscar la dirección IP del teléfono IP, vaya a DHCP > DHCP Status en el router (puede variar según el modelo). Otra forma consiste en pulsar el botón Setup y navegar hasta Network en el teléfono Cisco (los menús y las opciones pueden variar según el modelo de teléfono).

"Network

1 WANConnection Type DHCP 2 CurrentIP

2 Content 17 192.168.1.115 save

cisco SPA50	siness Pro 02G Configuration	Utility					(Admin Login) basic advance
Voice	Call History	Personal Direc	tory Attendant	Console Status			
Info	System Phone	User					
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, Ir	nc. All Rights Reserved.						SPA502G IP Pho

C.AI

Paso 2. Navegue hasta Voz > Extensión 1, se abre la página de extensión.

دالارمال، Small Business Pro دוsco SPA502G Configuratio	n Utility			<u>User Login</u>	<u>basic</u> advanced
Voice Call History	Personal Directory	Attendant Console Status			
Info System SIP	Provisioning Regiona	I Phone User	Attendant Console		
Ext 1					
General					^
Line Enab	e: yes ▼				
Share Line Appearance					
Share E	tt: private 🔻		Shared User ID:		
Subscription Expin	s: 3600				
NAT Settings					
NAT Mapping Enab	e: no 🔻		NAT Keep Alive Enable:	no 🔻	
NAT Keep Alive M	g: \$NOTIFY		NAT Keep Alive Dest:	\$PROXY	
Network Settings					
SIP TOS/DiffServ Value	e: 0x68		SIP CoS Value:	3 🔻	
RTP TOS/DiffServ Value	e: 0xb8		RTP CoS Value:	6 🔻	
Network Jitter Lev	el: high 🔻		Jitter Buffer Adjustment:	up and down 🔻	
SIP Settings					-
	Undo Al	Changes Submit All Changes			
© 2009 Cisco Systems, Inc. All Rights Reserved.					SPA502G IP Phone

Paso 3. En la sección Proxy y Registro, escriba el servidor proxy en el campo Proxy. En este ejemplo, se utilizará la dirección de Raspberry Pi (192.168.3.10) como servidor proxy. VLAN 100 está en la subred con 192.168.3.x.

Nota: Configurará la dirección IP del Raspberry Pi más adelante en este artículo, si desea obtener más información, haga clic en el enlace que se redirigirá a esa sección: <u>Cambiar la dirección del Raspberry Pi para que esté en una subred diferente</u>.

cisco SPA5020	s Pro 6 Configuration l	Jtility						<u>User Login</u>	basic advanced
Voice	Call History	Personal Direc	tory Attenda	nt Console Status					
Info Sy	ystem SIP	Provisioning	Regional	Phone	User Attendant C	onsole			
Ext 1									
	CFWD Notifier:		j						^
Proxy and Registration									
	Proxy:	192.168.3.10)		Use	Outbound Proxy:	no 🔻		
	Outbound Proxy:]		Use C	B 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 Re	dundancy Method:	Normal	•	
Subscriber Information									
	Display Name:]			User ID:			
	Password:]			Use Auth ID:	no 🔻		
	Auth ID:								
	Mini Certificate:								
	SRTP Private Key:								-
			Undo All Changes	Submit All Cha	inges				
© 2009 Cisco Systems, Inc. All	Rights Reserved.								SPA502G IP Phone

Paso 4. En Subscriber Information, introduzca el nombre para mostrar y el ID de usuario (número de extensión) de la extensión compartida. En este ejemplo, utilizaremos la extensión 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.	Alis Gali Villioul Reg.	110 •
	Use DNS SRV:	no 🔻 DNS SRV Auto Prefix:	no 🔻
	Proxy Fallback Intvl:	3600 Proxy Redundancy Method:	Normal v
Subscriber Informatio	on		
	Display Name:	1003 User ID:	1003
	Password:	Use Auth ID:	no 🔻
	Auth ID:		
	Mini Certificate:		
	SRTP Private Key:		
Audio Configuration			
	Preferred Codec:	G711u V Use Pref Codec Only:	no 🔻
	Second Preferred Codec:	Unspecified 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, I	nc. All Rights Reserved.		SPA502G IP Phone

Nota: La extensión 1003 ya se ha creado y configurado en Raspberry Pi.

