Technische Details

Physische und Umgebungsspezifikationen

In der folgenden Tabelle werden die Gehäusespezifikationen und die Spezifikationen zur Betriebsumgebung für die Cisco IP-Telefon 8800-Serie aufgeführt.

Tabelle 1: Physische und Umgebungsspezifikationen

Spezifikation	Wert oder Bereich
Betriebstemperatur	0 °C bis 40 °C (32 °F bis 104 °F)
Relative Luftfeuchtigkeit beim Betrieb	In Betrieb: 10 % bis 90 % (nicht kondensierend) Außer Betrieb: 10 % bis 95 % (nicht kondensierend)
Lagertemperatur	-10 °C bis 60 °C (14 °F bis 140 °F)
Höhe	229,1 mm
Breite	257,34 mm

Spezifikation	Wert oder Bereich
Tiefe	40 mm
Gewicht	1,19 kg
Netzanschluss	100–240 VAC, 50–60 Hz, 0,5 A bei Verwendung des Netzteils 48 VDC, 0,2 A bei Inline-Stromversorgung über das Netzwerkkabel
Kabel	Kategorie 3/5/5e/6 für 10-Mbit/s-Kabel mit 4 Paaren Kategorie 5/5e/6 für 100-Mbit/s-Kabel mit 4 Paaren Kategorie 5e/6 für 1000-Mbit/s-Kabel mit vier Paaren **Hinweis** Kabel weisen vier Leiterpaare auf, sodass sich eine Summe von ach ergibt.
Entfernung	Entsprechend der Ethernet-Spezifikation sollte die Kabellänge zwischen einen IP-Telefon und dem Switch höchstens 100 m betragen.

Kabelspezifikationen

Im Folgenden sind die Kabelspezifikationen aufgeführt:

- RJ-9-Buchse (4 Leiter) für Hörer- und Headset-Port
- RJ-45-Buchse für den LAN 10/100/1000BaseT-Anschluss (10/100/1000-Netzwerk-Port am Telefon)
- RJ-45-Buchse für einen zweiten 10/100/1000BaseT-kompatiblen Anschluss (10/100/1000-Computer-Port am Telefon)
- 3,5-mm-Buchse für Lautsprecheranschluss (nur Cisco IP-Telefon 8861)
- 48-Volt-Netzanschluss
- USB-Ports/-Anschluss: Ein (Cisco IP-Telefon 8851) bzw. zwei USB-Ports (Cisco IP-Telefon 8861)
- 3 Erweiterungsmodulanschlüsse, die beim Cisco IP-Telefon 8851 und beim Cisco IP-Telefon 8861 als USB-Anschluss berücksichtigt werden

Pin-Belegungen für Netzwerk- und Computerports

Obwohl sowohl der Netzwerk- als auch der Computerport für die Netzwerkverbindung verwendet werden, dienen sie unterschiedlichen Zwecken und weisen unterschiedliche Pin-Belegungen auf.

- Der Netzwerkport ist der 10/100/1000 SW-Port auf dem Cisco IP-Telefon.
- Der Computerport ist der 10/100/1000 PC-Port auf dem Cisco IP-Telefon.

Netzwerkport-Stecker

In der folgenden Tabelle sind die Pin-Belegungen des Netzwerkport-Steckers aufgeführt.

Tabelle 2: Pin-Belegungen des Netzwerkport-Steckers

Pin-Nummer	Funktion
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Hinweis	BI steht für bidirektional und DA, DB, DC und DD geben Daten A, Daten B, Daten C und Daten D an.

Computerport-Stecker

In der folgenden Tabelle sind die Pin-Belegungen des Computerport-Steckers aufgeführt.

Tabelle 3: Pin-Belegungen des Computerport-Steckers

Pin-Nummer	Funktion
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Hinweis	BI steht für bidirektional und DA, DB, DC und DD geben Daten A, Daten B, Daten C und Daten D an.

Stromversorgung des Telefons

Cisco IP-Telefon kann über eine externe Stromversorgung oder mit „Power over Ethernet“ (PoE) betrieben werden. Ein separates Netzteil stellt die externe Stromversorgung sicher. Der Switch kann PoE über das Ethernet-Telefonkabel bereitstellen.

Cisco IP-Telefon 8861 und Cisco IP-Telefon 8865 sind Geräte der PoE-Klasse 4 und benötigen zur Unterstützung von Zusatzfunktionen einen Switch oder eine Leitungskarte, die Klasse 4 unterstützen.

Weitere Informationen zur Stromversorgung Ihres Telefons finden Sie im Datenblatt zu Ihrem Telefon.

Wenn Sie ein Telefon installieren, das über eine externe Stromquelle betrieben wird, schließen Sie die Stromversorgung an, bevor Sie das Ethernet-Kabel mit dem Telefon verbinden. Wenn Sie ein Telefon entfernen, das über eine externe Stromquelle betrieben wird, stecken Sie das Ethernet-Kabel vom Telefon aus, bevor Sie die Stromversorgung trennen.

