So erstellen Sie ein einfaches Sprachnetzwerk mit Raspberry Pi

Ziel

Dieses Dokument enthält Anweisungen zur Konfiguration eines Basissprachnetzwerks mit Raspberry Pi als Kommunikationsserver unter Verwendung von Asterisks. Virtual Local Area Network (VLAN) und Quality of Service (QoS) werden zur Priorisierung des Datenverkehrs durch Trennung von Sprach- und Datenverkehr eingesetzt. Ziel dieses Netzwerks ist es, interne Tests einzurichten. Mit diesen Tests können Sie Ihr Netzwerk entsprechend skalieren, feststellen, ob Sie über ausreichend Bandbreite für die erwartete Sprachmenge verfügen, und mögliche Konflikte zwischen den Geräten finden. Darüber hinaus können Sie damit entscheiden, ob Sie das System lokal oder in der Cloud hosten möchten. Wenn ein Unternehmen eine bestimmte Größe erreicht hat, bevorzugt es möglicherweise einen eigenen lokalen Anrufcontroller wie PBX oder IP PBX. Dies würde interne Anrufe effizienter machen, da Anrufe zwischen Telefonen innerhalb des Unternehmens nicht aus dem Gebäude heraus und dann wieder zurück in das Gebäude geleitet werden müssten.

Wichtiger Hinweis: Der Raspberry Pi wird von Cisco nicht unterstützt. Dieses Dokument dient nur Support-Zwecken und ist keine Lösung.

Einleitung

Damit ein Unternehmen seine Geschäftsprozesse effektiv gestalten kann, benötigen die Mitarbeiter Zugriff auf ein Sprachnetzwerk. Dies erleichtert die Kommunikation zwischen Mitarbeitern und ihren Kunden und ermöglicht den Mitarbeitern die Möglichkeit, intern zu kommunizieren. Jeder Mitarbeiter kann mit einem Festnetztelefon und/oder einem Mobiltelefon ausgestattet werden, was jedoch sehr teuer werden kann. Häufig entscheiden sich Unternehmen dafür, ein Sprachnetzwerk einzurichten, das stattdessen Voice over Internet Protocol (VoIP) verwendet.

Die VoIP-Technologie ermöglicht Ihnen, über das Internet Telefonanrufe von jedem Standort an jeden Standort der Welt zu tätigen und zu empfangen, und zwar mit minimalen, wenn überhaupt, Ferngebühren. Dies kann auf jedem Gerät verwendet werden, das das Internet verwendet.

Mit VoIP kann ein Unternehmen Geld sparen und gleichzeitig die Produktivität, Kommunikation und Kundenzufriedenheit steigern. Mitarbeiter können verschiedene Funktionen nutzen, z. B. Anrufweiterleitung, Warteschleifenmusik und integrierte Voicemail.

Eine gemeinsame Funktion von VoIP, die viele Unternehmen nutzen, ist die Anrufweiterleitung, die auch als automatische Anrufverteilung bezeichnet wird. Die Anrufweiterleitung verteilt eingehende Anrufe an den nächsten verfügbaren Mitarbeiter, anstatt sie an die Voicemail weiterzuleiten. So wird sichergestellt, dass Kundenanrufe so effizient wie möglich beantwortet werden. Nach Geschäftsschluss können Anrufe direkt an die Voicemail weitergeleitet werden.

Das Hinzufügen von Benutzern und das Aktualisieren von Funktionen ist ein einfacher Prozess, der hilfreich ist, wenn Ihr Unternehmen expandiert oder sich Ihre Anforderungen ändern. Im Gegensatz zu herkömmlichen Telefonsystemen ist keine teure Verkabelung erforderlich.

Um ein VoIP-Netzwerk einzurichten, müssen Sie verschiedene Optionen in Betracht ziehen. Sie können einen VoIP-Service für Ihr eigenes Telefonsystem mithilfe von Telefonanlagen ohne Telefonanlage, Telefonanlage (PBX) oder einem anderen VoIP-System hosten.

Berücksichtigen Sie dabei Ihr Budget, die Anzahl der Mitarbeiter und Standorte, die in Ihrer Region verfügbaren Services und das Unternehmenswachstum. Auch Schulungen und zusätzliche Geräte wie Headsets sind möglicherweise erforderlich. VoIP kann Ihre Datennutzung erhöhen, und Sie müssen möglicherweise Ihre Bandbreite erhöhen, um den Sprachdatenverkehr im Netzwerk zu berücksichtigen.

Sie sollten auch ein Backup planen, "Plan B", falls Ihr Netzwerk jemals ausfällt. Wenn Sie den Strom verlieren, wird Ihr VoIP-System nicht verbunden. Diese Redundanz sollte implementiert werden, um die Telefondienste sofort wiederherzustellen und eine Unterbrechung der Geschäftsproduktivität zu verhindern.

In diesem Artikel stellen wir unser eigenes Telefonsystem mithilfe von Asterisk, einer Telefonanlage auf einem Raspberry Pi, bereit.

Hinweis: Wenn Sie diese Schritte durchgeführt haben und auch aus Ihrem internen Netzwerk heraus anrufen möchten, müssen Sie einen Internet Telefony Service Provider (ITSP) auswählen.

Definitionen

Ein virtuelles LAN (VLAN) ermöglicht die logische Segmentierung eines LAN (Local Area Network) in verschiedene Broadcast-Domänen. In Umgebungen, in denen über das Netzwerk möglicherweise vertrauliche Daten übertragen werden, kann durch die Erstellung von VLANs die Sicherheit verbessert werden. Eine Übertragung kann dann auf ein spezifisches VLAN beschränkt werden. Nur Benutzer in einem bestimmten VLAN können auf Daten in diesem VLAN zugreifen und diese bearbeiten. Mithilfe von VLANs kann auch die Leistung verbessert werden, da Broadcasts und Multicasts seltener an unnötige Ziele gesendet werden müssen.

Alle Ports sind standardmäßig VLAN 1 zugewiesen. Wenn Sie also verschiedene VLANs einrichten, müssen Sie die Ports manuell dem entsprechenden VLAN zuweisen.

Jedes VLAN muss mit einer eindeutigen VLAN-ID (VID) zwischen 1 und 4094 konfiguriert werden. Das Gerät reserviert die VID 4095 als verworfenes VLAN. Alle Pakete, die dem Verwerfungs-VLAN zugewiesen wurden, werden beim Eingang verworfen und nicht an einen Port weitergeleitet.

Quality of Service (QoS) ermöglicht die Priorisierung des Datenverkehrs für verschiedene Anwendungen, Benutzer oder Datenflüsse. Sie kann auch verwendet werden, um die Leistung auf einem bestimmten Niveau zu garantieren, was sich auf die QoS für den Client auswirkt. Die QoS wird im Allgemeinen von den folgenden Faktoren beeinflusst: Jitter, Latenz und Paketverlust. In den meisten Fällen wird Video oder VoIP Priorität eingeräumt, da sie am stärksten von QoS beeinflusst werden.