Paso 5. Introduzca la contraseña de la extensión que ha configurado en la sección Extensión de Raspberry Pi. Esto también se conoce como Secreto en la sección Editar extensión en el Raspberry Pi. En este ejemplo, se utilizó la contraseña 12345. Nota: La contraseña 12345 sólo se utilizó como ejemplo; se recomienda una contraseña más compleja.

cisco SPA5	usiness Pro 02G Configuration l	Itility			<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		Ans Gair Without Reg.	
	Use DNS SRV:	no 🔻		DNS SRV Auto Prefix:	no 🔻
	Proxy Fallback Intvl:	3600		Proxy Redundancy Method:	Normal 🔻
Subscriber Informati	on				
	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 v		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 Ch	anges Submit All Changes		
© 2009 Cisco Systems,	Inc. All Rights Reserved.				SPA502G IP Phone

Paso 6. Elija la opción deseada de la lista desplegable Use Auth ID. Las opciones son Yes y No. Para habilitar la autenticación del protocolo de inicio de sesión (SIP), donde los mensajes SIP se pueden desafiar para determinar si están autorizados antes de que puedan transmitir, elija Yes en la lista desplegable Auth ID. En este ejemplo, elegimos Yes.

uluilu Small Business Pro	Itility	User Login basic advanced
Voice Call History	Personal Directory Attendant Console Status	
Info System SIP	Provisioning Regional Phone User Attendant Console	
Ext 1		
register Expires.	SOUD MITS Gall Williout Reg.	
Use DNS SRV:	no 🔻 DNS SRV Auto Prefix:	no 🔻
Proxy Fallback Intvl:	3600 Proxy Redundancy Method:	Normal
Subscriber Information		
Display Name:	1003 User ID:	1003
Password:	12345 Use Auth ID:	yes V
Auth ID:		
Mini Certificate:		
SRTP Private Key:		
Audio Configuration		
Preferred Codec:	G711u V Use Pref Codec Only:	no 🔻
Second Preferred Codec:	Unspecified Third Preferred Codec:	Unspecified T
G729a Enable:	yes T 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, Inc. All Rights Reserved.		SPA502G IP Phone

Paso 7. Ingrese la extensión que intenta configurar para este teléfono en el campo Auth ID. El ID de autenticación es para la autenticación SIP.

CISCO SPA502G Configuration	Utility	<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		
i reĝiste	. yes '	
Register Expire	: 3600 Ans Call Without Reg:	no 🔻
Use DNS SR	DNS SRV Auto Prefix:	no 🔻
Proxy Fallback Int.	: 3600 Proxy Redundancy Method:	Normal
Subscriber Information	- 1002 HereID	1002
Display Nation	. 1003 Use Auth ID:	
Passwon	USE Additio	yes •
Additio	: [1003	
Mini Certificati		
SRTP Private Ke		
Audio Configuration		
Preferred Code	: G711u VUse Pref Codec Only:	no 🔻
Second Preferred Code	: Unspecified Third Preferred Codec:	Unspecified
G729a Enable	: yes 🔻 G722 Enable:	yes 🔻
G726-16 Enable	G726-24 Enable:	yes 🔻
	Undo All Changes Submit All Changes	
© 2009 Cisco Systems, Inc. All Rights Reserved.		SPA502G IP Phone

Paso 8. A continuación, haga clic en Enviar todos los cambios.

Nota: Vuelva al paso 1 de la sección Configuración de teléfonos SPA/MPP si tiene más teléfonos SPA/MPP que configurar.

Configuración de VLAN en el switch

Paso 1. Inicie sesión en la utilidad basada en web y navegue hasta VLAN Management > Create VLAN.

Nota: La configuración puede variar en función del dispositivo. En este ejemplo, estamos utilizando el SF220-24P para configurar las VLAN.

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

Paso 2. Haga clic en Add... para crear una nueva VLAN.

