How to Create a Basic Voice Network using Raspberry Pi

Objective

This document provides instructions on how to configure a basic voice network with Raspberry Pi as the communication server using Asterisks. Virtual Local Area Network (VLAN) and Quality of Service (QoS) will be used to help prioritize traffic by separating voice and data traffic. The goal of this network is to set up internal testing. These tests will help you to scale your network appropriately, see if you have enough bandwidth for the voice volume you expect, and find any other possible contention between equipment. It can also help determine whether you want to host it locally or in the cloud. Once a company has reached a certain size, they might prefer to have their own local call controller like PBX, or IP PBX. This would make internal calls more efficient since calls between phones inside of the company would not have to be routed out of the building and then back in.

Important Note: The Raspberry Pi is not a Cisco supported product, this document is for support purposes only and is not a solution document.

Introduction

In order for a company to conduct effective business, employees need to have access to a voice network. This facilitates communication between employees and their customers as well as allowing employees the ability to communicate internally. Each employee can be provided with a landline phone and/or a cell phone, but this can get quite expensive. Companies often choose to set up a voice network that utilizes Voice over Internet Protocol (VoIP) instead.

VoIP technology allows you to use the internet to make and receive telephone calls from any location, to any location in the world with minimal, if any, long distance charges. This can be utilized on any device that uses the internet.

VoIP can save a company money while increasing productivity, communication, and customer satisfaction. Employees can utilize different features such as call routing, music on hold, and integrated voicemail.

A common feature of VoIP that many businesses use is call routing, also known as an automatic call distributor. Call routing distributes incoming calls to the next available agent

instead of sending them to voicemail. This ensures that customer calls will be answered as efficiently as possible. After business hours, calls can be sent directly to voicemail.

Adding users and upgrading features is a simple process, which is helpful when your business is expanding or your needs change. Unlike a traditional phone system, no expensive wiring needs to be done.

To set up a VoIP network, you have options to consider. You can host a VoIP service for your own phone system using KSU, KSU-less, Private Branch Exchange (PBX) or another VoIP system.

Your budget, number of employees and locations, services available in your area, and growth of the company should all be considered. Training and additional equipment, such as headsets, may need to be available as well. VoIP can increase your data usage and you may need to raise your bandwidth to account for the voice network traffic.

You should also plan for a backup, "Plan B", in case your network ever goes down. If you lose power, your VoIP system will not connect. This redundancy should be implemented to immediately restore your phone services and prevent interruption of your business productivity.

In this article, we will be deploying our own phone system using Asterisk, a PBX on a Raspberry Pi.

Note: Once you have completed these steps and would also want the ability to call out of your internal network, you would need to choose an Internet Telephony Service Provider (ITSP).

Definitions

A Virtual Local Area Network (VLAN) allows you to logically segment a Local Area Network (LAN) into different broadcast domains. In scenarios where sensitive data may be broadcast on a network, VLANs can be created to enhance security by designating a broadcast to a specific VLAN. Users on a specific VLAN are the only ones that can access and manipulate data on that VLAN. VLANs can also be used to enhance performance by reducing the need to send broadcasts and multicasts to unnecessary destinations.

All ports, by default, are assigned to VLAN 1, so once you set up different VLANs, you need to manually assign each ports to the appropriate VLAN.

Each VLAN must be configured with a unique VLAN ID (VID) with a value from 1 to 4094. The device reserves VID 4095 as the Discard VLAN. All packets classified to the Discard VLAN are discarded at ingress, and are not forwarded to a port.

Quality of Service (QoS) allows you to prioritize traffic for different applications, users, or data flows. It can also be used to guarantee performance to a specified level, thus, affecting the QoS for the client. QoS is generally affected by the following factors: jitter, latency, and packet loss. Most often, video or VoIP is given priority as they are most affected by QoS.

Private Branch Exchange (PBX) is a telephone switching system that manages incoming and outgoing calls for internal users in a company. A PBX is connected to the public phone system and automatically routes incoming calls to specific extensions. It also shares and manages multiple lines. A typical small business PBX system includes external and internal phone lines, a computer server that manages call switching and routing, and a console for manual control.

An IP PBX can do everything a traditional small business PBX can do and more. It performs the switching and connecting of VoIP as well as landline calls. An IP PBX system runs on an IP data network, which saves costs and minimizes network management. You can use IP phones, softphones (which don't require any phone hardware beyond a computer and microphone headset), and landline phones on an IP PBX phone system.

A Raspberry Pi is an inexpensive, small, portable computer that functions like a desktop computer.

Asterisk is an open source framework that can make a computer, such as a Raspberry Pi, into a communication server. This allows you to build your own business PBX phone system. In this article, Asterisk uses FreePBX as a graphical user interface (GUI) that controls and manages Asterisk where you can configure extensions, users, etc.

Applicable Devices

- Router
- Power over Ethernet (PoE) Switch
- Raspberry Pi (Pi 3 B+, Pi 3, Pi 3, B+, B, and A models)
- 2 or more Cisco SPA/MPP IP Phones

Software Version

• 14.0.1.20 (FreePBX)

- 13.20.0 (Asterisk)
- 1.1.1.06 (RV325 Router)
- 1.1.4.1 (SF220-24P)
- 7.1.3 (SPA502G)

To configure Basic Voice Network with Raspberry Pi, follow the guideline below:

Topology:



The image for the RasPBX can be found <u>here</u>. This image needs to be installed on the Raspberry Pi.

Note: In this document, the Raspberry Pi with the RasPBX image is already configured. To access the GUI of the Raspberry Pi, type in <u>http://raspbx.local</u> or the IP address of the Raspberry Pi in your browser to configure the PBX. The default FreePBX login is user: admin password: admin. Also, the Raspberry Pi was preconfigured to have a static IP address.