Eine Telefonanlage (PBX) ist ein Telefonvermittlungssystem, das ein- und ausgehende Anrufe für interne Benutzer in einem Unternehmen verwaltet. Ein PBX-System ist mit dem öffentlichen Telefonsystem verbunden und leitet eingehende Anrufe automatisch an bestimmte Nebenstellen weiter. Darüber hinaus können mehrere Leitungen gemeinsam genutzt und verwaltet werden. Ein typisches PBX-System für kleine und mittlere Unternehmen umfasst externe und interne Telefonleitungen, einen Computerserver für die Anrufumschaltung und -weiterleitung und eine Konsole für die manuelle Steuerung.

Ein **IP-**PBX-System kann alle Funktionen eines herkömmlichen Small Business-PBX-Systems ausführen und vieles mehr. Er übernimmt das Switching und Verbinden von VoIP- und Festnetzanrufen. Ein IP-PBX-System wird auf einem IP-Datennetzwerk ausgeführt, wodurch Kosten eingespart und die Netzwerkverwaltung minimiert wird. Sie können IP-Telefone, Softphones (die keine andere Telefonhardware als einen Computer und ein Mikrofon-Headset benötigen) und Festnetztelefone auf einem IP-PBX-Telefonsystem verwenden.

Ein **Raspberry Pi** ist ein kostengünstiger, kleiner, tragbarer Computer, der wie ein Desktop-Computer funktioniert.

Asterisk ist ein Open-Source-Framework, das einen Computer, wie z. B. einen Raspberry Pi, zu einem Kommunikationsserver machen kann. Auf diese Weise können Sie Ihr eigenes Telefonanlagensystem für Unternehmen einrichten. In diesem Artikel verwendet Asterisk FreePBX als grafische Benutzeroberfläche (GUI), die Asterisk steuert und verwaltet, wo Sie Erweiterungen, Benutzer usw. konfigurieren können.

Unterstützte Geräte

- Router
- Power over Ethernet (PoE)-Switch
- Raspberry Pi (Modelle Pi 3 B+, Pi 3, Pi 3, B+, B und A)
- 2 oder mehr Cisco SPA/MPP IP-Telefone

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 (SPA 502G)

Um Basic Voice Network mit Raspberry Pi zu konfigurieren, folgen Sie den folgenden Richtlinien:

Topologie:



Das Bild für das RasPBX finden Sie hier. Dieses Image muss auf dem Raspberry Pi installiert werden.

Hinweis: In diesem Dokument ist der Raspberry Pi mit dem RasPBX-Image bereits konfiguriert. Um auf die grafische Benutzeroberfläche des Raspberry Pi zuzugreifen, geben Sie <u>http://raspbx.local</u> oder die IP-Adresse des Raspberry Pi in Ihrem Browser ein, um das PBX-System zu konfigurieren. Die Standard-FreePBX-Anmeldung lautet user: **admin** password: **admin**. Außerdem wurde der Raspberry Pi so vorkonfiguriert, dass er eine statische IP-Adresse hat.

Inhalt

- 1. Einrichten von VLANs auf dem Router
- 2. Konfigurieren von SPA-/MPP-Telefonen
- 3. Konfigurieren von VLANs auf einem Switch
- 4. Einrichten von Sprach-VLANs auf einem Switch
- 5. Konfigurieren der Schnittstelleneinstellungen eines Switches
- 6. Konfigurieren der Port-VLAN-Zugehörigkeit auf einem Switch
- 7. Ändern der IP-Adresse von Raspberry Pi in ein anderes Subnetz
- 8. Schlussfolgerung

Einrichten von VLANs auf dem Router

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und navigieren Sie zu **Port Management > VLAN Membership**.

Hinweis: Dies kann je nach Modell variieren. In diesem Beispiel wird RV325 verwendet. Weitere Informationen zum Zugriff auf die webbasierte Setup-Seite finden Sie <u>hier</u>.

CISCO RV325 Gi	gabit Dual V	/AN VPN Route	er					cisco English	Log Out	
Getting Started System Summary	VLAN Membership									
▶ Setup	VLAN: 🔲 Enat	le								
DHCP	Create VLANs ar	nd assign the Outgoing Fran	ne Type.							
System Management Port Management	Up to fourteen ne	ew VLANs can be created.	VLAN IDs must be in th	e range (44094)						
Port Setup	VLAN Table									
Port Status	VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
Traffic Statistics	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged
QoS:CoS/DSCP Setting	25	Guest	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
DSCP Marking	0 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Tagged
Firewall	Add Edit	Delete								
▶ VPN										
Certificate Management	Save	Cancel								
▶ Log										
 SSL VPN 										
User Management										
Wizard										
© 2013 Cisco Systems, Inc. All Rid	ahts Reserved.									•

Schritt 2: Aktivieren Sie das Kontrollkästchen Aktivieren, um VLAN auf dem Router zu aktivieren.

cisco RV325 Gig	gabit Dual W	/AN VPN Route	r				c	isco English	Log Out	About Help
Getting Started System Summary Setup	VLAN Memb	ership								
DHCP System Management Port Management	Create VLANs an Up to fourteen ne	id assign the Outgoing Fram w VLANs can be created. V	ie Type. /LAN IDs must be in th	e range (44094)						
Port Setup Port Status	VLAN Table	Description	Inter VI AN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LAN6
Traffic Statistics VLAN Membership	1	Default	Disabled	Enabled	Untagged	Untagged	Untagged	Untagged	Untagged	Untagged
QoS:CoS/DSCP Setting DSCP Marking	25	Guest Voice	Disabled Disabled	Disabled Disabled	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged	Tagged Tagged
802.1X Configuration Firewall	Add Edit	Delete								
▶ VPN										_
Certificate Management	Save	Cancel								
 SSL VPN 										
User Management										
Wizard										
© 2013 Cisco Systems, Inc. All Rig	◀ ghts Reserved.). F

Schritt 3: Klicken Sie im Abschnitt *VLAN Table (VLAN-Tabelle)* auf **Add (Hinzufügen**), um eine neue VLAN-ID zu erstellen.