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

Paso 3. Para crear una única VLAN, seleccione el botón de opción VLAN. Ingrese el ID de VLAN y el nombre de VLAN. A continuación, haga clic en Apply para guardar la VLAN. En este ejemplo, crearemos VLAN 100 para voz y 200 para datos.

Nota: El sistema requiere algunas VLAN para el uso interno del sistema y, por lo tanto, no se pueden crear introduciendo el VID inicial y el VID final, ambos incluidos. Al utilizar la función Range, el número máximo de VLAN que puede crear a la vez es 100.

🗋 Add VLAN - Google Chrome	- 0	×
A Not secure https://192.168.1.100/html/vlan_createAdd.html		
VLAN ID: (Range: 2 - 4094)		
VLAN Name: Voice (5/32 Characters Used)		
Range		
* VLAN Range:	(Range: 2 - 4094)	
Apply Close		

Nota: Repita el paso 2 si necesita crear otra VLAN única.

Configuración de la VLAN de voz en el switch

Paso 1. Inicie sesión en la configuración web y navegue hasta VLAN Management > Voice VLAN > Properties.

Nota: La configuración de la VLAN de voz automática aplicará automáticamente la configuración de QoS para la VLAN de voz y dará prioridad al tráfico de voz.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch	Save cisco Language: English Logout About Help									
Getting Started Status and Statistics Administration	oS/802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.										
 Port Management VLAN Management 	Voice VLAN Settings:										
Default VLAN Settings Create VLAN	Administrative Status:	Operational Status:									
Interface Settings Port to VLAN	Voice VLAN ID: (Range: 1 - 4094, Default: 1)	Voice VLAN ID: 1									
Port VLAN Membership GVRP Settings Voice VLAN	Cos/k02.1p: 5 ▼ (Default: 5) DSCP: 46 ▼ (Default: 46)	CoS/802.1p: 5 DSCP: 46									
Telephony OUI Telephony OUI	Dynamic Voice VLAN Settings:										
Spanning Tree MAC Address Tables	Dynamic Voice VLAN: Enable Auto Voice VLAN Enable Telephony OUI Disable										
Multicast IP Configuration	Apply Cancel										
Access Control											
Quality of Service SNMP											
© 2014-2017 Cisco Systems, Inc. A	I Rights Reserved.										

Paso 2. En Estado administrativo, ingrese la VLAN que debe ser la VLAN de voz en el campo ID de VLAN de voz. En este ejemplo, se ingresa la VLAN 100 como la VLAN de voz.

Nota: Los cambios en el ID de VLAN de voz, la clase de servicio (CoS)/802.1p y/o el punto de código de servicio diferenciado (DSCP) hacen que el dispositivo anuncie la VLAN de voz administrativa como una VLAN de voz estática. Si se selecciona la opción Activación automática de VLAN de voz activada por VLAN de voz externa, se deben mantener los valores predeterminados. En este ejemplo, CoS/802.1p se deja como valor predeterminado de 5 y DSCP se deja como valor predeterminado de 46.

Small Business cisco SF220-24P	cisco Language: English 🗸 Logout About Halp 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 VLAN Management 	Voice VLAN Settings:												
Default VLAN Settings Create VLAN	Administrative Status: Operational Status:												
Interface Settings Port to VLAN	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												
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 Enable Teacheny OII												
MAC Address Tables	Disable												
Multicast													
Security	Apply Cancel												
 Access Control 													
Quality of Service													
SNMP													
© 2014-2017 Cisco Systems, Inc. A	I Richts Reserved.												

Paso 3. Haga clic en Apply para guardar la configuración.