Table of Contents

1. Setting Up VLANs on the Router

- 2. Configuring SPA/MPP Phones
- 3. Configuring VLANs on a Switch
- 4. Setting Up Voice VLANs on a Switch
- 5. Configuring Interface Settings on a Switch
- 6. Configuring Port VLAN Membership on a Switch
- 7. Changing Raspberry Pi's IP Address to be on a Different Subnet
- 8. Conclusion

Setting Up VLANs on the Router

Step 1. Log in to the web-based utility and navigate to Port Management > VLAN Membership.

Note: This may vary depending on the model. In this example, RV325 is used. For more information about accessing the web-based setup page, click <u>here</u>.

cisco RV325 Gi	gabit Dual V	VAN VPN Route	er					cisco English	Log Out	About Help
Getting Started System Summary > Setup > DHCP > System Management	VLAN Memb	/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 Management Port Setup	VLAN Table	ew vertras can be created.	VEAR IDS must be in th	e range (++00+)						
Port Status Traffic Statistics (VLAN Membership) QoS:CoS/DSCP Setting	VLAN ID 1 25	Description Default Guest	Inter VLAN Routing Disabled Disabled	Device Management Enabled Disabled	LAN1 Untagged Tagged	LAN2 Untagged	LAN3 Untagged Tagged	LAN4 Untagged Tagged	LAN5 Untagged Tagged	LAN6 Untagged Tagged
DSCP Marking 802.1X Configuration	Add Edit	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
VPN Certificate Management										
► Log ► SSL VPN	Save	Cancel								
User Management Wizard										
	•									÷
© 2013 Cisco Systems, Inc. All Rig	phts Reserved.									

Step 2. Check the Enable checkbox to enable VLAN on the router.

cisco RV325 Gi	gabit Dual V	VAN VPN Route	er					cisco English	▼ Log Out	About Help		
Getting Started System Summary > Setup > DHCP	VLAN Memb	VLAN Membership										
 System Management Port Management 	Up to fourteen n	ew VLANs can be created.	VLAN IDs must be in th	e range (44094)								
Port Setup	VLAN Table											
Port Status Traffic Statistics	VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6		
VLAN Membership QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged		
DSCP Marking	100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged		
802.1X Configuration ► Firewall	Add Edit	Delete										
► VPN												
Certificate Management	Save	Cancel										
► Log ► SSL VPN												
User Management												
Wizard												
© 2013 Cisco Systems, Inc. All Rig	phts Reserved.											

Step 3. In the VLAN Table section, Click Add to create a new VLAN ID.

cisco RV325 Gi	gabit Dual W	/AN VPN Router	_				cisco	English v	Log Out Ab	out Help
Getting Started System Summary	VLAN Membe	LAN Membership								
Setup DHCP System Management Port Management	VLAN: Create VLANs an Up to fourteen ne	VLAN: Create VLANs and assign the Outgoing Frame Type. Up to fourteen new VLANs can be created. VLAN IDs must be in the range (44094)								
Port Setup Port Status	VLAN Table	Description	Inter VI AN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LA
Traffic Statistics VLAN Membership	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Un
QoS:CoS/DSCP Setting DSCP Marking	25	Guest Voice	Disabled Disabled	Disabled Disabled	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Taç Taç
802.1X Configuration Firewall 			Disabled V	Enabled •	Tagged V	Tagged v	Tagged v	Tagged V	Tagged	▼ Ta
VPN Certificate Management	Add Edit	Delete								
► Log ► SSL VPN	Save	Cancel								
User Management Wizard										
vizalu	4									Þ
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.									

Step 4. Enter a VLAN number in the VLAN ID field. VLAN IDs must be in range 4 to 4094. In this example, 200 is used for data as VLAN ID. Next, enter a description for the VLAN in the Description field. Data is entered as the example for description. Then click Save.

Note: VLAN 100 for voice was created by default on this router. Up to fourteen new VLANs can be created.

cisco RV325 Gi	gabit Dual \	NAN VPN Router					cisco	English T	Log Out About	Help
Getting Started System Summary	VLAN Mem	AN Membership								
Setup DHCP System Management Port Management	VLAN: Create VLANs Up to fourteen	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	VLAN Table									
Port Status	VLAN IE	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	Тас
802.1X Configuration	1 200	Data	Disabled T	Enabled T	Tagged v	Tagged V	Tagged V	Tagged V	Tagged	▼ Ta
Firewall	Add	t Delete								
 VPN Cartificate Management 		Delete								
Certificate Management										
SSI VPN	Save	Cancel								
User Management										
Wizard										
										•
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.									

Step 5. To edit a VLAN, check the checkbox of the appropriate VLAN. In this example, VLAN 1, 100, and 200 will be edited. Then click Edit to edit the VLANs.

cisco RV325 Gig	IIIIII Small Business English V Log Out About Help CISCO RV325 Gigabit Dual WAN VPN Router									
Getting Started System Summary	VLAN Membe	LAN Membership								
Setup DHCP System Management Port Management	VLAN: Create VLANs and Up to fourteen ne	LAN: S Enable reate VLANs and assign the Outgoing Frame Type. Ip to fourteen new VLANs can be created, VLAN IDs must be in the range (44094)								
Port Setup Port Status	VLAN Table	Description	Inter VI AN Routing	Device Management	LAN1	LAN2	LAN3	I AN4	LAN5	LAN6
Traffic Statistics VLAN Membership	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged
QoS:CoS/DSCP Setting DSCP Marking	25100	Guest Voice	Disabled Disabled	Disabled Disabled	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged
802.1X Configuration Firewall	200	Data	Disabled	Enabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
 VPN Certificate Management 		Delete								
 Log SSL VPN User Management 	Save	Cancel								
Wizard										
© 2013 Cisco Systems, Inc. All Ric	ts Reserved.									•

Step 6. (Optional) In the Inter VLAN Routing drop-down list, choose Enabled or Disabled to route packets from one VLAN to another VLAN. Having this enabled is useful because internal network administrators will be able to remotely access your devices to help troubleshoot your issues. This will reduce the time of having to constantly switch VLANs in order to access the devices.