CISCO DV/225 Ci	achit Ducl M						cisco	English 🔻		
Gotting Started	gabit Dual v	AN VPN Router								
Svetem Summany	VLAN Memb	ership								
Setup										
> DHCP	VLAN: 🗹 Enab	le								
 System Management 	Create VLANs ar	nd assign the Outgoing Frame	Type.							
Port Management	Up to fourteen ne	ew VLANs can be created. VLA	N IDs must be in the r	ange (44094)						
Port Setup	VLAN Table									
Port Status	VI AN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LA
Traffic Statistics		Default	Disabled	Enabled	Untagged	Lintagged	Lintagged	Untagged	Untagged	Un
VLAN Membership	9 25	Quest	Disabled	Disabled	Toggod	Taggod	Toggod	Toggod	Toggod	To
DSCP Marking	20	Guesi	Disabled	Disabled	Taggeu	Tagged	Tagged	Tagged	Tagged	Ta
802.1X Configuration	100	voice	Disabled	Disabled	lagged	lagged	ragged	Tagged	Tagged	Taç
Firewall			Disabled V	Enabled V	Tagged V	Tagged V	Tagged V	Tagged	 Tagged 	▼ Ta
VPN	Add Edit	Delete								
 Certificate Management 										
▶ Log										
SSL VPN	Save	Cancel								
User Management										
Wizard										
	4							_	_	•
© 2013 Cisco Systems, Inc. All Rig	ghts Reserved.									

Schritt 4: Geben Sie im Feld für die *VLAN-ID* eine VLAN-Nummer ein. Die VLAN-IDs müssen zwischen 4 und 4094 liegen. In diesem Beispiel wird 200 als VLAN-ID für Daten verwendet. Geben Sie als Nächstes eine Beschreibung für das VLAN in das Feld *Description (Beschreibung)* ein. Als Beispiel für die Beschreibung werden Daten eingegeben. Klicken Sie dann auf **Speichern**.

Hinweis: VLAN 100 für Sprache wurde standardmäßig auf diesem Router erstellt. Es können bis zu vierzehn neue VLANs erstellt werden.

cisco RV325 Gi	igabit Dual WAN VPN Router					cisco	English 🔻		
Getting Started System Summary	VLAN Membership								
Setup DHCP System Management Port Management	VLAN: Z Enable Create VLANs and assign the Outgoing Frame Up to fourteen new VLANs can be created. VL	: Type. AN IDs must be in the ra	inge (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	Та
DSCP Marking	🗌 100 Voice ₍₂₎	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged	Tagged	Та
802.1X Configuration	1 (200) (Data	Disabled V	Enabled V	Tagged V	Tagged 🔻	Tagged V	Tagged 🔻	Tagged	▼ Ta
Firewall	Add Edit Delete								
Certificate Management									
▶ Log									
SSL VPN	3 Save Cancel								
User Management									
Wizard									
	4								Þ

Schritt 5: Um ein VLAN zu bearbeiten, aktivieren Sie das Kontrollkästchen des entsprechenden VLAN. In diesem Beispiel werden VLAN 1, 100 und 200 bearbeitet. Klicken Sie anschließend auf **Edit** (Bearbeiten), um die VLANs zu bearbeiten.



Schritt 6: Wählen Sie optional in der Dropdown-Liste "*Inter VLAN Routing*" die Option **Enabled** (**Aktiviert**) oder **Disabled** (**Deaktiviert**) **aus**, um Pakete von einem VLAN zu einem anderen VLAN weiterzuleiten. Die Aktivierung dieser Funktion ist nützlich, da interne Netzwerkadministratoren von einem entfernten Standort aus auf Ihre Geräte zugreifen können, um Probleme zu beheben. Dadurch wird die Zeit reduziert, die erforderlich ist, um ständig VLANs wechseln zu müssen, um auf die Geräte zuzugreifen.

- Disabled (Deaktiviert): Das bedeutet, dass Inter-VLAN-Routing inaktiv ist.
- Enabled (Aktiviert): Stellt dar, dass VLAN-übergreifendes Routing in diesem VLAN aktiv ist. Beim VLAN-übergreifenden Routing werden die Pakete nur an die VLANs weitergeleitet, in denen sie aktiviert sind.

Hinweis: In diesem Beispiel wird Inter-VLAN-Routing für die VLAN-ID 1, 100 und 200 aktiviert.

cisco RV325 Gi	gabit Dual V	VAN VPN Router					cisco	English v	Log Out Abou	it Help
Getting Started System Summary	VLAN Memb	pership								
Setup DHCP System Management Port Management	VLAN: VLANs a Create VLANs a Up to fourteen r	ble and assign the Outgoing Frame new VLANs can be created. VL/	Type. AN IDs must be in the ra	ange (44094)						
Port Setup Port Status	VLAN Table VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4	LAN5	LA
VLAN Membership QoS:CoS/DSCP Setting	1 25	Default Guest	Enabled Disabled	Enabled Disabled	Untagged v Tagged	Untagged T agged	Untagged v Tagged	Untagged Tagged	Untagged Tagged	▼ U Tag
DSCP Marking 802.1X Configuration	100 200	Voice Data	Enabled V Enabled V	Disabled Enabled	Tagged ▼ Tagged ▼	Tagged ▼ Tagged ▼	Tagged ▼ Tagged ▼	Tagged Tagged	Tagged Tagged	▼ Ta ▼ Ta
Firewall VPN Contificate Management	Add Edit	Delete								
Certificate Management Log SSL VPN Licer Management	Save	Cancel								
Wizard										
© 2013 Cisco Systems, Inc. All Rig	∢ ghts Reserved.									×

Schritt 7. Wählen Sie die gewünschte Option aus der Dropdown-Liste für den LAN-Port aus, mit dem Sie verbunden sind, und die Einstellung muss mit dem verbundenen Port übereinstimmen. Wenn Sie mit mehr als einem Port verbunden sind, müssen Sie für jeden Port, den Sie verbinden, dieselben Einstellungen wählen. Der Standardwert ist tagged, für VLAN 1 jedoch untagged.

Hinweis: Wenn Sie in Schritt 6 Inter-VLAN-Routing aktivieren, müssen Sie das VLAN mit Tags versehen, um den Datenverkehr zu unterscheiden.

Markiert

- Stellt dar, dass die Zuordnung zwischen dem Port und dem VLAN als markiert ist.
- Tagged wird verwendet, um zu bestimmen, zu welchem VLAN der Datenverkehr über die eindeutige VLAN-ID gehört, wenn mehrere VLANs für denselben Port erstellt werden.

Nicht markiert

- Stellt dar, dass die Zuordnung zwischen dem Port und dem VLAN nicht markiert ist.
- Sie wird verwendet, wenn nur ein VLAN erstellt wird und der Datenverkehr das VLAN erkennt. Nur ein VLAN kann für jeden LAN-Port als nicht markiert werden.
- Wenn sich das Standard-VLAN auf dem Port befindet, sollte die Markierung immer aufgehoben werden, auch wenn der Port über mehrere VLANs verfügt.