Tabelle 4: Richtlinien für die Stromversorgung von Cisco IP-Telefonen

Art der Stromversorgung	Richtlinien
Externe Stromversorgung: Erfolgt über CP-PWR-CUBE-4= externe Stromversorgung	Cisco IP-Telefon verwendet zur Stromversorgung den CP-PWR-CUBE-4.
PoE-Energie: Wird von einem Switch über das Ethernet-Kabel am Telefon bereitgestellt.	Cisco IP-Telefons 8851, 8851NR, 8861, 8865 und 8865NR unterstützen 802.3at PoE Zubehör. Weitere Informationen finden Sie im Datenblatt zu Ihrem Telefon. Zur Sicherstellung des unterbrechungsfreien Betriebs des Telefons benötigt der Swit Backup-Stromversorgung Stellen Sie sicher, dass die CatOS- oder IOS-Version, die auf dem Switch ausgeführt beabsichtigte Telefonbereitstellung unterstützt. Informationen zur Betriebssystemversi Sie in der Dokumentation für den Switch.
Universal Power over Ethernet (UPoE)	Cisco IP-Telefon 8865 und 8865NR unterstützen UPoE.

Die Dokumente in der folgenden Tabelle enthalten weitere Informationen zu den folgenden Themen:

- Cisco Switches, die für den Einsatz mit Cisco IP-Telefonen geeignet sind
- Cisco IOS-Versionen, die eine bidirektionale Energieaushandlung unterstützen
- Weitere Anforderungen und Einschränkungen im Zusammenhang mit der Stromversorgung

Tabelle 5: Zusätzliche Informationen

Thema des Dokuments	URL
PoE-Lösungen	http://www.cisco.com/c/en/us/solutions/enterprise-networks/power-over-ethernet-solutions/index.html
UPoE	http://www.cisco.com/c/en/us/solutions/enterprise-networks/upoe
Cisco Catalyst-Switches	http://www.cisco.com/c/en/us/products/switches/index.html

Thema des Dokuments	URL
Integrierte Dienst-Router	http://www.cisco.com/c/en/us/products/routers/index.html
Cisco IOS Software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/inc

Stromausfall

Die Verfügbarkeit der Notfalldienste auf dem Telefon ist nur dann gewährleistet, wenn das Telefon mit Strom versorgt ist. Bei einem Stromausfall können Notrufnummern erst nach Wiederherstellung der Stromzufuhr gewählt werden. Bei einer Unterbrechung der Stromversorgung oder bei einem Stromausfall müssen Sie das Gerät möglicherweise zurücksetzen oder neu konfigurieren, um Notrufnummern wählen zu können.

Senkung des Stromverbrauchs

Mit dem Energiesparmodus oder EnergyWise-Modus (Power Save Plus) können Sie die Menge der Energie reduzieren, die Cisco IP-Telefon verbraucht.

Energiesparmodus

Im Energiesparmodus ist die Hintergrundbeleuchtung deaktiviert, wenn das Telefon nicht verwendet wird. Das Telefon verbleibt über die festgelegte Dauer im Energiesparmodus oder bis der Benutzer den Hörer abnimmt oder eine beliebige Taste drückt.

Power Save Plus (EnergyWise)

Cisco IP-Telefon unterstützt den Cisco EnergyWise-Modus (Power Save Plus). Wenn Ihr Netzwerk einen EnergyWise-Controller umfasst (beispielsweise einen Cisco Switch mit aktivierter EnergyWise-Funktion), können Sie diese Telefone so konfigurieren, dass sie basierend auf einem Zeitplan in und aus dem Energiesparmodus wechseln, um den Energieverbrauch weiter zu reduzieren.

Richten Sie die einzelnen Telefone so ein, dass die EnergyWise-Einstellungen aktiviert bzw. deaktiviert werden können. Wenn EnergyWise aktiviert ist, können Sie eine Aus- und Einschaltzeit und auch weitere Parameter konfigurieren. Diese Parameter werden als Teil der XML-Datei für die Telefonkonfiguration an das Telefon gesendet.

Energieaushandlung über LLDP

Zwischen Telefon und Switch erfolgt eine Energieaushandlung über den Stromverbrauch des Telefons. Für den Betrieb des Cisco IP-Telefon gibt es mehrere Stromeinstellungen, wodurch zum Beispiel der Stromverbrauch gesenkt wird, wenn weniger Strom zur Verfügung steht.

Nach dem Neustart eines Telefons führt der Switch mit einem Protokoll (CDP oder LLDP) die Energieaushandlung durch. Der Switch verbindet sich mit dem ersten Protokoll, das einen Schwellengrenzwert (TLV) enthält, der vom Telefon übertragen wird. Wenn der Systemadministrator das Protokoll auf dem Telefon deaktiviert, kann das Telefon keine Zubehörkomponenten einschalten, da der Switch nicht auf Stromanfragen im anderen Protokoll reagiert.

Cisco empfiehlt, bei Verbindungen zu einem Switch, der die Energieaushandlung unterstützt, die Energieaushandlungsfunktion immer aktiviert zu lassen (Standard).

Wenn die Energieaushandlung deaktiviert ist, trennt der Switch die Stromversorgung zum Telefon möglicherweise. Wenn der Switch die Energieaushandlung nicht unterstützt, deaktivieren Sie die

Energieaushandlungsfunktion, bevor Sie Zubehörkomponenten über PoE aktivieren. Wenn die Energieaushandlung deaktiviert ist, kann das Telefon die Zubehörkomponenten bis zum maximalen gemäß IEEE 802.3af-2003-Norm zugelassenen Wert mit Strom versorgen.

Hinweis

- Wenn CDP und Energieaushandlung deaktiviert sind, kann das Telefon die Zubehörkomponenten bis zu 15,4 W mit Strom versorgen.

Netzwerkprotokolle

Die Cisco IP-Telefon 8800-Serie unterstützt verschiedene eigene und Industriestandard-konforme Netzwerkprotokolle, die für die Sprachkommunikation benötigt werden. Die folgende Tabelle enthält eine Übersicht der von den Telefonen unterstützten Netzwerkprotokolle.