- Disabled It represents that Inter VLAN Routing is inactive
- Enabled It represents that Inter VLAN Routing is active on this VLAN. Inter VLAN routing routes the packets only among those VLANs that have it enabled.

Note: In this example, we will be enabling Inter VLAN Routing for VLAN ID 1, 100, and 200.

cisco RV325 Gig	abit Dual WAN VPN Router					cisco	English v	Log Out	About	Help
Getting Started System Summary	VLAN Membership									
Setup DHCP System Management	VLAN: Create VLANs and assign the Outgoing Frame T Up to fourteen new VLANs can be created. VLAN	VLAN:								
Port Setup	VLAN Table									
Port Status	VLAN ID Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5		LA
VLAN Membership	1 Default	Enabled V	Enabled	Untagged V	Untagged V	Untagged V	Untagged V	Untagg	ed 🔻	U
QoS:CoS/DSCP Setting	25 Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged		Тас
DSCP Marking 802 1X Configuration	100 Voice	Enabled V	Disabled •	Tagged v	Tagged V	Tagged v	Tagged v	Tagged	•	Ta
Firewall	200 Data	Enabled V	Enabled v	Tagged T	Tagged V	Tagged v	Tagged •	Tagged	•	Ta
▶ VPN	Add Edit Delete									
 Certificate Management 										
▶ Log	Save Cancel									
SSL VPN										
User Management										
Wizard										
										•
© 2013 Cisco Systems, Inc. All Rig	Reserved.									

Step 7. Choose the desired option from the drop-down list for the LAN port with which you are connected and the setting should be matched with the connected port. If you are connected with more than one port, for each port you are connected, you need to choose the same settings. The default is tagged but for VLAN 1 is untagged.

Note: If you enable inter VLAN routing in Step 6, you have to tag the VLAN to distinguish the traffic.

Tagged

- Represents that the association between the port and the VLAN as tagged.
- Tagged is used to determine which VLAN the traffic belongs through the unique VLAN ID when multiple VLANs are created for same port.

Untagged

- Represents that the association between the port and the VLAN is untagged.
- It is used when only one VLAN is created and the traffic is aware of the VLAN. Only one VLAN can be marked as untagged for each LAN port.
- If the default VLAN is on the port, it should always be untagged even if the port has multiple VLANs.

Excluded

- Represents that the interface is not a member of the VLAN.
- If you choose this option, traffic is disabled between the VLAN and the port.

cisco RV325 Gig	ss Gigabit Dual WAN VPN Router Log 0≀	ut About Help								
Getting Started System Summary	VLAN Membership	AN 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)	/LAN: ☑ 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									
Port Status	VLAN ID Description Inter VLAN Routing Device Management LAN1 LAN2 LAN3 LAN4 LAN	N5 LA								
Traffic Statistics	1 Default Enabled V Enabled Untagged V Untag	ntagged 🔻 U								
QoS:CoS/DSCP Setting	25 Guest Disabled Disabled Tagged Taggged Tagged Tagged Tagged Tagged Tagged Tagged Tagged Tagged Tagg	ged Tag								
DSCP Marking	100 Voice Enabled V Disabled V Tagged V	igged 🔻 Ta								
802.1X Configuration	200 Data Enabled V Enabled V Tagged V Tagged V Tagged V Tagged V Tag	igged 🔻 Ta								
Firewall	Add Edit Delete									
► VPN										
Certificate Management										
	Save Cancel									
Viser Management										
Wizard										
	4	•								
© 2013 Cisco Systems, Inc. All Rig	Rights Reserved.									

Step 8. Click Save to save the settings.

Note: On the router, you can log in to the web-based utility and navigate to DHCP > DHCP Setup to configure the VLANs to a specific subnet that you want. By default, the VLANs are configured to be on a different subnet.

Configuring SPA/MPP Phones

Users can also configure the phones to pull a profile from a manually configured profile location, a location found via DHCP option 150, or from a Cisco EDOS server. The following is an example of a manual configuration.

Step 1. Enter the IP address of the SPA/MPP on your browser and navigate to Admin Login and then advanced.

Note: The configuration for the SPA/MPP phone may vary depending on the model. In this example, we are using the SPA502G. To find the IP address of your IP phone, navigate to DHCP > DHCP Status on your router (may vary depending on the model). Another way is to press the Setup button and navigate to Network on your Cisco phone (menus and options may vary depending on the phone model).

<u>"</u>]Network

sawe

1 WANConnection Type DHCP 2.

P Illren ĥ 2.168.1.115 1 edit

small Business cisco SPA502G	^{s Pro} Configuration	Utility		-			(Admin Login) bas	ic (advanced)
Voice	Call History	Personal Directory	Attendant	Console Status				
Info	/stem 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		-
		Unc	lo All Changes	Submit All Changes				
© 2009 Cisco Systems, Inc. All	Rights Reserved.						SP	502G IP Phone

C.AI

Step 2. Navigate to Voice > Ext 1, the extension page opens.

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

Step 3. In the Proxy and Registration section, type in the proxy server in the Proxy field. In this example, the address of the Raspberry Pi (192.168.3.10) will be used as the proxy server. VLAN 100 is on the subnet with 192.168.3.x.

