



Technische details

- Fysieke en operationele omgevingspecificaties, op pagina 1
- Kabelspecificaties, op pagina 2
- Voedingsvereisten telefoon, op pagina 4
- Netwerkprotocollen, op pagina 6
- VLAN-interactie, op pagina 10
- Interactie Cisco Unified Communications Manager, op pagina 10
- Interactie Cisco Unified Communications Manager Express, op pagina 11
- Interactie Voicemailstelsysteem, op pagina 11
- Overzicht telefoon opstarten, op pagina 12
- Externe apparaten, op pagina 14
- Gegevens USB-poort, op pagina 14
- Configuratiebestanden telefoon, op pagina 15
- Telefoongedrag tijdens netwerkcongestie, op pagina 15
- Het gedrag van de telefoon op een netwerk met twee netwerkroUTERS, op pagina 15
- Application Programming Interface, op pagina 16

Fysieke en operationele omgevingspecificaties

De volgende tabel beschrijft de fysieke en operationele omgevingspecificaties voor de Cisco IP-telefoon 8800-serie.

Tabel 1: Fysieke en operationele omgevingspecificaties

Specificatie	Waarde of bereik
Bedrijfstemperatuur	0° tot 40°C (32° tot 104°F)
Relatieve vochtigheid bij in bedrijf	In gebruik: 10% tot 90% (niet-condenserend) Niet in gebruik: 10% tot 95% (niet-condenserend)
Opslagtemperatuur	-10° tot 60°C (14° tot 140°F)
Hoogte	229.1 mm (9,02 inch)
Breedte	257.34 mm (10,13 inch)

Specificatie	Waarde of bereik
Diepte	40 mm (1,57 inch)
Gewicht	2,62 kg (lb 1,19)
Voeding	100-240 VAC, 50-60 Hz, 0,5 A, bij gebruik van de AC-adapter 48 VDC, 0,2 A, bij gebruik van de in-line voeding via het netsnoer
Snoeren	Categorie 3/5/5e/6 voor 10-Mbps snoeren met 4 paar Categorie 5/5e/6 voor 100-Mbps snoeren met 4 paar Categorie 5e/6 voor 1000-Mbps snoeren met 4 paar Opmerking Snoeren hebben 4 paar draden voor in totaal 8 conductors.
Afstandsvereisten	Conform de Ethernet-specificatie wordt een maximale kabellengte ondersteund door Cisco IP-telefoon en de switch van 100 meter (330 feet).

Kabelspecificaties

De volgende gegevens geven de kabelspecificaties aan:

- RJ-9-aansluiting (4-conductor) voor aansluiting van handset en hoofdtelefoon
- RJ-45-aansluiting voor de 10/100/1000 BaseT LAN-verbinding (10/100/1000 netwerkpoort op de telefoon)
- RJ-45-aansluiting voor een tweede 10/100/1000 BaseT compatibele verbinding (10/100/1000 computerpoort op de telefoon)
- 3,5 mm aansluiting voor de luidspreker (alleen Cisco IP-telefoon 8861)
- 48-volts voedingsconnector
- USB-poorten/connector: een USB-poort voor Cisco IP-telefoon 8851 en twee USB-poorten voor Cisco IP-telefoon 8861
- 3 verbindingen voor toetsuitbreidingsmodules die worden beschouwd als USB-connector voor Cisco IP-telefoon 8851 en 8861

Pinouts netwerk- en computerpoort

Hoewel zowel de netwerk- als de computer(toegangs)poort worden gebruikt voor netwerkconnectiviteit, dienen deze verschillende doelen en hebben ze verschillende poortpinouts.

- De netwerkpoort is de 10/100/1000 SW-poort op de Cisco IP-telefoon.
- De computerpoort (toegang) is de 10/100/1000 pc-poort op de Cisco IP-telefoon.

Connector netwerkpoort

In de volgende tabel worden de connectorpinouts van de netwerkpoort beschreven.