Tabelle 6: Von der Cisco IP-Telefon 8800-Serie unterstützte Netzwerkprotokolle

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Bluetooth	Bluetooth ist ein Kurzstrecken-Funkprotokoll (WPAN-Protokoll), das die Kommunikation zwischen Geräten über kurze Distanzen regelt.	Telefone des Typs Cisco IP-Telefon 8845, 8865 und 8851 unterstützen Bluetooth 4.1. Cisco IP-Telefon 8861 unterstützt Bluetooth 4.0. Cisco IP-Telefon 8811, 8841, 8851NR und 8865NR unterstützen kein Bluetooth.
Bootstrap Protocol (BootP)	Mit BootP kann ein Netzwerkgerät, beispielsweise Cisco IP-Telefon, bestimmte Startinformationen (z. B. die IP-Adresse) abfragen.	—
Cisco Audio Session Tunnel (CAST)	Mit dem CAST-Protokoll können Telefone und zugehörige Anwendungen Remote-IP-Telefone erkennen und mit diesen kommunizieren, ohne dass Änderungen an den herkömmlichen Komponenten zur Signalübertragung erforderlich sind.	Cisco IP-Telefon verwendet CAST als Schnittstelle zwischen CUVA und Cisco Unified Communications Manager mit Cisco IP-Telefon als SIP-Proxy.
Cisco Discovery Protocol (CDP)	CDP ist ein Protokoll für die Geräteerkennung, das auf allen Geräten von Cisco ausgeführt wird. Mithilfe von CDP kann sich ein Gerät innerhalb des Netzwerks für andere Geräte erkennbar machen und Informationen über andere Geräte empfangen.	Cisco IP-Telefons nutzen CDP für die Übertragung von Informationen, wie beispielsweise Zusatz-VLAN-ID, Energiemanagementdaten einzelner Ports oder Konfigurationsinformationen zur Quality of Service (QoS), an den Cisco Catalyst-Switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP ist ein Cisco-eigenes Protokoll, mit dessen Hilfe für Geräte eine Peer-to-Peer-Hierarchie hergestellt werden kann. Über diese Hierarchie können die in der Hierarchie befindlichen Geräte Firmware-Dateien an die benachbarten Geräte weitergeben.	CPPDP wird von der Funktion „Gemeinsame Firmware für Gruppe“ genutzt.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Dynamic Host Configuration Protocol (DHCP)	DHCP reserviert und weist IP-Adressen zu Netzwerkgeräten zu. DHCP ermöglicht das Einbinden eines IP-Telefons in ein Netzwerk, wobei das Telefon anschließend betriebsbereit ist, ohne dass manuell eine IP-Adresse zugewiesen oder zusätzliche Netzwerkparameter konfiguriert werden müssen.	DHCP ist standardmäßig aktiviert. Wenn DHCP deaktiviert ist, müssen Sie die IP-Adresse, die Subnetzmaske, das Gateway und einen TFTP-Server auf jedem Telefon manuell konfigurieren. Wir empfehlen, die angepasste DHCP-Option 150 zu verwenden. Mit dieser Methode können Sie die IP-Adresse des TFTP-Servers als Optionswert konfigurieren. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager. **Hinweis** Wenn Sie Option 150 nicht nutzen können, empfiehlt sich die DHCP-Option 66.
Hypertext Transfer Protocol (HTTP)	HTTP ist das Standardprotokoll zum Übertragen von Informationen und Dokumenten im Internet und dem Web.	Cisco IP-Telefons nutzen HTTP für XML-Dienste und zur Fehlerbehebung.
Hypertext Transfer Protocol Secure (HTTPS)	HTTPS ist eine Kombination der Übertragungsprotokolle HTTP und SSL/TLS, die eine Verschlüsselung und sichere Identifizierung von Servern ermöglicht.	Webanwendungen, die sowohl HTTP als auch HTTPS unterstützen, verfügen zu diesem Zweck über zwei konfigurierte URLs. Cisco IP-Telefons, die HTTPS unterstützen, wählen die HTTPS-URL aus.
IEEE 802.1X	Der Standard IEEE 802.1X definiert ein Protokoll zur Client-Server-basierten Zugriffskontrolle und Authentifizierung, das dafür sorgt, dass sich ausschließlich autorisierte Clients über öffentlich zugängliche Ports mit einem LAN verbinden können. Bis der Client authentifiziert ist, erlaubt die 802.1X-Zugriffssteuerung nur den EAPOL-Verkehr (Extensible Authentication Protocol over LAN) über den Port, mit dem der Client verbunden ist. Nach der erfolgreichen Authentifizierung kann der normale Verkehr über den Port weitergeleitet werden.	Die Implementierung des Standards IEEE 802.1X erfolgt auf dem Cisco IP-Telefon durch Unterstützung der Authentifizierungsmethoden EAP-FAST und EAP-TLS. Wenn auf dem Telefon die 802.1X-Authentifizierung aktiviert ist, sollten Sie das PC-Port- und Sprach-VLAN deaktivieren.