Note: You'll be configuring the IP address of the Raspberry Pi later in this article, if you want to learn more click the link to be redirected to that section: <u>Changing Address of the</u> <u>Raspberry Pi to be on a Different Subnet</u>.

cisco SPA50	iness Pro)2G Configuration	Utility						<u>User Login</u>	<u>basic</u> advanced
Voice	Call History	Personal Direc	ctory Attenda	nt Console Status					
Info	System SIP	Provisioning	Regional	Phone	User Attendar	t Console			
Ext 1									
	CFWD Notifier:]						^
Proxy and Registration	n								
, ,	Proxy:	192.168.3.10)			Use Outbound Proxy:	no 🔻		
	Outbound Proxy:]		Us	e OB Proxy In Dialog:	yes 🔻		
	Register:	yes 🔻			M	ake Call Without Reg:	no 🔻		
	Register Expires:	3600]			Ans Call Without Reg:	no 🔻		
	Use DNS SRV:	no 🔻			1	ONS SRV Auto Prefix:	no 🔻		
	Proxy Fallback Intvl:	3600]		Proxy	Redundancy Method:	Normal	•	
Subscriber Information	n								
	Display Name:]			User ID:			
	Password:]			Use Auth ID:	no 🔻		
	Auth ID:]						
	Mini Certificate:								
	SRTP Private Key:								-
			Undo All Changes	Submit All Char	nges				
© 2009 Cisco Systems, In	nc. All Rights Reserved.								SPA502G IP Phone

Step 4. Under the Subscriber Information, enter in the display name and user ID (extension number) for the shared extension. In this example, we will be using the extension 1003.

cisco SPA5	siness Pro 02G Configuration l	tility		<u>User Login</u> basic advanced
Voice	Call History	Personal Directory Attendant C	onsole Status	
Info	System SIP	Provisioning Regional Ph	one User Attendant Console	
Ext 1				
	register Expires.	000	Ans Gair Without Reg.	10 *
	Use DNS SRV:	no 🔻	DNS SRV Auto Prefix:	no 🔻
	Proxy Fallback Intvl:	3600	Proxy Redundancy Method:	Normal 🔻
Subscriber Informatic	on			
	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 T	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

Note: Extension 1003 has already been created and configured on the Raspberry Pi.

Step 5. Enter in the password of the extension that you have configured in the Raspberry Pi extension section. This is also known as Secret under the Edit Extension Section in the Raspberry Pi. In this example, the password 12345 was used.

Note: The password 12345 was only used as an example; a more complex password is recommended.

cisco SPA50	iness Pro)2G Configuration l		<u>User Login</u> basic advanced		
Voice	Call History	Personal Directory	Attendant Console Status		
Info	System SIP	Provisioning Regional	Phone	ser Attendant Console	
Ext 1					
	Register Expires.	3000		Ans Gair Without Reg.	10 •
	Use DNS SRV:	no 🔻		DNS SRV Auto Prefix:	no 🔻
	Proxy Fallback Intvl:	3600		Proxy Redundancy Method:	Normal
Subscriber Informatio	n				
	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 T		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 Chang	es	
© 2009 Cisco Systems, Ir	nc. All Rights Reserved.				SPA502G IP Phone

Step 6. Choose the desired option from the Use Auth ID drop-down list. The options are Yes and No. To enable Session Initiation Protocol (SIP) authentication, where SIP messages can be challenged to determine if it is authorized before they can transmit, choose Yes from the Auth ID drop-down list. In this example, we chose Yes.

cisco SPA502	ess Pro G Configuration l	Jtility				<u>User Login</u> basic advanced
Voice	Call History	- Personal Direc	ctory Attendan	t Console Status		
Info	System SIP	Provisioning	Regional	Phone User	Attendant Console	
Ext 1						
	register Expires.	3000			Ans Gair Without Re	±9. <u>110 ×</u>
	Use DNS SRV:	no 🔻	_		DNS SRV Auto Pret	īx: no ▼
	Proxy Fallback Intvl:	3600			Proxy Redundancy Metho	od: Normal 🔻
Subscriber Information			_			
	Display Name:	1003			User I	D: 1003
	Password:	12345			Use Auth I	D: ves V
	Auth ID:					
	Mini Certificate:					
	SRTP Private Key:					
Audio Configuration						
	Preferred Codec:	G711u 🔻			Use Pref Codec On	ly: no 🔻
	Second Preferred Codec:	Unspecified v			Third Preferred Code	ec: Unspecified V
	G729a Enable:	yes 🔻			G722 Enab	le: yes 🔻
	G726-16 Enable:	yes 🔻			G726-24 Enab	le: yes 🔻
	G726-32 Enable:	yes 🔻			G726-40 Enab	le: yes 🔻
			Undo All Changes	Submit All Changes		
© 2009 Cisco Systems, Inc. /	All Rights Reserved.					SPA502G IP Phone

Step 7. Enter the extension that you are trying to configure for this phone in the Auth ID field. The Authentication ID is for SIP authentication.

رالی Small Business Pro دוארס SPA502G Config	guration l	Jtility						<u>User Login</u> <u>basic</u> advanced
Voice	Call History	Personal Dire	ectory Attend	dant Console Status				
Info System	SIP	Provisioning	Regional	Phone	User Attendant Co	onsole		
Ext 1								
	negioter.	yes *	_		Wanc	oan minourney.	L 110 •	A
F	Register Expires:	3600			Ans	Call Without Reg:	no 🔻	
	Use DNS SRV:	no 🔻			DNS	SRV Auto Prefix:	no 🔻	
Pro	xy Fallback Intvl:	3600			Proxy Red	lundancy Method:	Normal	•
Subscriber Information								
	Display Name:	1003				User ID:	1003	
	Password:	12345				Use Auth ID:	yes 🔻	
	Auth ID:	(1003	2			-		
	Mini Certificate:							
SF	RTP Private Key:							
Audio Configuration								
F	Preferred Codec:	G711u 🔻			Use	Pref Codec Only:	no 🔻	
Second F	Preferred Codec:	Unspecified T			Third	Preferred Codec:	Unspecified T	
	G729a Enable:	yes 🔻				G722 Enable:	yes 🔻	
C	G726-16 Enable:	yes 🔻				G726-24 Enable:	yes 🔻	•
			Undo All Change	s Submit All Char	nges			
© 2009 Cisco Systems, Inc. All Rights Rese	erved.							SPA502G IP Phone

Step 8. Then click Submit All Changes.

Note: Go back to Step 1 of Configuring SPA/MPP Phones section if you have more SPA/MPP phones to configure.

Configuring VLANs on the Switch

Step 1. Log in to the web-based utility and navigate to VLAN Management > Create VLAN.