Ausgeschlossen

- Stellt dar, dass die Schnittstelle kein Mitglied des VLAN ist.
- Wenn Sie diese Option auswählen, wird der Datenverkehr zwischen dem VLAN und dem Port deaktiviert.

cisco RV325 Gi	gabit Dual V	/AN VPN Router					cisco	English 🔻	Log Out Abou	it Help
Getting Started System Summary > Setup > DHCP	VLAN Memb	ership le nd assign the Outgoing Frame ⁻	Type.							-
System Management Port Management Det Seture	Up to fourteen ne	ew VLANs can be created. VLA	N IDs must be in the r	ange (44094)						_
Port Status Traffic Statistics VLAN Membership	VLAN ID	Description Default	Inter VLAN Routing	Device Management Enabled	LAN1 Untagged	LAN2 Untagged V	LAN3 Untagged V	LAN4 Untagged	LAN5 Untagged	LA T U
QoS:CoS/DSCP Setting DSCP Marking 802.1X Configuration	25 100 200	Guest Voice Data	Enabled Enabled Enabled	Disabled Disabled Enabled	Tagged Tagged Tagged	Tagged Tagged Tagged	Tagged Tagged Tagged Tagged	Tagged Tagged Tagged	Tagged Tagged Tagged	Ta(▼ Ta ▼ Ta
Firewall VPN Certificate Management	Add Edit	Delete								
Log SSL VPN	Save	Cancel								
Wizard										
© 2013 Cisco Systems, Inc. All Rig	Interpretender In									Þ

Schritt 8: Klicken Sie auf Speichern, um die Einstellungen zu speichern.

Hinweis: Sie können sich auf dem Router beim webbasierten Dienstprogramm anmelden und zu **DHCP > DHCP Setup** navigieren, um die VLANs für ein bestimmtes Subnetz zu konfigurieren. Standardmäßig sind die VLANs in einem anderen Subnetz konfiguriert.

Konfigurieren von SPA-/MPP-Telefonen

Benutzer können die Telefone auch so konfigurieren, dass sie ein Profil von einem manuell konfigurierten Profilstandort, einem über die DHCP-Option 150 gefundenen Standort, oder von einem Cisco EDOS-Server abrufen. Nachfolgend finden Sie ein Beispiel für eine manuelle Konfiguration.

Schritt 1: Geben Sie die IP-Adresse des SPA/MPP in Ihren Browser ein, und navigieren Sie zu Admin Login (Admin-Anmeldung) und dann zu Advanced (Erweitert).

Hinweis: Die Konfiguration für das SPA-/MPP-Telefon kann je nach Modell variieren. In diesem Beispiel wird das SPA502G verwendet. Um die IP-Adresse Ihres IP-Telefons zu finden, navigieren Sie zu **DHCP > DHCP Status (DHCP-Status** auf Ihrem Router) (kann je nach Modell variieren). Eine weitere Möglichkeit besteht darin, die **Setup-**Taste zu drücken und auf Ihrem Cisco Telefon zu **Network (Netzwerk)** zu navigieren (Menüs und Optionen können je nach Telefonmodell variieren).

<u>"Network</u>	Ŧ
1 WANConnection Type	23
DHCP	5
2 Current IP	-
192.168.1.115	
save edit (cano	cel Ì

cisco SPA502G	s Pro 6 Configuration	Jtility					(Admin Login) basic advanced)
Voice	Call History	Personal Direc	tory Attendant	Console Status			
Info Sy	/stem 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							
Filolie Status	Current Time:	12/18/2017 06:52:56			Flansed Time:	00:00:07	
	Broadcast Pkts Sent:	9			Broadcast Bytes Sent:	2014	
	Broadcast Pkts Recv:	6			Broadcast Bytes Recv:	360	•
			Undo All Changes	Submit All Changes			
© 2009 Cisco Systems, Inc. All	Rights Reserved.			the state			SPA502G IP Phone

Schritt 2: Navigieren Sie zu Voice > Ext 1, die Durchwahlseite wird geöffnet.

cisco SPA50	ness Pro 2G Configuration l	Utility					<u>Jser Login</u> <u>basic</u> advanced
Voice	Call History	Personal Dire	ectory Attenda	nt Console Status			
Info	System SIP	Provisioning	Regional	Phone User	Attendant Console		
Ext 1							
General							^
	Line Enable:	yes 🔻					
Share Line Appearance	•						
	Share Ext:	private 🔻			Shared User ID:		
	Subscription Expires:	3600					
NAT Settings							
	NAT Mapping Enable:	no 🔻			NAT Keep Alive Enable:	no 🔻	
	NAT Keep Alive Msg:	\$NOTIFY			NAT Keep Alive Dest:	\$PROXY	
Network Settings							
	SIP TOS/DiffServ Value:	0x68			SIP CoS Value:	3 🔻	
	RTP TOS/DiffServ Value:	0xb8			RTP CoS Value:	6 🔻	
	Network Jitter Level:	high 🔻			Jitter Buffer Adjustment:	up and down 🔻	
SIP Settings							•
			Undo All Changes	Submit All Changes			
© 2009 Cisco Systems, Inc	c. All Rights Reserved.						SPA502G IP Phone

Schritt 3: Geben Sie im Abschnitt *Proxy and Registration (Proxy und Registrierung)* den Proxyserver in das Feld *Proxy (Proxy) ein.* In diesem Beispiel wird die Adresse des Raspberry Pi (192.168.3.10) als Proxyserver verwendet. VLAN 100 befindet sich im Subnetz mit 192.168.3.x.

Hinweis: Sie konfigurieren die IP-Adresse des Himbeer-Pi später in diesem Artikel, wenn Sie mehr erfahren möchten, klicken Sie auf den Link zu diesem Abschnitt umgeleitet werden: <u>Ändern der Adresse des Himbeer-Pi auf ein anderes Subnetz</u>.

cisco SPA50	siness Pro D2G Configuration L	Jtility						<u>User Login</u>	basic advanced
Voice	Call History	Personal Direct	ory Attendan	t Console Status					
Info	System SIP	Provisioning	Regional	Phone	User Attendant C	onsole			
Ext 1									
	CFWD Notifier:								^
Proxy and Registratio	'n								
	Proxy:	(192.168.3.10)		Use	Outbound Proxy:	no 🔻		
	Outbound Proxy:				Use O	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 Rec	lundancy Method:	Normal	•	_
Subscriber Informatio	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, Ir	nc. All Rights Reserved.								SPA502G IP Phone

Schritt 4: Geben Sie unter *Subscriber Information (Teilnehmerinformationen)* den Anzeigenamen und die Benutzer-ID (Durchwahlnummer) für die freigegebene Durchwahlnummer ein. In diesem Beispiel wird die Durchwahl 1003 verwendet.