IEEE 802.11n/802.11ac	Der Standard IEEE 802.11 regelt die Kommunikation von Geräten in einem lokalen Funknetzwerk (WLAN). Teilstandard 802.11n arbeitet sowohl im 2,4-GHz- als auch im 5-GHz-Frequenzbereich, während 802.11ac nur für den 5-GHz-Frequenzbereich zuständig ist.	Die 802.11-Schnittstelle ist insbesondere in Situationen, in denen keine Ethernet-Verkabelung zur Verfügung steht bzw. eingesetzt werden soll, eine geeignete Bereitstellungsalternative. Nur Cisco IP-Telefon 8861 und 8865 unterstützen WLAN.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Internet Protocol (IP)	IP ist ein Messaging-Protokoll, das Pakete im Netzwerk verarbeitet und sendet.	Damit Netzwerkgeräte mittels IP kommunizieren können, müssen ihnen eine IP-Adresse, ein Subnetz und ein Gateway zugewiesen sein. Wenn Sie für Cisco IP-Telefon DHCP (Dynamic Host Configuration Protocol) nutzen, erfolgt die Zuweisung von IP-Adresse, Subnetz und Gateway automatisch. Wenn Sie DHCP nicht verwenden, müssen Sie diese Eigenschaften jedem Telefon manuell zuweisen. Cisco IP-Telefons unterstützen die Verwendung von IPv6-Adressen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
Link Layer Discovery Protocol (LLDP)	LLDP ist ein standardisiertes Netzwerkerkennungsprotokoll (ähnlich wie CDP), das auf einigen Geräten von Cisco und Drittanbietern unterstützt wird.	Das Cisco IP-Telefon unterstützt LLDP auf dem PC-Port.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED ist eine Erweiterung des LLDP-Standards speziell für Produkte zur Sprachübertragung.	Das Cisco IP-Telefon unterstützt LLDP-MED auf dem SW-Port, um folgende Informationen weiterzugeben: • Sprach-VLAN-Konfiguration • Geräteerkennung • Energieverwaltung • Bestandsverwaltung
Real-Time Transport Protocol (RTP)	RTP ist ein Protokoll zur Übertragung von Echtzeitdaten (z. B. interaktive Sprachübertragung) in Datennetzwerken.	Cisco IP-Telefons verwenden das RTP-Protokoll, um Echtzeit-Sprachverkehr zu senden und von anderen Telefonen und Gateways zu empfangen.
Real-Time Control Protocol (RTCP)	RTCP wird gemeinsam mit RTP genutzt und liefert QoS-Daten (z. B. Jitter-Werte, Latenz, Round-Trip-Verzögerung) von RTP-Datenströmen.	RTCP ist standardmäßig aktiviert.
Session Description Protocol (SDP)	Bei SDP handelt es sich um den Teil des SIP-Protokolls, der festlegt, welche Parameter während einer Verbindung zwischen zwei Endgeräten verfügbar sind. Beim Erstellen von Konferenzen werden nur die SDP-Funktionen verwendet, die von allen an der Konferenz teilnehmenden Endgeräten unterstützt werden.	Normalerweise werden SDP-Funktionen wie Codec-Typen, DTMF-Erkennung oder Komfortrauschen vom Cisco Unified Communications Manager oder dem Medien-Gateway im laufenden Betrieb global konfiguriert. Bei manchen SIP-Endgeräten können diese Parameter jedoch direkt auf dem Endgerät konfiguriert werden.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Session Initiation Protocol (SIP)	SIP ist der IETF-Standard (Internet Engineering Task Force) für Multimedia-Konferenzen über IP. SIP ist ein ASCII-basiertes Steuerungsprotokoll auf Anwendungsebene (definiert in RFC 3261), das verwendet werden kann, um Anrufe zwischen zwei oder mehr Endpunkten zu initiieren, aufrechtzuerhalten und abzubrechen.	SIP ist wie andere VoIP-Protokolle für die Funktionen des Signalübertragungs- und Sitzungsmanagements innerhalb eines Netzwerks für paketbasierte Telefonie zuständig. Mittels Signalübertragung können Anrufinformationen über Netzwerkgrenzen hinweg transportiert werden, während das Sitzungsmanagement die Steuerung der Attribute eines End-to-End-Anrufs ermöglicht. Cisco IP-Telefons unterstützen das SIP-Protokoll sowohl beim Betrieb im reinen IPv6-Modus und im reinen IPv4-Modus wie auch im kombinierten IPv4/IPv6-Modus.
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	Cisco IP-Telefons nutzen TCP für die Verbindung mit dem Cisco Unified Communications Manager sowie für den Zugriff auf XML-Dienste.
Transport Layer Security (TLS)	TLS ist ein Standardprotokoll zum Schützen und Authentifizieren der Kommunikation.	Wenn entsprechende Sicherheitseinstellungen konfiguriert sind, verwenden Cisco IP-Telefons das TLS-Protokoll zum sicheren Registrieren beim Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP ermöglicht die Dateiübertragung über das Netzwerk. Auf dem Cisco IP-Telefon ermöglicht TFTP das Abrufen einer für den Telefontyp spezifischen Konfigurationsdatei.	Für TFTP muss im Netzwerk ein TFTP-Server vorhanden sein, den der DHCP-Server automatisch identifizieren kann. Wenn das Telefon einen anderen als den vom DHCP-Server festgelegten TFTP-Server verwenden soll, müssen Sie die IP-Adresse dieses TFTP-Servers manuell über das Menü „Netzwerkkonfiguration“ des Telefons zuweisen. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.
User Datagram Protocol (UDP)	UDP ist ein verbindungsloses Protokoll für die Übertragung von Datenpaketen.	Dieses Protokoll wird ausschließlich für RTP-Datenströme verwendet. Von der SIP-Signalübertragung der Telefone wird UDP nicht unterstützt.