Note: The configuration may vary depending on the device. In this example, we are using the SF220-24P to configure VLANs.

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	
 Voice VLAN 	
Spanning Tree	
MAC Address Tables	
▶ Multicast	
 IP Configuration 	
 Security 	
 Access Control 	
 Quality of Service 	
► SNMP	
© 2014-2017 Cisco Systems, Inc. Al	I Rights Reserved.

Step 2. Click Add... to create a new VLAN.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started	Croate VI AN
 Status and Statistics 	
 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. A	I Rights Reserved.

Step 3. To create a single VLAN, select VLAN radio button. Enter the VLAN ID and VLAN Name. Then click Apply to save the VLAN. In this example, we will be creating VLAN 100 for voice and 200 for data.

Note: Some VLANs are required by the system for internal system usage, and therefore cannot be created by entering the starting VID and ending VID, inclusive. When using the Range function, the maximum number of VLANs you can create at once is 100.

🗋 Add VLAN - Google Chrome		- 0	×						
Not secure https://192.168.1.100/html/vlan_createAdd.html									
VLAN ID: 100	(Range: 2 - 4094)								
VLAN Name: Voice	(5/32 Characters Used)								
Range									
VLAN Range:	-	(Range: 2 - 4094)							
Apply Close									

Note: Repeat Step 2 if you need to create another single VLAN.

Setting Up Voice VLAN on the Switch

Step 1. Log in to the web configuration and navigate to VLAN Management > Voice VLAN > Properties.

Note: Configuring Auto Voice VLAN will automatically apply QoS settings for voice VLAN and prioritize the voice traffic.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch
Getting Started Status and Statistics Administration	Properties CoS/802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.
Port Management VLAN Management	Voice VLAN Settings:
Create VLAN	Administrative Status: Operational Status:
Interface Settings Port to VLAN	O 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
Voice VLAN Properties Telephony QUI	DSCP: 46 (Default: 46) DSCP: 46
Telephony OUI Interface	Dynamic vole v LA settings.
Spanning Tree	Dynamic Voice VLAN: © Enable Auto Voice VLAN Enable Telephony OUI
MAC Address Tables Multicast	Olisable
 IP Configuration 	Apply Cancel
 Security 	
 Access Control 	
 Quality of Service 	
▶ SNMP	
© 2014-2017 Cisco Systems, Inc. A	lil Rights Reserved.

Step 2. Under the Administrative Status, enter the VLAN that is to be the voice VLAN in the Voice VLAN ID field. In this example, VLAN 100 is entered to be the voice VLAN.

Note: Changes in the voice VLAN ID, Class of Service (CoS)/802.1p, and/or Differentiated Service Code Point (DSCP) cause the device to advertise the administrative voice VLAN as a static voice VLAN. If the option Auto Voice VLAN activation triggered by external voice VLAN is selected, then the default values need to be maintained. In this example, CoS/802.1p is left as default of 5 and DSCP is left as default of 46.

Small Business cisco SF220-24P	cisco Language: English v Logout About He 24-Port 10/100 PoE Smart Switch
Getting Started Status and Statistics Administration Port Management	Properties CoSV802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAN.
VLAN Management Default VLAN Settings Create VLAN	Voice VLAN Settings: Administrative Status: Operational Status:
Interface Settings Port to VLAN Port VLAN Membership	© Voice VLAN ID: 100 (Range: 1 - 4094, Default: 1) Voice VLAN ID: 1 CoS/802.1p: 5 (Default: 5) CoS/802.1p: 5
GVRP Settings Voice VLAN Properties	DSCP: 46 (Default: 46) DSCP: 46
Telephony OUI Telephony OUI Interface ▶ Spanning Tree	Dynamic Voice VLAN Settings: Dynamic Voice VLAN:
MAC Address Tables Multicast	Enable Telephony OUI Disable
IP Configuration Security Access Control	Apply Cancel
Quality of Service SNMP	
© 2014-2017 Cisco Systems, Inc. Al	Il Rights Reserved.

Step 3. Click Apply to save your settings.

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 Port Management	Properties CoS/802.1p and DSCP values are used only for LLDP MED Network Policy and Auto Voice VLAI	N.
 VLAN Management 	Voice VLAN Settings:	
Default VLAN Settings Create VLAN	Administrative Status: O	perational Status:
Interface Settings Port to VLAN	Voice VLAN ID: 100 (Range: 1 - 4094, Default: 1) Vo	bice VLAN ID: 1
Port VLAN Membership	CoS/802.1p: 5 ▼ (Default: 5) Co	p\$/802.1p: 5
GVRP Settings Voice VLAN	DSCP: 46 T (Default: 46) DS	SCP: 46
Telephony OUI	Dynamic Voice VLAN Settings:	
Spanning Tree	Dynamic Voice VLAN: Enable Auto Voice VLAN Enable Telephony OUI	
 Multicast 	. Disable	
 IP Configuration 	Apply Cancel	
 Security 		
 Access Control 		
 Quality of Service 		
▶ SNMP		
© 2014-2017 Cisco Systems, Inc. Al	II Rights Reserved.	

Configuring Interface Settings on the Switch

Interfaces, the physical ports on the switch, can be assigned to one of the following settings:

- General: the port can support all functions as defined in the IEEE 802.1q specification. The interface can be a tagged or untagged member of one or more VLANs.
- Access: Can only have one VLAN configured on the interface and can only carry one VLAN.
- Trunk: Can carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across the network.
- Dot1p-Tunnel: puts the interface in QinQ mode. This enables the user to use their own VLAN arrangements (PVID) across the provider network. The switch will be in QinQ mode when it has one or more dot1p-tunnel ports.

Step 1. Log in to the web configuration and navigate to VLAN Management > Interface Settings.