Tabel 2: Connectorpinouts netwerkpoort

Pinnummer	Functie
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-
Opmerking BI staat voor bidirectioneel, terwijl DA, DB, DC en DD staan voor respectievelijk Data A, Data B, Data C en Data D.	

Connector computerpoort

In de volgende tabel worden de connectorpinouts van de computerpoort beschreven.

Tabel 3: Connectorpinouts computerpoort (toegang)

Pinnummer	Functie
1	BI_DB+
2	BI_DB-
3	BI_DA+
4	BI_DD+
5	BI_DD-
6	BI_DA-
7	BI_DC+
8	BI_DC-
Opmerking BI staat voor bidirectioneel, terwijl DA, DB, DC en DD staan voor respectievelijk Data A, Data B, Data C en Data D.	

Voedingsvereisten telefoon

Cisco IP-telefoon kan worden gevoed met externe voeding of via Power over Ethernet (PoE). Een losse netvoeding levert externe voeding. De switch kan PoE leveren via de Ethernet-kabel van de telefoon.

Cisco IP-telefoon 8861 en 8865 zijn PoE klasse 4-apparaten en vereisen een switch of een lijnkaart met klasse 4-mogelijkheden ter ondersteuning van extra functies.

Raadpleeg voor meer informatie over de eisen van de telefoon het gegevensblad van de telefoon.

Wanneer u een telefoon installeert die wordt gevoed met een externe voeding, sluit u de voeding aan voordat u de Ethernet-kabel op de telefoon aansluit. Wanneer u een telefoon verwijdert die wordt gevoed met een externe voeding, haalt u de Ethernet-kabel los van de telefoon voordat u de voeding loshaalt.

Tabel 4: Richtlijnen voor voeding van Cisco IP-telefoon

Voedingstype	Richtlijnen
Externe voeding: geleverd via CP-PWR-CUBE-4= externe netvoeding	Cisco IP-telefoon gebruikt de CP-PWR-CUBE-4 netvoeding.
PoE-voeding: geleverd door de switch via de Ethernet-kabel die op de telefoon is aangesloten.	Cisco IP-telefoons 8851, 8851NR, 8861, 8865 en 8865NR ondersteunen 802.3at PoE gebruik van accessoires. Raadpleeg voor meer informatie het gegevensblad van de telefoon. De switch vereist een reservevoeding zodat de werking van de telefoon niet wordt onderbroken. Controleer of de CatOS- of IOS-versie die op de switch werkt, de gewenste telefoonimplimentatie ondersteunt. Zie de documentatie voor uw switch voor informatie over de versie van het besturingssysteem.
Universal Power over Ethernet (UPoE)	Cisco IP-telefoon 8865 en 8865NR ondersteunen UPoE.

De documenten in de volgende tabel bevatten meer informatie over de volgende onderwerpen:

- Cisco-switches die met Cisco IP-telefoon werken
- Cisco IOS-versies die bidirectionele onderhandelingen over voeding ondersteunen
- Andere vereisten en beperkingen over voeding

Tabel 5: Aanvullende informatie

Documentonderwerpen	URL
PoE-oplossingen	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/index.html
Cisco Catalyst Switches	http://www.cisco.com/c/en/us/products/switches/index.html
Integrated Service Routers	http://www.cisco.com/c/en/us/products/routers/index.html

Documentonderwerpen	URL
Cisco IOS-software	http://www.cisco.com/c/en/us/products/ios-nx-os-software/in

Stroomstoring

Als u contact wilt opnemen met nooddiensten, moet uw telefoon worden voorzien van stroom. Als er een onderbreking in de stroomvoorziening optreedt, zijn nooddiensten pas weer bereikbaar wanneer de stroomvoorziening is hersteld. Bij een stroomstoring of stroomuitval moet u de apparatuur wellicht resetten of configureren voordat u nooddiensten kunt bellen.

Energiebesparingen

U kunt de hoeveelheid energie beperken die door Cisco IP-telefoon wordt verbruikt door de modus Energiebesparing of EnergyWise (Power Save Plus) te gebruiken.