Weitere Informationen zur Unterstützung von LLDP-MED können Sie dem „Whitepaper LLDP-MED and Cisco Discovery Protocol“ (LLDP-MED und das Cisco Discovery Protocol) entnehmen, das unter folgender Adresse abrufbar ist:

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper0900aecd804cd46d.shtml

Verwandte Themen

802.1X-Authentifizierung
Netzwerkeinstellungen konfigurieren
Überprüfung des Telefons beim Starten
VLAN-Interaktion, auf Seite 10

VLAN-Interaktion

Das Cisco IP-Telefon enthält einen internen Ethernet-Switch, über den Pakete an das Telefon, an den Computerport und an den Netzwerkport auf der Rückseite des Telefons weitergeleitet werden können.

Wenn ein Computer an den Computerport angeschlossen ist, verwenden der Computer und das Telefon dieselbe physische Verbindung mit dem Switch und denselben Port am Switch. Dies wirkt sich folgendermaßen auf die VLAN-Konfiguration im Netzwerk aus:

- Die derzeit vorhandenen VLANs können auf IP-Subnetz-Basis konfiguriert werden. Möglicherweise sind jedoch keine zusätzlichen IP-Adressen verfügbar, die dem Telefon im gleichen Subnetz wie andere Geräte, die sich mit dem gleichen Port verbinden, zugewiesen werden können.
- Durch den bei Telefonen mit VLAN-Unterstützung vorhandenen Datenverkehr wird möglicherweise die Qualität des VoIP-Datenverkehrs verringert.
- Die Netzwerksicherheit meldet möglicherweise einen Bedarf zur Trennung des VLAN-Sprachdatenverkehrs vom VLAN-Datenverkehr.

Diese Probleme können Sie lösen, indem Sie den Sprachdatenverkehr in ein separates VLAN verlegen. Der Switch-Port, an den das Telefon angeschlossen ist, wird für separate VLANs für Folgendes konfiguriert:

- Weiterleitung des Sprachdatenverkehrs zum und vom IP-Telefon (zusätzliches VLAN z. B. in der Cisco Catalyst 6000-Serie)
- Datenverkehr zum und vom PC, der über den Computerport des IP-Telefons an den Switch angeschlossen ist (systemeigenes VLAN)

Durch die Verlegung der Telefone in ein separates, zusätzliches VLAN wird die Qualität des Sprachdatenverkehrs verbessert, und Sie können eine große Anzahl von Telefonen zu einem bestehenden Netzwerk hinzufügen, das eigentlich nicht genügend IP-Adressen für alle Telefone besitzt.

Weitere Informationen finden Sie in der Dokumentation für den Cisco Switch. Außerdem finden Sie Informationen zu Switches unter folgender URL:

http://cisco.com/en/US/products/hw/switches/index.html

Cisco Unified Communications Manager-Interaktion

Cisco Unified Communications Manager ist ein offenes Anrufverarbeitungssystem, das dem Industriestandard entspricht. Die Cisco Unified Communications Manager-Software startet und bricht Anrufe zwischen Telefonen ab, indem herkömmliche PBX-Funktionen im IP-Firmennetzwerk integriert werden. Cisco Unified Communications Manager verwaltet die Komponenten des Telefonie-Systems, beispielsweise die Telefone, die Gateways für den Zugriff und die für Funktionen erforderlichen Ressourcen, beispielsweise Konferenzanrufe und Routenplanung. Cisco Unified Communications Manager stellt auch Folgendes bereit:

- Firmware für Telefone

- Certificate Trust List-(CTL-) und Identity Trust List-(ITL-)Dateien, die TFTP- und HTTP-Dienste verwenden
- Telefonregistrierung
- Der Anruf wird beibehalten, damit eine Mediensitzung fortgesetzt wird, wenn das Signal zwischen Communications Manager und einem Telefon unterbrochen wird.

Weitere Informationen zum Konfigurieren von Cisco Unified Communications Manager für Telefone, die in diesem Kapitel beschrieben werden, finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager.

Hinweis Wenn das Telefonmodell, das Sie konfigurieren möchten, nicht in der Dropdown-Liste Telefontyp in der Cisco Unified Communications Manager-Verwaltung angezeigt wird, laden Sie das neueste Gerätepaket für Ihre Version von Cisco Unified Communications Manager von Cisco.com herunter.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Cisco Unified Communications Manager Express-Interaktion

Wenn Ihr Telefon mit Cisco Unified Communications Manager Express (Unified CME) verwendet wird, muss es in den CME-Modus wechseln.

Wenn ein Benutzer die Konferenzfunktion aufruft, ermöglicht das Tag dem Telefon, entweder eine lokale oder eine Netzwerk-Hardware-Konferenzbrücke zu verwenden.

Die Telefone bieten keine Unterstützung für folgende Aktionen:

- Übergabe: Wird nur im Übergabeszenario für verbundene Anrufe unterstützt.
- Konferenz: Wird nur im Übergabeszenario für verbundene Anrufe unterstützt.
- Zusammenführen: Wird bei Verwendung der Konferenztaste oder bei Hookflash-Zugriff unterstützt.
- Halten: Wird bei Verwendung der Halten-Taste unterstützt.
- Aufschalten und Zusammenführen: Wird nicht unterstützt.
- Direkte Übergabe: Wird nicht unterstützt.
- Auswählen – wird nicht unterstützt.

Die Benutzer können nicht über verschiedene Leitungen hinweg Konferenzen erstellen und Anrufe übergeben.