Small Business SF220-24P	24-P	Port 10	/100 P	oE Smart Swi	tch				cisco Language	English	T	Logout		Hel
Getting Started Status and Statistics	Inter	face Se	ettings											^
 Administration 	Inter	face Setti	ngs Table							Showing	1-26 of 26	All ▼ pe	er page	
 Port Management 	Filter	r: Interface	Type equals	s to Port 🔻 Go										1
VLAN Management		Entry No	Interface	Interface V/LAN Mode	Administrative B\/ID	Frame Type	Ingrose Filtering	Liplink						4
Default VLAN Settings		Entry NO.	EE1	Trupk	Authinistrative P VID	Admit All	Enabled	Disabled						4
Create VLAN		2	EE2	Trunk	1	Admit All	Enabled	Disabled						
Port to VLAN		2	FE2 EE2	Trunk	1	Admit All	Enabled	Disabled						
Port VLAN Membership		3	FES	Trunk	1	Admit All	Enabled	Disabled						4
GVRP Settings		4	FE6	Trunk	1	Admit All	Enabled	Disabled						
Voice VLAN		0	FED	Trunk	1	Admit All	Enabled	Disabled						4
Properties Telephony OLU		0	FE0	Trunk	1	Admit All	Enabled	Disabled						
Telephony OUI Interface		/	FE/	Trunk	1	Admit All	Enabled	Disabled						4
Spanning Tree		0	FEO	Trunk	1	Admit All	Enabled	Disabled						
MAC Address Tables		9	FE9	Trunk	1	Admit All	Enabled	Disabled						4
Multicast		10	FEIU	Trunk	1	Admit All	Enabled	Disabled						
 IP Configuration 		11	FEII	Trunk	1	Admit All	Enabled	Disabled						
Security		12	FE12	Trunk	1	Admit All	Enabled	Disabled						
 Access Control 		13	FE13	Trunk	1	Admit All	Enabled	Disabled						
Quality of Service		14	FE14	Trunk	1	Admit All	Enabled	Disabled						
▶ SNMP		15	FE15	Trunk	1	Admit All	Enabled	Disabled						
		16	FE16	Trunk	1	Admit All	Enabled	Disabled						
		17	FE17	Trunk	1	Admit All	Enabled	Disabled						
		18	FE18	Trunk	1	Admit All	Enabled	Disabled			_	_	_	-
© 2014-2017 Cisco Systems, Inc. Al	I Rights F	Reserved.												

Step 2. Select the interface mode for the VLAN. In this example, we will be configuring the Raspberry Pi (port: FE3) to be an access port.

Small Business CISCO SF220-24P	24-1	Port 10	/100 P	oE Smart Swi	tch				cisco Languag	e: English	▼ Lo	gout About	Help
Getting Started	Inte	erface Se	ettings										-
 Status and Statistics 			Jungo										
 Administration 	Inte	erface Settir	ngs Table							Showing 1-26	of 26 All	 per page 	9
 Port Management 	Filte	er: Interface	Type equa	Is to Port V Go									
▼ VLAN Management		Entry Ma	Interface	Interface VII ANI Made	Administrative D)/ID	France Turce	Ingrees Filtering	Linlink					-
Default VLAN Settings		Entry No.	Interface	Trush	Administrative PVID	Frame Type	Final Land	Disabled					-
Create VLAN		1	FEI	Trunk	1	Admit All	Enabled	Disabled					
Port to VLAN		2	FE2	Trunk	1	Admit All	Enabled	Disabled					
Port VLAN Membership	Ο	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 		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					
	0	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	Reserved.											

Step3. Then click Edit... to edit the interface.

Small Business CISCO SF220-24P	24-P	ort 10	/100	PoE Smart Sv	witch				cisco Lang	uage: English	*	Logout	Help
Getting Started		7	FE7	Trunk	1	Admit All	Enabled	Disabled					•
 Status and Statistics 		8	FE8	Trunk	1	Admit All	Enabled	Disabled					
 Administration 		9	FE9	Trunk	1	Admit All	Enabled	Disabled					
 Port Management 		10	FE10	Trunk	1	Admit All	Enabled	Disabled					
 VLAN Management 		11	FE11	Trunk	1	Admit All	Enabled	Disabled					
Default VLAN Settings		12	FE12	Trunk	1	Admit All	Enabled	Disabled					
Create VLAN		13	FE13	Trunk	1	Admit All	Enabled	Disabled					
Port to VLAN		14	FE14	Trunk	1	Admit All	Enabled	Disabled					
Port VLAN Membership		15	EE15	Trunk	1	Admit All	Enabled	Disabled					
GVRP Settings		16	FE16	Trunk	1	Admit All	Enabled	Disabled					
Voice VLAN		17	FE17	Trunk	1	Admit All	Enabled	Disabled					
 Spanning Tree 		19	EE19	Trunk	1	Admit All	Enabled	Disabled					
 MAC Address Tables 		10	EE10	Trunk	1	Admit All	Enabled	Disabled					
 Multicast 		19	FE 19	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					
	\odot	25	GE1	Trunk	1	Admit All	Enabled	Disabled					
		26	GE2	Trunk	1	Admit All	Enabled	Disabled					
		Copy Set	tings	Edit									- -
© 2014-2017 Cisco Systems, Inc. A	© 2014-2017 Cisco Systems, Inc. All Rights Reserved.												

Step 4. In the Interface VLAN Mode field, choose Access to configure the interface as an untagged member of a single VLAN.

🖹 Edit Interface Settings -	Google Chrome	_		Х
A 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-Tu	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				•

Step 5. Click Apply to save your settings.

🗋 Edit Interface Settings -	Google Chrome	_		×
A 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	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				•

Configuring Port VLAN Membership on the Switch

Once the VLANs are created, you need to assign VLANs to the ports you wish to attach.

Step 1. Log in to the web configuration and navigate to VLAN Management > Port VLAN Membership.