Small Business cisco SF220-24P	24-Port 10/100 PoE Smart Switch	Save cisco Language: English 🗸 Logout About Help										
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 VLAN Management 	Voice VLAN Settings:											
Default VLAN Settings Create VLAN	Administrative Status:	Operational Status:										
Interface Settings Port to VLAN	C Voice VLAN ID: 100 (Range: 1 - 4094, D	fault: 1) Voice VLAN ID: 1										
Port VLAN Membership	CoS/802.1p: 5 ▼ (Default: 5)	CoS/802.1p: 5										
Voice VLAN	DSCP: 46 V (Default: 46)	DSCP: 46										
Properties Telephony OUI Telephony OUI Interface	Dynamic Voice VLAN Settings:											
Spanning Tree MAC Address Tables	Dynamic Voice VLAN: Enable Auto Voice VLAN Enable Telephony OUI Dischle											
 Multicast 	Disable											
IP Configuration	Apply Cancel											
 Security 												
 Access Control 												
 Quality of Service 												
▶ SNMP												
© 2014-2017 Cisco Systems, Inc. A	Rights Reserved.											

Configuración de los parámetros de la interfaz en el switch

Las interfaces, los puertos físicos en el switch, se pueden asignar a una de las siguientes configuraciones:

- General: el puerto admite todas las funciones definidas en la especificación IEEE 802.1q. La interfaz puede ser un miembro etiquetado o no etiquetado de una o más VLAN.
- Acceso: solo puede tener una VLAN configurada en la interfaz y solo puede llevar una VLAN.
- Troncal: puede transportar el tráfico de varias VLAN a través de un único enlace y le permite extender las VLAN a través de la red.
- Dot1p-Tunnel: pone la interfaz en modo QinQ. Esto permite al usuario utilizar sus propias disposiciones de VLAN (PVID) en la red del proveedor. El switch estará en modo QinQ cuando tenga uno o más puertos de túnel dot1p.

Paso 1. Inicie sesión en la configuración web y navegue hasta VLAN Management > Interface Settings.

Small Business CISCO SF220-24P	24-Po	ort 10/	/100 P	oE Smart Swi	tch			-	cisco Lang	uage: English	۲	Logout	About	Hel
Getting Started Status and Statistics	Interf	ace Se	ttings											-
 Administration 	Interfa	erface Settings Table Showing 1-26 of 26 All V per page												
Port Management VLAN Management	Filter:	Interface	Type equal	s to Port 🔻 Go										
Default VLAN Settings	E	Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Uplink						
Create VLAN		1	FE1	Trunk	1	Admit All	Enabled	Disabled						
(Interface Settings)		2	FE2	Trunk	1	Admit All	Enabled	Disabled						
Port to VLAN		3	FE3	Trunk	1	Admit All	Enabled	Disabled						
Port VLAN Membership	\bigcirc	4	FE4	Trunk	1	Admit All	Enabled	Disabled						
Voice VLAN		5	FE5	Trunk	1	Admit All	Enabled	Disabled						
Properties	\bigcirc	6	FE6	Trunk	1	Admit All	Enabled	Disabled						
Telephony OUI		7	FE7	Trunk	1	Admit All	Enabled	Disabled						
Telephony OUI Interface		8	FE8	Trunk	1	Admit All	Enabled	Disabled						
Spanning Tree	\odot	9	FE9	Trunk	1	Admit All	Enabled	Disabled						
 MAC Address Tables 		10	FE10	Trunk	1	Admit All	Enabled	Disabled						
Multicast	\odot	11	FE11	Trunk	1	Admit All	Enabled	Disabled						
IP Configuration		12	FE12	Trunk	1	Admit All	Enabled	Disabled						
Security		13	FE13	Trunk	1	Admit All	Enabled	Disabled						
Access Control		14	FE14	Trunk	1	Admit All	Enabled	Disabled						
 Quality of Service SNMD 		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. Al	Rights R	eserved.												

Paso 2. Seleccione el modo de interfaz para la VLAN. En este ejemplo, configuraremos el Raspberry Pi (puerto: FE3) como puerto de acceso.