Unified CME unterstützt Intercom-Anrufe, was auch als Whisper-Paging bezeichnet wird. Jedoch wird die Seite vom Telefon bei Anrufen abgelehnt.

Sowohl der Sitzungsleitungsmodus als auch der erweiterte Leitungsmodus werden im CME-Modus unterstützt.

Interaktion mit dem Sprachnachrichtensystem

In Cisco Unified Communications Manager können Sie verschiedene Sprachnachrichtensysteme integrieren, u. a. das Sprachnachrichtensystem Cisco Unity Connection. Weil die Integration mit vielen verschiedenen Systemen möglich ist, müssen Sie die Benutzer über den Umgang mit dem bei Ihnen vorhandenen System informieren.

Damit ein Benutzer an Voicemail übergeben kann, richten Sie ein *xxxxx Wählmuster ein und konfigurieren Sie es als "Alle Anrufe an Voicemail umleiten". Weitere Informationen finden Sie in der Dokumentation zu Cisco Unified Communications Manager.

Sie müssen jedem Benutzer folgende Informationen zur Verfügung stellen:

- Wie der Zugriff auf das Konto des Sprachnachrichtensystems erfolgt.

  Stellen Sie sicher, dass die Taste „Nachrichten“ auf dem Cisco IP-Telefon in Cisco Unified Communications Manager konfiguriert wurde.

- Wie das Initialkennwort für den Zugriff auf das Sprachnachrichtensystem lautet.

  Konfigurieren Sie für das Sprachnachrichtensystem ein Standardkennwort für alle Benutzer.

- Wie das Telefon anzeigt, dass Sprachnachrichten vorhanden sind.

  Verwenden Sie Cisco Unified Communications Manager, um eine Nachrichtenanzeigemethode (MWI) einzurichten.

Übersicht über den Startvorgang des Telefons

Beim Herstellen einer Verbindung mit dem VoIP-Netzwerk durchläuft das Cisco IP-Telefon einen Standardstartvorgang. Je nach Netzwerkkonfiguration kommen nicht alle der folgenden Schritte bei Ihrem Cisco IP-Telefon zur Anwendung.

1. Schließen Sie das Telefon zur Stromversorgung an den Switch an. Wenn ein Telefon keine externe Stromzufuhr bezieht, sorgt der Switch für die interne Stromversorgung über das angeschlossene Ethernet-Kabel.
2. (Nur für Cisco IP-Telefon 8861 und 8865 im Wireless LAN) Führen Sie einen Scan nach einem Access Point durch. Cisco IP-Telefon 8861 und 8865 scannen mit dem Funksignal den HF-Bereich. Das Telefon durchsucht die Netzwerkprofile und scannt nach Access Points, die eine passende SSID und einen passenden Authentifizierungstyp enthalten. Das Telefon ordnet sich dem Access Point mit dem höchsten RSSI zu, der mit dem Netzwerkprofil übereinstimmt.
3. (Nur für Cisco IP-Telefon 8861 und 8865 im Wireless LAN) Authentifizieren Sie sich am Access Point. Das Cisco IP-Telefon startet den Authentifizierungsvorgang. In der folgenden Tabelle wird der Authentifizierungsvorgang beschrieben:

Authentifizierungstyp	Schlüsselverwaltungsoptionen	Beschreibung
Offen	Keine	Jedes Gerät kann sich beim Access Point authentifizieren. Als zusätzliche Sicherheitsmaßnahme können Sie optional die statische WEP-Verschlüsselung verwenden.

Authentifizierungstyp	Schlüsselverwaltungsoptionen	Beschreibung
Gemeinsamer Schlüssel	Keine	Das Telefon verschlüsselt den Text mithilfe des WEP-Schlüssels, und der Access Point muss den WEP-Schlüssel verifizieren, mit dem der Text verschlüsselt wurde, bevor der Netzwerkzugriff verfügbar ist.
PEAP oder EAP-FAST	Keine	Der RADIUS-Server authentifiziert den Benutzernamen und das Kennwort, bevor der Netzwerkzugriff verfügbar ist.

4. Laden Sie das gespeicherte Telefon-Image. Beim Startvorgang führt das Telefon ein Bootstrapladeprogramm aus, mit dem ein im Flash-Speicher gespeichertes Telefonfirmware-Image geladen wird. Dieses Image verwendet das Telefon zur Initialisierung der Soft- und Hardware.
5. Konfigurieren Sie das VLAN. Wenn das Cisco IP-Telefon mit einem Cisco Catalyst-Switch verbunden ist, informiert der Switch das Telefon nun über das Sprach-VLAN, das auf dem Switch definiert ist. Das Telefon muss die VLAN-Mitgliedschaft kennen, bevor es mit der DHCP-Anfrage (Dynamic Host Configuration Protocol) nach einer IP-Adresse fortfahren kann.
6. Rufen Sie eine IP-Adresse ab. Wenn das Cisco IP-Telefon die IP-Adresse über DHCP erhält, startet das Telefon eine entsprechende Anfrage an den DHCP-Server. Wenn Sie in Ihrem Netzwerk kein DHCP verwenden, müssen Sie jedem Telefon lokal eine statische IP-Adresse zuweisen.
7. Rufen Sie die CTL-Datei ab. Der TFTP-Server speichert die CTL-Datei. Diese Datei enthält die für die Herstellung einer sicheren Verbindung zwischen dem Telefon und Cisco Unified Communications Manager erforderlichen Zertifikate.