Small Business CISCO SF220-24P	24-	Port 10)/100	PoE Smart Sv	vitch				🚫 Save	cisco	Language	English	ı	•	Logou	t About	Help
Getting Started Status and Statistics Administration	Po F-F	rt VLAN Forbidden me	Membe	ership T - Tagged member	U - Untagged mer	nber	P - PVID	G - Guest	VLAN								*
Port Management	Po	ort VLAN Me	mbership	Table								s	howing 1-2	6 of 26	All 🔻	per page	
VLAN Management	Fil	ter: Interface	e Tvpe eau	als to Port V Go						_		_		_			1.1
Default VLAN Settings		Interface	Mode	Administrative VI ANs	Operational VI ANs	LAG											-
Interface Settings		FE1	Trunk	1UP	1UP 100T	LAG											
Port to VLAN		FE2	Trunk	1UP	1UP. 100T												
Port VLAN Membership		FE3	Access	1UP	1UP												
Voice VI AN		FE4	Trunk	1UP	1UP												
Spanning Tree		FE5	Trunk	1UP	1UP												
MAC Address Tables		FE6	Trunk	1UP	1UP												
Multicast		FE7	Trunk	1UP	1UP												
IP Configuration		FE8	Trunk	1UP	1UP												
 Security 		FE9	Trunk	1UP	1UP												
 Access Control 		FE10	Trunk	1UP	1UP												
Quality of Service		FE11	Trunk	1UP	1UP												
► SNMP		FE12	Trunk	1UP	1UP												
		FE13	Trunk	1UP	1UP												
		FE14	Trunk	1UP	1UP												
		FE15	Trunk	1UP	1UP												
© 2014-2017 Cisco Systems Inc. A	Right	FE16	Trunk	1UP	1UP										_		

Step 2. In the Port VLAN Membership Table, select the interface that you want to configure the VLAN membership. In this example, we will be configuring the Raspberry Pi (Port: FE3) to be on VLAN 100.

Note: Any voice devices will already be configured to the voice VLAN that you have selected in the <u>Setting Up Voice VLAN on the Switch</u> section.

Small Business CISCO SF220-24P	24-Port 1(D/100 I	PoE Smart Sv	vitch				cisco	Language:	English	·	Logou	t About	Help
Getting Started	Port VI AN	Membe	ership											^
 Status and Statistics 														
 Administration 	F - Forbidden m	ember	I - lagged member	U - Untagged me	mber	P - PVID	G - Guest VLAN							
 Port Management 	Port VLAN Me	embership	Table							Showir	ng 1-26 of 26	All 🔻	per page	
 VLAN Management 	Filter: Interfac	e Type equ	als to Port 🔻 Go											
Default VLAN Settings														-
Create VLAN	Interface	Mode	Administrative VLANs	Operational VLANs	LAG									-
Rort to VLAN	FE1	Trunk	1UP	1UP, 100T										
Port VLAN Membership	FE2	Trunk	1UP	1UP, 100T										
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										
	FE13	Trunk	1UP	1UP										
	— FE14	Trunk	1UP	1UP										
	FE15	Trunk	1UP	1UP										
	FE16	Trunk	1UP	1UP										-
© 2014-2017 Cisco Systems, Inc. Al	Rights Reserved.													

Step 3. Click Join VLAN... to modify the port that you want to configure VLANs.

Small Business CISCO SF220-24P	24-	Port 10)/100 Po	oE Smart Swi	tch			cisco Language: English	T	Logout	About	Help
Getting Started		EE8	Trunk	1UP	1UP							•
 Status and Statistics 		FE9	Trunk	1UP	1UP							
 Administration 		FE10	Trunk	111P	111P							
 Port Management 		FE11	Trunk	1110	1110							
 VLAN Management 		FE 10	Trunk	100	100							
Default VLAN Settings		FE12	Trunk	100	100							
Create VLAN		FEIJ	Trunk	IUP	IUP							
Interface Settings		FE14	Trunk	10P	10P							
Port to VLAN		FE15	Trunk	10P	10P							
GVRP Settings		FE16	Trunk	10P	10P							
Voice VLAN		FE17	Trunk	1UP	1UP							
Spanning Tree		FE18	Trunk	1UP	1UP							
MAC Address Tables		FE19	Trunk	1UP	1UP							
 Multicast 		FE20	Trunk	1UP	1UP							
 IP Configuration 		FE21	Trunk	1UP	1UP							
 Security 		FE22	Trunk	1UP	1UP							
 Access Control 		FE23	Trunk	1UP	1UP							
 Quality of Service 		FE24	Trunk	1UP	1UP							
▶ SNMP		GE1	Trunk	1UP	1UP							
		GE2	Trunk	1UP	1UP							
	J	bin VLAN)	Details									
	F - F	orbidden me	ember	T - Tagged member	U - Untagged member	P - PVID	G - Guest VLAN					-
© 2014-2017 Cisco Systems, Inc. Al	ll Right	s Reserved.										

Step 4. Select 1UP and click the < to remove VLAN 1 from the interface in the Select VLAN section. Only 1 untagged VLAN can be added to the interface when it is an access port.

🗅 Join VLAN - Google Chrome	_	×
▲ Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3		
Interface: Port FE3 LAG 1		
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		

Step 5. Select 100 and click > to add the untagged VLAN to the interface.

🗋 Join VLAN - Google Chrome	_	×
▲ Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3		
Interface: Port FE3 LAG I		
Mode: Access		
Select VLAN:		
1 1 Image: Construction of the second state of		
Excluded Tagged Untagged		
PVID		
Apply Close		

Step 6. Click Apply to save your settings.

🗋 Join VLAN - Google Chrome	_	Х
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 Image: Construction of the second		
Tagging: Forbidden		
Excluded		
Untagged		
PVID		
Apply Close		

Step 7. Select the Interface port that is connected to the router in the Interface field. In this example, port GE1 is selected.