Energiebesparing

In de Energiebesparingsmodus wordt de achtergrondverlichting van het scherm uitgeschakeld wanneer de telefoon niet wordt gebruikt. De telefoon blijft in de Energiebesparingsmodus voor de geplande duur of tot de gebruiker de handset opneemt of op een knop drukt.

Power Save Plus (EnergyWise)

De Cisco IP-telefoon ondersteunt de modus Cisco EnergyWise (Power Save Plus). Wanneer uw netwerk een EnergyWise-controller (EW) bevat (bijvoorbeeld een Cisco-switch met de EnergyWise-voorziening ingeschakeld), kunt u de telefoons zo configureren dat ze sluimeren (uitschakelen) en ontwakken (inschakelen) volgens een schema om het energieverbruik verder te verminderen.

Configureer elke telefoon zodanig dat deze de EnergyWise-instellingen kan in- of uitschakelen. Als EnergyWise is ingeschakeld, configureert u een slaap- en een wektijd naast andere parameters. Deze parameters worden naar de telefoon verzonden als onderdeel van het XML-bestand voor telefoonconfiguratie.

Power Negotiation Over LLDP

De telefoon en de switch onderhandelen over de voeding die de telefoon verbruikt. Cisco IP-telefoon werkt met meerdere energie-instellingen, die het stroomverbruik verlagen wanneer minder stroom beschikbaar is.

Nadat een telefoon opnieuw is opgestart, is de switch op één protocol (CDP of LLDP) ingesteld voor het onderhandelen over de voeding. De switch wordt vergrendeld op het eerste protocol (met een drempelwaarde [Threshold Limit Value, TLV]) die door de telefoon wordt verzonden. Als de systeembeheerder dat protocol op de telefoon uitschakelt, kan de telefoon geen accessoires opstarten omdat de switch niet reageert op de voedingsaanvragen in het andere protocol.

Cisco raadt aan dat Power Negotiation altijd is ingeschakeld (standaard) wanneer verbinding wordt gemaakt met een switch die voedingsonderhandelingen ondersteunt.

Als Power Negotiation is uitgeschakeld, kan de switch de voeding naar de telefoon afsluiten. Als de switch geen voedingsonderhandelingen ondersteunt, schakelt u de functie Power Negotiation uit voordat u accessoires over PoE opstart. Wanneer de functie Power Negotiation is uitgeschakeld, kan de telefoon accessoires voeden tot het maximum dat de IEEE 802.3af-2003-standaard toestaat.



Opmerking

- Wanneer CDP en Power Negotiation zijn uitgeschakeld, kan de telefoon accessoires tot 15,4 W voeden.

Netwerkprotocollen

Cisco IP-telefoon 8800-serie ondersteunt diverse industriestandaard en Cisco-netwerkprotocollen die vereist zijn voor gesproken communicatie. In de volgende tabel ziet u een overzicht van de netwerkprotocollen die door de telefoons worden ondersteund.