Hinweis: Die Durchwahl 1003 wurde bereits auf dem Raspberry Pi erstellt und konfiguriert.

cisco SPA502G Configuration	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.	2000 Arts Gall Without Reg.	
Use DNS SRV:	no 🔻 DNS SRV Auto Prefix:	no 🔻
Proxy Fallback Intvi:	3600 Proxy Redundancy Method:	Normal
Subscriber Information		
Display Name:	(1003 User ID: (1003
Password:	Use Auth ID:	no 🔻
Auth ID:		
Mini Certificate:		
SRTP Private Key:		
Audio Configuration		
Preferred Codec:	G711u Vuse Pref Codec Only:	no 🔻
Second Preferred Codec:	Unspecified Third Preferred Codec:	Unspecified 🔻
G729a Enable:	yes 🔻 G722 Enable:	yes 🔻
G726-16 Enable:	yes T G726-24 Enable:	yes T
G726-32 Enable:	yes 🔻 G726-40 Enable:	yes 🔻
	Undo All Changes Submit All Changes	
© 2009 Cisco Systems, Inc. All Rights Reserved.		SPA502G IP Phone

Schritt 5: Geben Sie das Passwort der Erweiterung ein, die Sie im Raspberry Pi-Erweiterungsabschnitt konfiguriert haben. Dies ist auch als *Geheim* unter dem *Edit Extension* Abschnitt in der Himbeer Pi. In diesem Beispiel wurde das Kennwort **12345** verwendet.

Hinweis: Das Kennwort **12345** wurde nur als Beispiel verwendet. Ein komplexeres Kennwort wird empfohlen.

cisco SPA502G Configuration	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		
rtegister Expires.	3000 Arts Gall Without Reg.	110
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:	no 🔻
Auth ID:		
Mini Certificate:		
SRTP Private Key:		
Audio Configuration		
Preferred Codec:	G711u Vuse Pref Codec Only:	no 🔻
Second Preferred Codec:	Unspecified Third Preferred Codec:	Unspecified V
G729a Enable:	yes V 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

Schritt 6: Wählen Sie die gewünschte Option aus der Dropdown-Liste *Auth-ID verwenden*. Die Optionen lauten **Ja** und **Nein**. Um die SIP-Authentifizierung (Session Initiation Protocol) zu aktivieren, bei der SIP-Nachrichten angefordert werden können, um zu bestimmen, ob sie autorisiert sind, bevor sie übertragen können, wählen Sie **Ja** aus der *Auth ID*-Dropdown-Liste aus. In diesem Beispiel haben wir **Ja** gewählt.

cisco SPA5020	ss Pro G Configuration l	Jtility			<u>User Login</u> <u>basic</u> advanced
Voice	Call History	Personal Directory	Attendant Console Status		
Info	System SIP	Provisioning Regional	Phone User	Attendant Console	
Ext 1					
	rtegister Expires.	3000		Alls Gall Without Key.	
	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 🔻		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, Inc. A	All Rights Reserved.				SPA502G IP Phone

Schritt 7. Geben Sie die Durchwahl, die Sie für dieses Telefon konfigurieren möchten, in das Feld *Auth ID (Auth-ID)* ein. Die Authentifizierungs-ID ist für die SIP-Authentifizierung vorgesehen.

cisco SPA50	^{iness Pro} 12G Configuration l	tility	User Login basic advanced
Voice	Call History	Personal Directory Attendant Console Status	
Info	System SIP	Provisioning Regional Phone User Attendant Console	
Ext 1			
	r regiorei .		
	Register Expires:	3600 Ans Call Without Reg: no 🔻	
	Use DNS SRV:	no 🔻 DNS SRV Auto Prefix: no 🔻	
	Proxy Fallback Intvl:	3600 Proxy Redundancy Method: Normal	v
Subscriber Information	n		
	Display Name:	1003 User ID: 1003	
	Password:	12345 Use Auth ID: yes 🔻	
	Auth ID:	1003	
	Mini Certificate:		
	SRTP Private Key:		
Audio Configuration			
	Preferred Codec:	G711u ▼ Use Pref Codec Only: no ▼	
	Second Preferred Codec:	Unspecified Third Preferred Codec: Unspecified	·
	G729a Enable:	yes T G722 Enable: yes T	
	G726-16 Enable:	yes ▼ G726-24 Enable: yes ▼	
		Undo All Changes Submit All Changes	
© 2009 Cisco Systems, In	c. All Rights Reserved.		SPA502G IP Phone

Schritt 8: Klicken Sie dann auf Alle Änderungen übernehmen.

Hinweis: Gehen Sie zurück zu Schritt 1 im Abschnitt Konfigurieren von SPA/MPP-Telefonen, wenn Sie mehr SPA/MPP-Telefone konfigurieren müssen.

Konfigurieren von VLANs auf dem Switch

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und navigieren Sie zu VLAN Management > Create VLAN.

Hinweis: Die Konfiguration kann je nach Gerät variieren. In diesem Beispiel wird der SF220-24P zum Konfigurieren von VLANs verwendet.



Schritt 2: Klicken Sie auf Hinzufügen... um ein neues VLAN zu erstellen.



Schritt 3: Um ein einzelnes VLAN zu erstellen, wählen Sie das Optionsfeld **VLAN** aus. Geben Sie die **VLAN-ID** und den **VLAN-Namen ein**. Klicken Sie anschließend auf **Apply**, um das VLAN zu speichern. In diesem Beispiel erstellen wir VLAN 100 für Sprache und 200 für Daten.

Hinweis: Einige VLANs werden vom System für die interne Systemnutzung benötigt und können daher nicht durch Eingabe der Start-VID und End-VID erstellt werden. Wenn Sie die **Range**-Funktion verwenden, können Sie maximal 100 VLANs gleichzeitig erstellen.

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

Hinweis: Wiederholen Sie Schritt 2, wenn Sie ein weiteres einzelnes VLAN erstellen müssen.

Einrichten des Sprach-VLANs auf dem Switch

Schritt 1: Melden Sie sich bei der Webkonfiguration an, und navigieren Sie zu VLAN Management > Voice VLAN > Properties.

Hinweis: Bei der Konfiguration des Auto Voice VLAN werden automatisch QoS-Einstellungen für das Sprach-VLAN angewendet, und der Sprachverkehr wird priorisiert.

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

Schritt 2: Geben Sie unter Administrative Status (Verwaltungsstatus) im Feld Voice VLAN ID (Sprach-VLAN-ID) das VLAN ein, das das Sprach-VLAN sein soll. In diesem Beispiel wird VLAN 100 als Sprach-VLAN eingegeben.

Hinweis: Änderungen an der Sprach-VLAN-ID, der Class of Service (CoS)/802.1p und/oder dem Differentiated Service Code Point (DSCP) veranlassen das Gerät, das administrative Sprach-VLAN als statisches Sprach-VLAN anzukündigen. Wenn die Option "*Auto Voice VLAN Activation*" (Durch

externes Sprach-VLAN ausgelöste *automatische Sprach-VLAN-Aktivierung*) ausgewählt ist, müssen die Standardwerte beibehalten werden. In diesem Beispiel wird CoS/802.1p als Standardwert von 5 und DSCP als Standardwert von 46 belassen.