   Weitere Informationen hierzu finden Sie in der Dokumentation zu Ihrer jeweiligen Version von Cisco Unified Communications Manager.
8. Rufen Sie die ITL-Datei ab. Das Telefon ruft die ITL-Datei nach der CTL-Datei ab. Die ITL-Datei enthält die Zertifikate der für das Telefon vertrauenswürdigen Entitäten. Die Zertifikate werden für die Authentifizierung einer sicheren Verbindung zu den Servern oder einer von den Servern signierten digitalen Signatur verwendet. Cisco Unified Communications Manager 8.5 und höher unterstützt die ITL-Datei.
9. Konfigurieren Sie den Zugriff auf einen TFTP-Server. Der DHCP-Server weist nicht nur eine IP-Adresse zu, er leitet das Cisco IP-Telefon auch an einen TFTP-Server weiter. Wenn das Telefon eine statisch definierte IP-Adresse besitzt, müssen Sie den TFTP-Server lokal auf dem Telefon konfigurieren. Das Telefon kontaktiert den TFTP-Server dann direkt.

Hinweis Sie können auch einen alternativen TFTP-Server zuweisen, der anstelle des vom DHCP-Protokoll zugewiesenen Servers verwendet werden soll.

10. Rufen Sie die Konfigurationsdatei ab. Der TFTP-Server besitzt Konfigurationsdateien, in denen die Parameter für das Herstellen einer Verbindung zu Cisco Unified Communications Manager und andere Informationen für das Telefon definiert sind.
11. Stellen Sie eine Verbindung mit Cisco Unified Communications Manager her. In der Konfigurationsdatei ist festgelegt, wie das Cisco IP-Telefon mit Cisco Unified Communications Manager kommuniziert,

und es wird eine Software-ID für das Telefon bereitgestellt. Nachdem das Telefon die Datei vom TFTP-Server abgerufen hat, versucht es, eine Verbindung mit der Cisco Unified Communications Manager-Version mit der höchsten Priorität in der Liste herzustellen.

Wenn das Sicherheitsprofil des Telefons für die sichere Signalisierung (verschlüsselt oder authentifiziert) konfiguriert ist und Cisco Unified Communications Manager auf den sicheren Modus eingestellt ist, stellt das Telefon eine TLS-Verbindung her. Andernfalls stellt das Telefon eine nicht sichere TCP-Verbindung her.

Wenn das Telefon manuell zur Datenbank hinzugefügt wurde, wird es von Cisco Unified Communications Manager identifiziert. Wenn das Telefon nicht manuell zur Datenbank hinzugefügt wurde und die automatische Registrierung in Cisco Unified Communications Manager aktiviert ist, versucht das Telefon, sich selbst automatisch in der Cisco Unified Communications Manager-Datenbank zu registrieren.

Hinweis Wenn Sie den CTL-Client konfiguriert haben, ist die automatische Registrierung deaktiviert. In diesem Fall müssen Sie das Telefon manuell zur Cisco Unified Communications Manager-Datenbank hinzufügen.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Externe Geräte

Wir empfehlen die Verwendung von qualitativ hochwertigen, externen Geräten, die gegen unerwünschte RF-Signale (Radiofrequenz) und AF-Signale (Audiofrequenz) geschirmt sind. Externe Geräte sind beispielsweise Headsets, Kabel und Steckverbinder.

Je nach der Qualität dieser Geräte und deren Abstand zu anderen Geräten wie Mobiltelefonen oder Funkgeräten, kann trotzdem ein geringes Rauschen auftreten. In diesen Fällen empfehlen wir eine oder mehrere der folgenden Maßnahmen:

- Vergrößern Sie den Abstand zwischen dem externen Gerät und der RF- oder AF-Signalquelle.
- Verlegen Sie die Anschlusskabel des externen Geräts in einem möglichst großen Abstand zur RF- oder AF-Signalquelle.
- Verwenden Sie für das externe Gerät abgeschirmte Kabel oder Kabel mit hochwertiger Abschirmung und hochwertigen Anschlussteckern.
- Kürzen Sie das Anschlusskabel des externen Geräts.
- Führen Sie die Kabel des externen Geräts durch einen Ferritkern oder eine ähnliche Vorrichtung.

Cisco kann keine Garantie für die Leistung von externen Geräten, Kabeln und Steckern übernehmen.

Vorsicht Verwenden Sie in EU-Ländern ausschließlich externe Lautsprecher, Mikrofone und Headsets, die mit der EU-Richtlinie 89/336/EWG konform sind.

Informationen zum USB-Port

Cisco IP-Telefon 8851, 8851NR, 8861, 8865 und 8865NR unterstützen maximal fünf Geräte, die an den einzelnen USB-Ports angeschlossen sind. Jedes an das Telefon angeschlossene Gerät wird bei der Anzahl der maximal zulässigen Geräte berücksichtigt. Ihr Telefon kann beispielsweise am seitlichen Anschluss fünf USB-Geräte und am hinteren Anschluss fünf zusätzliche USB-Standardgeräte unterstützen. Viele USB-Produkte von Drittherstellern zählen jedoch als mehrere USB-Geräte, beispielsweise kann ein Gerät, das einen USB-Hub und ein Headset enthält, als zwei USB-Geräte zählen. Weitere Informationen hierzu finden Sie in der Dokumentation für das jeweilige USB-Gerät.

Hinweis

- Hubs ohne Stromversorgung werden nicht unterstützt; Hubs mit Stromversorgung mit mehr als vier Ports werden ebenfalls nicht unterstützt.
- USB-Headsets, die über einen USB-Hub an das Telefon angeschlossen sind, werden nicht unterstützt.