Tabel 6: Ondersteunde netwerkprotocollen voor Cisco IP-telefoon 8800-serie

Netwerkprotocol	Doel	Opmerkingen over gebruik
Bluetooth	Bluetooth is een draadloos persoonlijk netwerk-protocol (WPAN) dat aangeeft hoe apparaten over korte afstand communiceren.	Cisco IP-telefoons 8845, 8865 en 8851 ondersteunen Bluetooth 4.1. Cisco IP-telefoon 8861 ondersteunt Bluetooth 4.0. Cisco IP-telefoon 8811, 8841, 8851NR en 8865NR ondersteunen Bluetooth niet.
Bootstrap Protocol (BootP)	BootP schakelt een netwerkapparaat, zoals Cisco IP-telefoon, in om bepaalde opstartgegevens te detecteren, zoals het IP-adres.	—
Cisco Audio Session Tunnel (CAST)	Met het CAST-protocol kunnen uw telefoons en de bijbehorende toepassingen communiceren met de externe IP-telefoons zonder dat wijzigingen in de signaleringsonderdelen nodig zijn.	Cisco IP-telefoon gebruikt CAST als een interface tussen CUVA en Cisco Unified Communications Manager met Cisco IP-telefoon als SIP-proxy.
Cisco Discovery Protocol (CDP)	CDP is een apparaatdetectieprotocol dat werkt op alle door Cisco gefabriceerde apparatuur. Een apparaat kan CDP gebruiken om zijn bestaan aan te geven voor andere apparaten en informatie over andere apparaten te ontvangen in het netwerk.	Cisco IP-telefoons gebruiken CDP om informatie te communiceren als de hulp-VLAN-id, voedingsbeheerdetails per poort en QoS-configuratiegegevens (Quality of Service) met de Cisco Catalyst-switch.
Cisco Peer-to-Peer Distribution Protocol (CPPDP)	CPPDP is een eigen protocol van Cisco dat wordt gebruikt om een gelijkwaardige hiërarchie van apparaten te vormen. Deze hiërarchie wordt gebruikt om firmwarebestanden te distribueren van peer-apparaten naar hun aangrenzende apparaten.	CPPDP wordt gebruikt door de functie Peer firmware delen.

Netwerkprotocol	Doel	Opmerkingen over gebruik
Dynamic Host Configuration Protocol (DHCP)	<p>DHCP wijst een IP-adres dynamisch toe aan netwerkkapparaten.</p> <p>Met DHCP kunt u een IP-telefoon aansluiten op het netwerk en de telefoon laten werken zonder dat u handmatig een IP-adres moet toewijzen of aanvullende netwerkparameters moet configureren.</p>	<p>DHCP is standaard ingeschakeld. Als DHCP is uitgeschakeld, moet u het IP-adres, subnetmasker, gateway en TFTP-server lokaal handmatig op elke telefoon configureren.</p> <p>We raden u aan de aangepaste DHCP-optie 150 te gebruiken. Met deze methode kunt u het IP-adres van de TFTP-server configureren als de optiewaarde. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.</p> <p>Opmerking Als u de optie 150 niet kunt gebruiken, kunt u het proberen met de DHCP-optie 66.</p>
Hypertext Transfer Protocol (HTTP)	HTTP is de standaardmanier voor informatie-overdracht en het verplaatsen van documenten over internet en het web.	Cisco IP-telefoons gebruiken HTTP voor XML-services en probleemoplossing.
Hypertext Transfer Protocol Secure (HTTPS)	Hypertext Transfer Protocol Secure (HTTPS) is een combinatie van Hypertext Transfer Protocol met het SSL/TLS-protocol voor het leveren van codering en veilige identificatie van servers.	Voor webtoepassingen met ondersteuning voor zowel HTTP als HTTPS worden twee URL's geconfigureerd. Cisco IP-telefoons die HTTPS ondersteunen, kiezen de HTTPS-URL.
IEEE 802.1X	<p>Met de IEEE 802.1X-standaard wordt een protocol voor client-/servergebaseerd toegangsbeheer en verificatie gedefinieerd dat ervoor zorgt dat niet-geautoriseerde clients geen verbinding kunnen maken met een LAN via openbaar toegankelijke poorten.</p> <p>Totdat de client wordt geverifieerd, staat 802.1X-toegangsbeheer alleen EAPOL-verkeer (Extensible Authentication Protocol over LAN) toe via de poort waarmee de client is verbonden. Als de verificatie is gelukt, kan normaal verkeer de poort passeren.</p>	<p>Cisco IP-telefoon implementeert de IEEE 802.1X-standaard door ondersteuning te bieden voor de volgende verificatiemethoden: EAP-FAST en EAP-TLS.</p> <p>Wanneer 802.1X-verificatie wordt ingeschakeld op de telefoon, moet u de pc-poort en spraak-VLAN uitschakelen.</p>
IEEE 802.11n/802.11ac	<p>De IEEE 802.11-standaard geeft aan hoe apparaten communiceren via een draadloos LAN-netwerk (WLAN).</p> <p>802.11n werkt met de 2,4-GHz en 5-GHz band en 802.11ac werkt met de 5-GHz band.</p>	<p>De 802.11-interface is een implementatieoptie voor het geval de Ethernet-bekabeling niet beschikbaar of ongewenst is.</p> <p>Alleen Cisco IP-telefoons 8861 en 8865 ondersteunen WLAN.</p>