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:
Default VLAN Settings Create VLAN	Administrative Status: Operational Status:
Port to VLAN	Voice VLAN ID: (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: Category Control
MAC Address Tables Multicast	Disable
IP Configuration	Anniv Cancel
Security	
 Access Control 	
 Quality of Service 	
▶ SNMP	
© 2014-2017 Cisco Systems, Inc. Al	Rights Reserved.

Schritt 3: Klicken Sie auf Apply, um Ihre Einstellungen zu speichern.

Small Business CISCO SF220-24P	24-Port 10/100 PoE Smart Switch							
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	O Voice VLAN ID: 100 (Range: 1 - 4094, Default: 1) Voice VLAN ID: 1							
Port VLAN Membership GVRP Settings	CoS/802.1p: 5 V (Default: 5) CoS/802.1p: 5							
Voice VLAN Properties	DSCP: 46 V (Default: 46) DSCP: 46							
Telephony OUI Telephony OUI Interface	Dynamic Voice VLAN Settings:							
Spanning Tree MAC Address Tables	Dynamic Voice VLAN: Enable Auto Voice VLAN Enable Telephony OUI							
 Multicast 	O Disable							
 IP Configuration 	Cancel							
Security								
Quality of Service								
SNMP								
© 2014-2017 Cisco Systems, Inc. A	NI Rights Reserved.							

Konfigurieren der Schnittstelleneinstellungen des Switches

Die Schnittstellen, die physischen Ports am Switch, können einer der folgenden Einstellungen zugewiesen werden:

- Allgemein: Der Port kann alle Funktionen unterstützen, die in der IEEE 802.1q-Spezifikation definiert sind. Bei der Schnittstelle kann es sich um ein getaggtes oder nicht getaggtes Mitglied eines oder mehrerer VLANs handeln.
- Zugriff: Auf der Schnittstelle kann nur ein VLAN konfiguriert sein, und es kann nur ein VLAN übertragen werden.
- Trunk: Kann den Datenverkehr mehrerer VLANs über eine einzige Verbindung übertragen und ermöglicht die Erweiterung von VLANs über das Netzwerk.
- Dot1p-Tunnel: versetzt die Schnittstelle in den QinQ-Modus. So kann der Benutzer seine eigenen VLAN-Anordnungen (PVID) im Anbieternetzwerk verwenden. Der Switch befindet sich im QinQ-Modus, wenn er über einen oder mehrere dot1p-tunnel-Ports verfügt.

Schritt 1: Melden Sie sich bei der Webkonfiguration an, und navigieren Sie zu VLAN Management > Interface Settings.

Small Business cisco SF220-24P	24-	Port 10	/100 P	oE Smart Swi	tch				cisco Langu	^{lage:} English		• •			Help
Getting Started Status and Statistics	Inte	erface Se	ettings												^
 Administration 	Int	erface Settin	igs Table							SI	nowing 1-26 of	26 All	▼ per p	age	
 Port Management 	Filt	er: Interface	Type equal	s to Port V Go	1										
✓ VLAN Management			i jpe equa												
Default VLAN Settings		Entry No.	Interface	Interface VLAN Mode	Administrative PVID	Frame Type	Ingress Filtering	Uplink							
Create VLAN		1	FE1	Trunk	1	Admit All	Enabled	Disabled							
Port to VLAN		2	FE2	Trunk	1	Admit All	Enabled	Disabled							
Port VLAN Membership		3	FE3	Trunk	1	Admit All	Enabled	Disabled							
GVRP Settings		4	FE4	Trunk	1	Admit All	Enabled	Disabled							
 Voice VLAN 		5	FE5	Trunk	1	Admit All	Enabled	Disabled							
Properties		6	FE6	Trunk	1	Admit All	Enabled	Disabled							
Telephony OUI		7	FE7	Trunk	1	Admit All	Enabled	Disabled							
Spanning Tree		8	FE8	Trunk	1	Admit All	Enabled	Disabled							
MAC Address Tables		9	FE9	Trunk	1	Admit All	Enabled	Disabled							
Multicast		10	FE10	Trunk	1	Admit All	Enabled	Disabled							
IP Configuration		11	FE11	Trunk	1	Admit All	Enabled	Disabled							
▶ Security		12	FE12	Trunk	1	Admit All	Enabled	Disabled							
Access Control		13	FE13	Trunk	1	Admit All	Enabled	Disabled							
Quality of Service		14	FE14	Trunk	1	Admit All	Enabled	Disabled							
▶ SNMP		15	FE15	Trunk	1	Admit All	Enabled	Disabled							
		16	FE16	Trunk	1	Admit All	Enabled	Disabled							
		17	FE17	Trunk	1	Admit All	Enabled	Disabled							
		18	FE18	Trunk	1	Admit All	Enabled	Disabled							-
© 2014-2017 Cisco Systems, Inc. A	II Right	s Reserved.													

Schritt 2: Wählen Sie den Schnittstellenmodus für das VLAN aus. In diesem Beispiel wird der Raspberry Pi (Port: FE3) als Access-Port konfiguriert.

Small Business CISCO SF220-24P	24-1	Port 10	/100 P	oE Smart Swi	tch			-	cisco Language: English 🗸 Logout About H	lelp
Getting Started	Inte	erface Se	ttings							^
 Status and Statistics 			Juligo							
 Administration 	Inte	erface Settin	igs Table						Showing 1-26 of 26 All 🔻 per page	
 Port Management 	Filt	er: Interface	Type equal	s to Port 🔻 Go						
 VLAN Management 		Entry No.	Interface	Interface VI AN Mode	Administrative DV/ID	Frame Tune	Ingroop Filtering	Liplink		
Default VLAN Settings		Entry NO.	Therade	Truck	Administrative P VID	Admit All	Eachied	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		
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		
		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	Rights	Reserved								

Schritt 3: Klicken Sie dann auf Bearbeiten... um die Schnittstelle zu bearbeiten.

Small Business CISCO SF220-24P	24-Po	ort 10	/100	PoE Smart Sv	vitch						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	EE 10	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	FE15	Trunk		1	Admit All	Enabled	Disabled					
GVRP Settings		16	EE 16	Trunk		1	Admit All	Enabled	Disabled					
Voice VLAN		17	FE 17	Trunk		1	Admit All	Enabled	Disabled					
 Spanning Tree 		17	FE 17	Trunk		1	Admit All	Enabled	Disabled					
 MAC Address Tables 		18	FEIG	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 Settings Edit														
© 2014-2017 Cisco Systems, Inc. A	© 2014-2017 Cisco Systems, Inc. All Rights Reserved.													

Schritt 4: Wählen Sie im Feld *Interface VLAN Mode (Schnittstellen-VLAN-Modus)* Access (Zugriff) aus, um die Schnittstelle als nicht markiertes Mitglied eines einzelnen VLANs zu konfigurieren.