Din VLAN - Google Chrome -			\times
▲ Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3			
Success. To permanently save the configuration, go to the Copy/Save Configuration page or cli icon.	ck th	e Save	
Interface: OPORT GE1			
Mode: Trunk			
Select VLAN:			
100 10P 200 Image: Comparison of the second sec			
Tagging: Forbidden Excluded Tagged Untagged PVID			
Apply Close			

Step 8. Choose the VLAN that will be added to the selected interface and then click > to add them in the Select VLAN section. In this example, we will be selecting VLAN 100 and 200.

🗋 Join VLAN - G	oogle Chrome —		×					
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:								
E - Eorbidden m	IUP Image: Second se							
Tagging:	Forbidden							
	 Untagged 							
	PVID							
Apply	Close							

Step 9. Click Apply to save your settings.

Note: A reboot on the IP phones may be required in order for the IP address to change to the correct subnet.

Changing IP Address of Raspberry Pi to be on a Different Subnet

Step 1. Connect to your Raspberry Pi by Secure Shell (SSH) or connect your Raspberry Pi to a computer monitor. In this example, we will be using SSH to configure the Raspberry Pi.

Note: The port on the switch for your computer/laptop will need to be on the same VLAN as the Raspberry Pi and configured as an access port when setting up interface settings. Please see <u>Configuring Interface Settings on a Switch</u> and <u>Configuring Port VLAN</u> <u>Membership on the Switch</u> section of this article to review. Make sure that your IP address is on the same network as your Raspberry Pi in order to SSH into it. If your device is not on the same network as the Raspberry Pi, use a static IP address and manually change your IP address to be on the same network or you can type in the command ipconfig /release and ipconfig/renew in the command prompt to obtain a new IP address. SSH clients may vary depending on your operating system. In this example, PuTTY was used to SSH into the Raspberry Pi. For more details about SSH, click <u>here</u>.

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 se Specify the destination you want to connect Host Name (or IP address) Connection type: Raw Telnet Rlogin SSH Load, save or delete a stored session Saved Sessions Default Settings	ession et to Port 22 Serial Load Save Delete
	Close window on exit: Always Never Only on c	lean exit
About	Open	Cancel

Step 2. Type in the IP address of your Raspberry Pi in the Host Name (or IP address) field. In this example, 192.168.1.10 is entered.

Note: You can use DHCP table in the router to find the address of the Raspberry Pi. In this document, this Raspberry Pi was preconfigured to have a static IP address.

		×
		~
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 see 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 Close window on exit:	ssion t to Port 22 () Serial Load Save Delete
	Always Never Only on cle	ean exit
About	Open	Cancel

Step 3. Enter 22 as the port number in the Port field. Port 22 is the standard port for SSH protocol.

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: O Raw O Telnet O Rlogin O SSH Load, save or delete a stored session	ssion t to Port 22 O Serial
	Saved Sessions Default Settings	Load Save Delete
	Close window on exit: Always Never Only on cl	ean exit
About	Open	Cancel

Step 4. In the Connection type: section, click the SSH radio button to choose SSH as your method of connection with the switch. Then click Open to start the session.

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 Rlogin SSH	ssion t to Port 22 Serial
	Saved Sessions	Load Save Delete
	Close window on exit: Always Never Only on clean exit	
About	Open	Cancel

Step 5. Enter the username and password of the RasPBX in the login as and password field.

Note: The default user: root and the default password: raspberry



Step 6. To change the IP address of your Ethernet to be a static IP address, type in ifconfig eth0 [IP address] netmask [netmask]. In this example, we will be using 192.168.3.10 and the netmask of 255.255.255.0

ifconfig eth0 192.168.3.10 netmask 255.255.255.0

Note: You will be disconnected from the session when you change the IP address. In order to connect back to the Raspberry Pi, your computer/laptop needs to be on the same subnet as the Raspberry Pi (192.168.3.x).

🛃 192.168.3.10 - PuTTY		_		\times
Linux raspbx 4.9.59	-v7+ #1047 SMP Sun Oct 29 12:19:23 GMT 2017	armv7l		^
Welcome to RasPBX -	Asterisk for Raspberry Pi			
RasPBX is based on system are free sof described in the in	Debian. The programs included with the Debi tware; the exact distribution terms for eac dividual files in /usr/share/doc/*/copyrigh	an GNU/Li h program t.	nux 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 lates	t 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 Install Fail2Ban for additional security	HylaFAX		
install-dongle raspbx-backup	Install GSM/3G calling capability with cha Backup your complete system to an image fi	n_dongle le		
Last login: Mon Dec	18 19:56:37 2017 from 192.168.1.151			
rool@raspbx:~#(11co	niig einu 192.168.3.10 netmask 255.255.255.			

Step 7. Connect back to your Raspberry Pi using the static IP address that was configured in step 6. In this example, we use 192.168.3.10 to connect back.

Note: Make sure that your computer/laptop is on the same subnet as the Raspberry Pi as well as the VLAN. If your computer/laptop is on the same VLAN as the Raspberry Pi and you don't have the correct IP address, you can go to your command prompt and type in ipconfig /release and then ipconfig /renew to request a new IP address or you can configure your device to have a static IP address in the Ethernet properties.

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

Step 8. In the command line, type in route add default gw [Router IP address of subnet] to add a default gateway.

Note: you can use the command route to see the routing table.

route add default gw 192.168.3.1

🛃 192.168.3.10 - PuTTY		_		×
Linux raspbx 4.9.59	-v7+ #1047 SMP Sun Oct 29 12:19:23 GMT 2017 at	rmv7l		^
Welcome to RasPBX -	Asterisk for Raspberry Pi			
RasPBX is based on Debian. The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.				
RasPBX comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.				
List of RasPBX 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 raspbx-backup	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 14:45:13 2017 from 192.168.3.102			
rooteraspox:~# route add deraurt dw 192.108.3.1		~		

Conclusion

You should now have successfully set up a basic voice network. To verify this, pick up one of the SPA/MPP phones and you should hear a dial tone. In this document, one of the SPA/MPP phones has the extension 1002 and the other one has 1003. You should be able to call the extension 1003 when using extension 1002 SPA/MPP phone.

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。