Small Business CISCO SF220-24P	24-1	Port 1	0/	′100 P	oE Smart Swi	tch				cisco Language	English	•	Logou	t About	Help
Getting Started	Inte	rfaga	2.01	ttingo											^
 Status and Statistics 	inte	tenace bettings													
 Administration 	Inte	terface Settings Table Showing 1-26 of 26 All 🔻 per page													
 Port Management 	Filte	er Interfa	ace	Type equal	s to Port V Go	1									
 VLAN Management 		Entry M				A deviate to the DMD	E	to one of the stars	Linterio						-
Default VLAN Settings		Entry N	0.	Interrace	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Оріілк						-
Create VLAN			1	FE1	Trunk	1	Admit All	Enabled	Disabled						
Interface Settings			2	FE2	Trunk	1	Admit All	Enabled	Disabled						
Port VI AN Membership	0		3	FE3	Trunk	1	Admit All	Enabled	Disabled						4
GVRP Settings			4	FE4	Trunk	1	Admit All	Enabled	Disabled						
Voice VLAN			5	FE5	Trunk	1	Admit All	Enabled	Disabled						
 Spanning Tree 			6	FE6	Trunk	1	Admit All	Enabled	Disabled						
 MAC Address Tables 			7	FE7	Trunk	1	Admit All	Enabled	Disabled						
 Multicast 			8	FE8	Trunk	1	Admit All	Enabled	Disabled						
 IP Configuration 			9	FE9	Trunk	1	Admit All	Enabled	Disabled						
 Security 			10	FE10	Trunk	1	Admit All	Enabled	Disabled						
 Access Control 	\odot		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						
			17	FE17	Trunk	1	Admit All	Enabled	Disabled						-
© 2014-2017 Cisco Systems, Inc. Al	I Rights	s Reserve													

Paso 3. A continuación, haga clic en Edit... para editar la interfaz.

Small Business cisco SF220-24P	24-Po	ort 10/	′100 F	PoE Smart Switc	h				cisco	Language:	English	T	Logout	About	Help
Getting Started		7	EE7	Trupk	1	Admit All	Enabled	Disabled							-
 Status and Statistics 		,	EE0	Trunk	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	FEIU	Trunk	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							
Voice VLAN	\bigcirc	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		19	FE19	Trunk	1	Admit All	Enabled	Disabled							
IP Configuration		20	FE20	Trunk	1	Admit All	Enabled	Disabled							
Security		21	FE21	Trunk	1	Admit All	Enabled	Disabled							
 Access Control 		22	FE22	Trunk	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							
		Copy Setti	ngs	Edit											
															-
© 2014-2017 Cisco Systems, Inc. A	II Rights R	eserved.		2014-2017 Cisco Systems, Inc. All Rights Reserved.											

Paso 4. En el campo Interface VLAN Mode, elija Access para configurar la interfaz como un miembro sin etiqueta de una sola VLAN.

🗋 Edit Interface Settings	- Google Chrome	_		×
▲ Not secure https :	//192.168.1.100/html/vlan_intfEdit.html?port=FE3			
Interface:	Port FE3 LAG			
Interface VLAN Mode	e: General Access Trunk Dot1q-Tunnel (The switch will be in Q-in-Q mode when it ha	s one or more	e Dot1q-T	unnel pc
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	2			

Paso 5. Haga clic en Apply para guardar la configuración.

🖹 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 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				Þ

Configuración de la Pertenencia a VLAN de Puerto en el Switch

Una vez creadas las VLAN, debe asignar las VLAN a los puertos que desea conectar.

Paso 1. Inicie sesión en la configuración web y navegue hasta VLAN Management > Port VLAN Membership.

Small Business SF220-24P	24-I	Port 10)/100	PoE Smart Sw	vitch				🚫 Save	cisco	Language	English]	T	Logout	About	Help
Getting Started Status and Statistics Administration	Por F - F	rt VLAN Membership orbidden member T - Tagged member U - Untagged member P - PVID G - Guest VLAN															
 Port Management 	Po	Port VLAN Membership Table Showing 1-26 of 26 All V per page															
VLAN Management	Filt	er: Interface		als to Port V Go													1
Default VLAN Settings		late of a sec	Maria			140											
Create VLAN		Internace	Mode	Administrative VLANS	Operational VLANS	LAG											
Port to VLAN		FE1	Trunk	10P	10P, 1001												
Port VLAN Membership)		FE2	Trunk	10P	10P, 1001												
GVRP 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												
	0	FE13	Trunk	1UP	1UP												
		FE14	Trunk	1UP	1UP												
	0	FE15	Trunk	1UP	1UP												
		FE16	Trunk	1UP	1UP												-
© 2014-2017 Cisco Systems, Inc. Al	Rights	s Reserved.															