🗋 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 I	Dot1q-Tu	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			•

Schritt 5: Klicken Sie auf Apply, um Ihre Einstellungen zu speichern.

🗋 Edit Interface Settings - 0	🖹 Edit Interface Settings - Google Chrome – 🛛 🗙							
A Not secure https://	192.168.1.100/html/vlan_intfEdit.html?port=FE3							
Interface:	Port FE3 LAG I							
Interface VLAN Mode:	 General Access Trunk Dot1q-Tunnel (The switch will be in Q-in-Q mode when it has one 	e or more	Dot1q-Tu	nnel 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				•				

Konfigurieren der Port-VLAN-Zugehörigkeit auf dem Switch

Nachdem die VLANs erstellt wurden, müssen Sie den Ports, die Sie anschließen möchten, VLANs zuweisen.

Schritt 1: Melden Sie sich bei der Webkonfiguration an, und navigieren Sie zu VLAN Management > Port VLAN Membership.

Small Business	2 24 Port 10/100 PoE Smart Switch	Save cisco Language: English 🔹 Logout About Help
Getting Started Status and Statistics Administration	Port VLAN Membership F - Forbidden member T - Tagged member U - Untagged member P - PVID G - Gues	t VLAN
Port Management	Port VLAN Membership Table	Showing 1-26 of 26 All ▼ per page
VLAN Management	Filter: Interface Type equals to Port V Go	
Default VLAN Settings Create VLAN	Interface Mode Administrative VLANs Operational VLANs LAG	
Interface Settings	FE1 Trunk 1UP 1UP, 100T	
Port to VLAN	FE2 Trunk 1UP 1UP, 100T	
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	
© 2014 2017 Circo Systems Inc. A	All Rights Researed	
© 2014-2017 CISco Systems, Inc. A	All Rights Reserved.	

Schritt 2: Wählen Sie in der *Tabelle "Port VLAN Membership*" die Schnittstelle aus, die Sie für die VLAN-Mitgliedschaft konfigurieren möchten. In diesem Beispiel wird der Raspberry Pi (Port: FE3) für VLAN 100 konfiguriert.

Hinweis: Alle Sprachgeräte werden bereits für das Sprach-VLAN konfiguriert, das Sie im Abschnitt <u>Einrichten von Sprach-VLAN auf dem Switch</u> ausgewählt haben.

Small Business SF220-24P	24-I	Port 10)/100	PoE Smart Sv	vitch				Language: En	glish 🔻			Help
Getting Started Status and Statistics Administration	Por F - F	t VLAN orbidden me	Membe	ership T - Tagged member	U - Untagged memb	er P - PVID	G - Guest VLAN						*
 Port Management 	Poi	t VLAN Me	mbership	Table						Showing 1-26 of 26	All 🔻	per page	
✓ VLAN Management	E itte	ar: Interfac	Tune equ	ale to Port V Go				_		-			
Default VLAN Settings	1 110	51. <i>Internato</i>	e iype equ			10							4
Create VLAN		Interface	Mode	Administrative VLANS	Operational VLANS L	AG							4
Port to VLAN		FE1	Trunk	10P	10P, 1001								
Port VLAN Membership		FE2	Trunk	10P	10P, 1001								
GVRP Settings	\mathbf{O}	FE3	Access	10P	10P								4
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. All	Rights	Reserved.											

Schritt 3: Klicken Sie auf **Join VLAN...** um den Port zu ändern, den Sie VLANs konfigurieren möchten.

Small Business CISCO SF220-24P	24-	Port 1(0/100 Pc	E Smart Sw	itch			sco Language: English	 Logout 	Help
Getting Started		EEO	Truple	1110	1110					-
Status and Statistics		FEO	Trunk	TUP	IUP					
Administration		FE9	Trunk	TUP	TUP					
Port Management		FE10	Trunk	10P	10P					
✓ VLAN Management		FE11	Trunk	10P	10P					
Default VLAN Settings		FE12	Trunk	1UP	1UP					
Create VLAN		FE13	Trunk	1UP	1UP					
Interface Settings		FE14	Trunk	1UP	1UP					
Port to VLAN		FE15	Trunk	1UP	1UP					
Port VLAN Membership		FE16	Trunk	1UP	1UP					
GVRP Settings		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	Ĭ	FE24	Trunk	1UP	1UP					
SNMP		GE1	Trunk	1UP	1UP					
		GE2	Trunk	111P	111P					
	Ē				101					
	J	oin VLAN	Details							
	F - F	orbidden m	ember 1	- Tagged member	U - Untagged member	P - PVID	G - Guest VLAN			-
© 2014-2017 Cisco Systems, Inc. Al	ll Right	s Reserved.								

Schritt 4: Wählen Sie **1UP aus**, und klicken Sie auf den Befehl <, um VLAN 1 aus der Schnittstelle im Abschnitt *Select VLAN (VLAN auswählen) zu entfernen*. Nur ein nicht markiertes VLAN kann der Schnittstelle hinzugefügt werden, wenn es sich um einen Zugriffsport handelt.



Schritt 5: Wählen Sie **100 aus**, und klicken Sie auf >, um der Schnittstelle das nicht gekennzeichnete VLAN hinzuzufügen.

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:		
100 200 1 •		
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN		
Tagging: Forbidden Excluded Tagged Untagged		
PVID		
Apply Close		

Schritt 6: Klicken Sie auf Apply, um Ihre Einstellungen zu speichern.

🗋 Join VLAN - Google Chrome		×
A Not secure https://192.168.1.100/html/vlan_portMembershipEdit.html?port=FE3		
Interface: Port FE3 LAG		
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		

Schritt 7. Wählen Sie im Feld Interface (*Schnittstelle*) den Schnittstellenport aus, der mit dem Router verbunden ist. In diesem Beispiel ist Port GE1 ausgewählt.

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

Schritt 8: Wählen Sie das VLAN aus, das der ausgewählten Schnittstelle hinzugefügt werden soll, und klicken Sie dann im Abschnitt *Select VLAN (VLAN auswählen) auf* >, um das VLAN hinzuzufügen. In diesem Beispiel werden VLAN **100** und **200** ausgewählt.

🕒 Join VLAN - Google 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 GE1 LAG 1	
Mode: Trunk	
Select VLAN:	
F - Forbidden member, T - Tagged member, U - Untagged member, P - PVID, G - Guest VLAN	
Tagging: Forbidden Excluded Tagged Untagged PVID	
Apply Close	

Schritt 9. Klicken Sie auf Apply, um Ihre Einstellungen zu speichern.

Hinweis: Möglicherweise ist ein Neustart der IP-Telefone erforderlich, damit die IP-Adresse in das richtige Subnetz geändert wird.