Jedes an das Telefon angeschlossene Erweiterungsmodul wird als USB-Gerät gezählt. Wenn drei Tastenerweiterungsmodule an das Telefon angeschlossen sind, zählen diese als drei USB-Geräte.

Konfigurationsdateien für Telefone

Die Konfigurationsdateien für Telefone sind auf dem TFTP-Server gespeichert und definieren die für die Verbindung mit dem Cisco Unified Communications Manager benötigten Parameter. Generell wird die Konfigurationsdatei eines Telefons immer dann automatisch geändert, wenn Sie im Cisco Unified Communications Manager eine Änderung vornehmen, die ein Zurücksetzen des Telefons erforderlich macht.

Außerdem enthalten Konfigurationsdateien auch Informationen zum geladenen Image, das auf dem Telefon ausgeführt werden sollte. Wenn diese Abbildinformationen nicht mit dem tatsächlich auf dem Telefon geladenen Image übereinstimmen, wird vom Telefon eine Anfrage an den TFTP-Server zur Bereitstellung der erforderlichen Softwaredateien gesendet.

Wenn Sie in Cisco Unified Communications Manager-Verwaltung sicherheitsrelevante Einstellungen konfigurieren, sind in der Telefonkonfigurationsdatei auch vertrauliche Informationen enthalten. Damit die Konfigurationsdatei entsprechend ihrer Vertraulichkeit geschützt ist, müssen Sie die Datei so konfigurieren, dass eine Verschlüsselung erfolgt. Weitere Informationen finden Sie in der Dokumentation für Ihre Version von Cisco Unified Communications Manager. Bei jedem Neustart und anschließender Registrierung bei Cisco Unified Communications Manager rufen die Telefone eine Konfigurationsdatei ab.

Wenn die folgenden drei Bedingungen gegeben sind, greift ein Telefon bei diesem Vorgang auf die auf dem TFTP-Server befindliche Standardkonfigurationsdatei XmlDefault.cnf.xml zu:

- Sie haben die automatische Registrierung aktiviert in Cisco Unified Communications Manager
- Das Telefon wurde nicht zur Cisco Unified Communications Manager-Datenbank hinzugefügt.
- Das Telefon registriert sich zum ersten Mal.

Verwandte Themen

Dokumentation Cisco Unified Communications Manager

Verhalten des Telefons bei Netzwerküberlastung

Alles, was zu einer Verschlechterung der Netzwerkleistung führt, kann auch die Audio- und Videoqualität beeinträchtigen. In manchen Fällen kann es sogar zu einem Abbruch des Telefonats kommen. Eine Netzwerküberlastung kann unter anderem von folgenden Aktivitäten verursacht werden:

- Administrative Aufgaben, beispielsweise einen internen Port- oder Sicherheits-Scan.
- Netzwerkangriffe, beispielsweise ein Denial-of-Service-Angriff.

Telefonverhalten in einem Netzwerk mit zwei Netzwerkroutern

Die Cisco IP-Telefon 8800-Serie verwendet eine Firewall zum Schutz vor Cyber-Angriffen wie z. B. einem Man-in-the-Middle-Angriff. Diese Firewall kann nicht deaktiviert werden. Wenn Sie Ihr Netzwerk mit zwei Netzwerkroutern im gleichen Subnetz und IP-Umleitung konfigurieren, kann dies dazu führen, dass der Datenverkehr auf einem Telefon gestoppt wird.

Die Telefon-Firewall stoppt den Datenverkehr, da dieses Netzwerk-Setup einem Man-in-the-Middle-Angriff ähnelt. Das Telefon empfängt Umleitungspakete für verschiedene Ziel-IPs in einem anderen Subnetz als das Telefon. Das Telefon befindet sich in einem Netzwerk mit mehreren Routern, und der Standardrouter sendet Datenverkehr an einen zweiten Router.

Wenn Sie den Verdacht haben, dass der Datenverkehr durch die Firewall gestoppt wurde, überprüfen Sie die Telefonprotokolle. Suchen Sie nach einer Benachrichtigung mit Fehlercode 1, die während eines Verbindungsversuchs vom Betriebssystem ausgegeben wurde. Eine der möglichen Signaturen lautet:

```
sip_tcp_create_connection: socket connect failed cpr_errno: 1.
```

Ein Netzwerk mit zwei Netzwerkroutern im gleichen Subnetz und IP-Umleitung ist keine gängige Konfiguration. Wenn Sie dieses Netzwerk-Setup verwenden, sollten Sie in Betracht ziehen, nur einen Router in einem Subnetz zu verwenden. Wenn jedoch zwei Netzwerkrouter im gleichen Subnetz erforderlich sind, deaktivieren Sie die IP-Umleitung auf dem Router, und starten Sie das Telefon neu.

Application Programming Interface

Cisco unterstützt die Nutzung der Telefon-API durch Drittanbieter-Anwendungen, die vom Entwickler der Drittanbieter-Anwendung über Cisco getestet und zertifiziert wurden. Alle Telefonprobleme im Zusammenhang mit einer Interaktion einer nicht zertifizierten Anwendung müssen vom Drittanbieter behoben werden und werden nicht von Cisco bearbeitet.

Einzelheiten zum Support-Modell für von Cisco zertifizierte Drittanbieter-Anwendungen/-Lösungen finden Sie auf der Website des Cisco Solution Partner-Programm.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.