Paso 2. En Port VLAN Membership Table, seleccione la interfaz en la que desea configurar la pertenencia a VLAN. En este ejemplo, configuraremos Raspberry Pi (Puerto: FE3) para

que esté en VLAN 100.

Nota: Cualquier dispositivo de voz ya se configurará en la VLAN de voz que haya seleccionado en la sección <u>Configuración de VLAN de voz en el switch</u>.

Small Business SF220-24P	24-1	Port 10)/100	PoE Smart Sw	vitch		-		cisco	Language:	English	•	Logo	ut About	Help
Getting Started	Dor	+ \ /I A NI	Momb	arahin											^
 Status and Statistics 	FUI	I VLAN	Membe	ersnip											
 Administration 	F - F	- Forbidden member T - Tagged member U - Untagged member P - PVID G - Guest VLAN													
 Port Management 	Po	Port VLAN Membership Table Showing 1-26 of 26 All V per page													
✓ VLAN Management	E itt.														
Default VLAN Settings	Fill	el. Interiace	e Type equ												4
Create VLAN		Interface	Mode	Administrative VLANs	Operational VLANs	LAG									
Interface Settings		FE1	Trunk	1UP	1UP, 100T										
Port to VLAN		FE2	Trunk	1UP	1UP, 100T										
GVRP Settings	\mathbf{O}														
 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										
		EE15	Trunk	1UP	1UP										
		FE16	Trunk	11 IP	111P										-
© 2014-2017 Cisco Systems, Inc. Al	I Rights	Reserved.	TUTK	.01	.51										

Paso 3. Haga clic en Join VLAN... para modificar el puerto que desea configurar las VLAN.

Small Business	04	Devit 4			it also			cisco Language: English	•	Logout	About	Help
CISCO SF220-24P	24-	-Port T	0/100 P	oe Smart Sw	/itch							
Getting Started	6	FE8	Trunk	1UP	1UP							-
 Status and Statistics 		FE9	Trunk	1UP	1UP							
 Administration 		FE10	Trunk	1UP	1UP							
 Port Management 		EE11	Trunk	1UP	1UP							
 VLAN Management 		EF12	Trunk	1UP	111P							
Default VLAN Settings		FE13	Trunk	111P	111P							
Create VLAN		EE14	Trunk	111P	1110							
Interface Settings		FE15	Trunk	111P	111P							
Port VLAN Membership		EE16	Trunk	100	110							
GVRP Settings		FEI0	Trunk	105	IUP							
Voice VLAN		FEIT	Trunk	TUP	IUP							
 Spanning Tree) FE18	Trunk	10P	10P							
 MAC Address Tables) FE19	Trunk	10P	10P							
 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							
		Join VLAN	Details.									
	F-	Forbidden n	nember	T - Tagged member	U - Untagged member	P - PVID	G - Guest VLAN					-
© 2014-2017 Cisco Systems, Inc. A	All Righ	ts Reserved	l.									

Paso 4. Seleccione 1UP y haga clic en < para quitar la VLAN 1 de la interfaz en la sección Select VLAN. Sólo se puede agregar 1 VLAN sin etiqueta a la interfaz cuando es un puerto de acceso.

Din 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		
PVID		
Apply Close		

Paso 5. Seleccione 100 y haga clic en > para agregar la VLAN sin etiqueta a la interfaz.

🗋 Join VLAN - G	oogle 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	4095P		
F - Forbidden r	nember, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN		
Tagging:	 Forbidden Excluded Tagged Untagged VID 		
Apply	Close		

Paso 6. Haga clic en Apply para guardar la configuración.

🗋 Join VLAN - G	oogle Chrome	_	×
A Not secure	https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3		
Interface:	● Port FE3 ▼ ● LAG 1 ▼		
Mode:	Access		
Select VLAN:			
200 1 F - Forbidden r	hember, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN		
Tagging:	Forbidden		
	Excluded Tagged		
	 Untagged 		
	PVID		
Apply	Close		

Paso 7. Seleccione el puerto de interfaz que está conectado al router en el campo Interface. En este ejemplo, el puerto GE1 está seleccionado.