Änderung der IP-Adresse von Raspberry Pi in einem anderen Subnetz

Schritt 1: Verbinden Sie Ihren Raspberry Pi mit Secure Shell (SSH) oder schließen Sie Ihren Raspberry Pi an einen Computermonitor an. In diesem Beispiel wird SSH verwendet, um den Raspberry Pi zu konfigurieren.

Hinweis: Der Port am Switch für Ihren Computer/Laptop muss sich im selben VLAN wie der Raspberry Pi befinden und als Zugriffsport konfiguriert werden, wenn Sie die Schnittstelleneinstellungen einrichten. Siehe <u>Konfigurieren der Schnittstelleneinstellungen für einen</u> <u>Switch und Konfigurieren der Port-VLAN-Zugehörigkeit im</u> Abschnitt<u>Switch</u> in diesem Artikel, um die Details zu überprüfen. Stellen Sie sicher, dass Ihre IP-Adresse im gleichen Netzwerk wie Ihr Raspberry Pi ist, um SSH in sie zu integrieren. Wenn sich Ihr Gerät nicht im selben Netzwerk wie der Raspberry Pi befindet, verwenden Sie eine statische IP-Adresse und ändern Sie Ihre IP-Adresse manuell in das gleiche Netzwerk. Alternativ können Sie den Befehl **ipconfig/release** und **ipconfig/renew** in der Eingabeaufforderung eingeben, um eine neue IP-Adresse zu erhalten. SSH-Clients können je nach Betriebssystem variieren. In diesem Beispiel wurde PuTTY verwendet, um SSH in den Raspberry Pi einzufügen. Weitere Informationen zu SSH erhalten Sie <u>hier</u>.

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

Schritt 2: Geben Sie die IP-Adresse Ihres Raspberry Pi in das Feld *Hostname (oder IP-Adresse) ein.* In diesem Beispiel wird 192.168.1.10 eingegeben.

Hinweis: Sie können die DHCP-Tabelle im Router verwenden, um die Adresse des Raspberry Pi zu finden. In diesem Dokument wurde dieser Raspberry Pi so vorkonfiguriert, dass er eine statische IP-Adresse hat.

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

Schritt 3: Geben Sie **22** als Portnummer in das Feld *Port* ein. Port 22 ist der Standardport für das SSH-Protokoll.

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 session				
	Host Name (or IP address)	°ort 22			
	 ○ Raw ○ Telnet ○ Rlogin ● SSH Load, save or delete a stored session Saved Sessions 	⊖ Serial			
	Default Settings	Load Save Delete			
	Close window on exit: Always Never Only on clea	an exit			
About	Open	Cancel			

Schritt 4: Klicken Sie im Abschnitt *Verbindungstyp* auf das Optionsfeld **SSH**, um SSH als Methode für die Verbindung mit dem Switch auszuwählen. Klicken Sie dann auf **Öffnen**, um die Sitzung zu starten.

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

Schritt 5: Geben Sie den Benutzernamen und das Kennwort des RasPBX-Systems in das Feld Anmelden als und Kennwort ein.

Hinweis: Standardbenutzer: root und Standardkennwort: Himbeere

P 192.168.1.10 - PuTTY	_	\times
login as: root root@192.168.1.10's password: []		~ 3
		\sim

Schritt 6: Um die IP-Adresse Ihres Ethernet in eine statische IP-Adresse zu ändern, geben Sie ifconfig eth0 [IP-Adresse] netmask [Netzmaske] ein. In diesem Beispiel verwenden wir 192.168.3.10 und die Netzmaske 255.255.255.0.

ifconfig eth0 192.168.3.10 netmask 255.255.255.0

Hinweis: Wenn Sie die IP-Adresse ändern, wird die Verbindung zur Sitzung getrennt. Um sich wieder mit dem Raspberry Pi zu verbinden, muss sich Ihr Computer/Laptop im gleichen Subnetz wie der Raspberry Pi befinden (192.168.3.x).

🛃 192.168.3.10 - PuTTY		_		Х	
Linux raspbx 4.9.59	-v7+ #1047 SMP Sun Oct 29 12:19:23 GMT 2017 a	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 Debiar tware; the exact distribution terms for each dividual files in /usr/share/doc/*/copyright.	n GNU/Li program	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 latest	add-ons	and		
configure-timezone install-fax	Set timezone for both system and PHP Install HvlaFAX				
add-fax-extension install-fail2ban	Add additional fax extension for use with Hy Install Fail2Ban for additional security	ylaFAX			
install-dongle raspbx-backup	Install GSM/3G calling capability with chan Backup your complete system to an image file	_dongle			
Last login: Mon Dec	18 19:56:37 2017 from 192.168.1.151				
root@raspbx:~#(ifco	nfig eth0 192.168.3.10 netmask 255.255.255.0				\checkmark

Schritt 7. Stellen Sie mithilfe der statischen IP-Adresse, die in Schritt 6 konfiguriert wurde, eine Verbindung zu Ihrem Raspberry Pi her. In diesem Beispiel verwenden wir 192.168.3.10, um eine Verbindung herzustellen.

Hinweis: Stellen Sie sicher, dass sich Ihr Computer/Laptop im gleichen Subnetz wie der Raspberry Pi und das VLAN befindet. Wenn sich Ihr Computer/Laptop im selben VLAN wie der Raspberry Pi befindet und Sie nicht über die richtige IP-Adresse verfügen, können Sie zu Ihrer Eingabeaufforderung wechseln und **ipconfig /release** und dann **ipconfig /renew** eingeben, um eine neue IP-Adresse anzufordern, oder Sie können Ihr Gerät so konfigurieren, dass es eine statische IP-Adresse in den Ethernet-Eigenschaften hat.

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 ses Specify the destination you want to connect Host Name (or IP address) 192.168.3.10 Connection type: O Raw O Telnet O Rlogin • SSH	to Port 22 O Serial
	Load, save or delete a stored session Saved Sessions	Load Save Delete
	Close window on exit: Always Never Only on clean exit Open Cancel	

Schritt 8: Geben Sie in der Befehlszeile route add default gw [Router-IP-Adresse des Subnetzes] ein, um ein Standard-Gateway hinzuzufügen.

Hinweis: Sie können die Routing-Tabelle mithilfe der Befehlsroute anzeigen.

route add default gw 192.168.3.1



Schlussfolgerung

Sie sollten nun erfolgreich ein einfaches Sprachnetzwerk eingerichtet haben. Um dies zu überprüfen, nehmen Sie eines der SPA/MPP-Telefone, und Sie sollten einen Wählton hören. In diesem Dokument hat eines der SPA/MPP-Telefone die Durchwahl 1002 und das andere die Durchwahl 1003. Sie sollten in der Lage sein, die Durchwahl 1003 anzurufen, wenn Sie die SPA-/MPP-Durchwahl 1002 verwenden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.