🗋 Join VLAN - G	oogle Chrome — 🗆 X								
A Not secure	https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3								
Success. To permanently save the configuration, go to the Copy/Save Configuration page or click the Save icon.									
Interface:	● Port GE1 ▼ LAG 1 ▼								
Mode:	Trunk								
Select VLAN:									
100 200 F - Forbidden n	nember, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN								
Tagging:	 Forbidden Excluded Tagged Untagged PVID 								
Apply	Close								

Paso 8. Elija la VLAN que se agregará a la interfaz seleccionada y luego haga clic en > para agregarla en la sección Select VLAN. En este ejemplo, seleccionaremos VLAN 100 y 200.

🗋 Join VLAN - G	🗋 Join VLAN - Google Chrome — 🗆 🗙							
▲ Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3								
Success. To permanently save the configuration, go to the Copy/Save Configuration page or click the Save icon.								
Interface:	● Port GE1 ▼ O LAG 1 ▼							
Mode:	Trunk							
Select VLAN:								
F - Forbladen I	Eorbidden Forbidden							
lagging.	Excluded							
	 Tagged Untagged 							
	PVID							
Apply	Close							

Paso 9. Haga clic en Apply para guardar la configuración.

Nota: Es posible que sea necesario reiniciar los teléfonos IP para que la dirección IP cambie a la subred correcta.

Cambiar la dirección IP de Raspberry Pi para que esté en una subred diferente

Paso 1. Conéctate a tu Raspberry Pi mediante Secure Shell (SSH) o conecta tu Raspberry Pi a un monitor de computadora. En este ejemplo, utilizaremos SSH para configurar el Raspberry Pi.

Nota: el puerto del switch para el ordenador/portátil deberá estar en la misma VLAN que el Raspberry Pi y configurado como puerto de acceso al configurar los parámetros de la interfaz. Consulte <u>Configuración de los parámetros de interfaz en un switch</u> y <u>Configuración de la pertenencia a VLAN de puerto en la sección Switch</u> de este artículo para revisar. Asegúrese de que su dirección IP está en la misma red que su Raspberry Pi para SSH en ella. Si su dispositivo no está en la misma red que el Raspberry Pi, utilice una dirección IP estática y cambie manualmente su dirección IP para que esté en la misma red o puede escribir el comando ipconfig /release e ipconfig/renew en el símbolo del sistema para

obtener una nueva dirección IP. Los clientes SSH pueden variar dependiendo de su sistema operativo. En este ejemplo, PuTTY se utilizó para introducir SSH en el Raspberry Pi. Para obtener más información sobre SSH, haga clic <u>aquí</u>.

PuTTY Configuration			×
Category:			
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Connection 	Basic options Specify the destination Host Name (or IP addr Connection type: O Raw O Telnet Load, save or delete a s Saved Sessions	s for your PuTTY s you want to conne ress) O Rlogin	eession Port 22 3H () Serial
- Data - Proxy - Telnet - Rlogin	Close window on exit: Always	er Only on 	Load Save Delete
About		Open	Cancel

Paso 2. Escriba la dirección IP de su Raspberry Pi en el campo Nombre de host (o dirección IP). En este ejemplo, se introduce 192.168.1.10.

Nota: Puede utilizar la tabla DHCP en el router para encontrar la dirección del Raspberry Pi. En este documento, esta Raspberry Pi estaba preconfigurada para tener una dirección IP estática.

PuTTY Configuration		×
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	Basic options for your PuTTY set Specify the destination you want to connect Host Name (or IP address) 192.168.1.10 Connection type: Raw Telnet Raw Telnet Raw Telnet Raw Default Settings Close window on exit: Always Never Only on classion	ssion t to Port 22 () Serial Load Save Delete
About	Open	Cancel

Paso 3. Ingrese 22 como el número de puerto en el campo Puerto. El puerto 22 es el puerto estándar para el protocolo SSH.

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

Paso 4. En la sección Tipo de conexión: , haga clic en el botón de opción SSH para elegir SSH como método de conexión con el switch. A continuación, haga clic en Abrir para iniciar la sesión.

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

Paso 5. Ingrese el nombre de usuario y la contraseña del RasPBX en el campo login as y password.

Nota: El usuario predeterminado: root y la contraseña predeterminada: raspberry



Paso 6. Para cambiar la dirección IP de su Ethernet para que sea una dirección IP estática, escriba ifconfig eth0 [dirección IP] netmask [máscara de red]. En este ejemplo, utilizaremos 192.168.3.10 y la máscara de red 255.255.255.0

ifconfig eth0 192.168.3.10 netmask 255.255.255.0

Nota: se le desconectará de la sesión cuando cambie la dirección IP. Para volver a conectarse a Raspberry Pi, el ordenador o portátil debe estar en la misma subred que Raspberry Pi (192.168.3.x).

🛃 192.168.3.10 - PuTTY		—		X
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 I system are free soft described in the ind	Debian. The programs included with the Debian tware; the exact distribution terms for each p dividual files in /usr/share/doc/*/copyright.	GNU/Li program	nux 1 are	
RasPBX comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.				
List of RasPBX spec:	ific commands:			
raspbx-upgrade	Keep your system up to date with the latest a security fixes	add-ons	and	
configure-timezone	Set timezone for both system and PHP			
add-fax-extension install-fail2ban install-dongle	Add additional fax extension for use with Hy Install Fail2Ban for additional security Install GSM/3G calling capability with chan of Backup your complete system to an image file	laFAX dongle		
Last login: Mon Dec	18 19.56.37 2017 from 192 168 1 151			
root@raspbx:~#(ifcom	nfig eth0 192.168.3.10 netmask 255.255.255.0			~

Paso 7. Vuelva a conectarse a su Raspberry Pi mediante la dirección IP estática que se configuró en el paso 6. En este ejemplo, utilizamos 192.168.3.10 para volver a conectar.

Nota: Asegúrese de que el ordenador/portátil se encuentra en la misma subred que el Raspberry Pi, así como la VLAN. Si su computadora/laptop está en la misma VLAN que Raspberry Pi y usted no tiene la dirección IP correcta, puede ir al símbolo del sistema y escribir ipconfig /release y luego ipconfig /renew para solicitar una nueva dirección IP o puede configurar su dispositivo para tener una dirección IP estática en las propiedades Ethernet.

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

Paso 8. En la línea de comandos, escriba route add default gw [dirección IP del router de la subred] para agregar una puerta de enlace predeterminada.

Nota: puede utilizar el comando route para ver la tabla de ruteo.

route add default gw 192.168.3.1

🛃 192.168.3.10 - PuTTY	_		Х
Linux raspbx 4.9.59	-v7+ #1047 SMP Sun Oct 29 12:19:23 GMT 2017 armv71		^
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 GNU/Lin tware; the exact distribution terms for each program dividual files in /usr/share/doc/*/copyright.	nux are	
RasPBX comes with A applicable law.	BSOLUTELY NO WARRANTY, to the extent permitted by		
List of RasPBX spec	ific commands:		
raspbx-upgrade	Keep your system up to date with the latest add-ons	and	
configure-timezone	Set timezone for both system and PHP		
install-fax add-fax-extension install-fail2ban install-dongle raspbx-backup	Add additional fax extension for use with HylaFAX Install Fail2Ban for additional security Install GSM/3G calling capability with chan_dongle Backup your complete system to an image file		
Last login: Mon Dec	e <u>18 14:45:13 2017 from 192.168</u> .3.102		
TOOCCTUDDDA. L(TOUC	<u>daa actaare yw 172.100.J.L</u>		· ·

Conclusión

Ahora debería haber configurado correctamente una red de voz básica. Para comprobarlo, descuelgue uno de los teléfonos SPA/MPP y oirá un tono de marcado. En este documento, uno de los teléfonos SPA/MPP tiene la extensión 1002 y el otro tiene 1003. Debería poder llamar a la extensión 1003 cuando utilice el teléfono SPA/MPP de la extensión 1002.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).