Netwerkprotocol	Doel	Opmerkingen over gebruik
Internet Protocol (IP)	IP is een berichtprotocol dat pakketten adresseert en verzendt via het netwerk.	<p>Als netwerkapparaten willen communiceren met IP, moeten ze een toegewezen IP-adres, subnet en gateway hebben.</p> <p>IP-adressen, subnetten en gateway-id's worden automatisch toegewezen als u de Cisco IP-telefoon gebruikt met Dynamic Host Configuration Protocol (DHCP). Als u DHCP niet gebruikt, moet u deze eigenschappen lokaal handmatig aan elke telefoon toewijzen.</p> <p>Cisco IP-telefoons ondersteunen IPv6-adressen. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.</p>
Link Layer Discovery Protocol (LLDP)	LLDP is een gestandaardiseerd netwerkdetectieprotocol (vergelijkbaar met CDP) dat wordt ondersteund op een aantal apparaten van Cisco en derden.	Cisco IP-telefoon ondersteunt LLDP op de pc-poort.
Link Layer Discovery Protocol-Media Endpoint Devices (LLDP-MED)	LLDP-MED is een uitbreiding van de LLDP-standaard voor spraakproducten.	<p>Cisco IP-telefoon ondersteunt LLDP-MED op de SW-poort voor het communiceren van informatie zoals:</p> <ul style="list-style-type: none"> • Configuratie spraak-VLAN • Apparaatdetectie • Voedingsbeheer • Inventarisbeheer
Real-Time Transport Protocol (RTP)	RTP is een standaardprotocol voor het transporteren van real-time gegevens, zoals interactieve spraak via gegevensnetwerken.	Cisco IP-telefoons gebruiken het RTP-protocol voor het verzenden en ontvangen van real-time spraakverkeer van andere telefoons en gateways.
Real-Time Control Protocol (RTCP)	RTCP werkt samen met RTP voor het leveren van QoS-gegevens (zoals jitter, latentie en retourvertraging) op RTP-stromen.	RTCP is standaard ingeschakeld.
Session Description Protocol (SDP)	SDP is het gedeelte van het SIP-protocol dat bepaalt welke parameters tijdens een verbinding beschikbaar zijn tussen twee eindpunten. Conferenties worden opgezet met behulp van de SDP-voorzieningen die worden ondersteund door alle eindpunten van de conferentie.	SDP-voorzieningen, zoals codectypen, DTMF-detectie en comfortabel geluid, worden normaal gesproken wereldwijd geconfigureerd door Cisco Unified Communications Manager of de gebruikte Media Gateway. Sommige SIP-eindpunten staan mogelijk configuratie toe van deze parameters op het eindpunt zelf.

Netwerkprotocol	Doel	Opmerkingen over gebruik
Session Initiation Protocol (SIP)	SIP is de IETF-standaard (Internet Engineering Task Force) voor multimediaconferentie via IP. SIP is een op ASCII gebaseerd controleprotocol op de applicatielaag (gedefinieerd in RFC 3261), dat kan worden gebruikt om gesprekken tussen twee of meer eindpunten tot stand te brengen, te onderhouden en te beëindigen.	Net als andere VoIP-protocollen levert SIP functies als signalering en sessiebeheer binnen een telefonienetwerk met pakketten. Met signalering kunnen gespreksgegevens over netwerkgrenzen heen worden verzonden. Sessiebeheer biedt de mogelijkheid om de kenmerken van een end-to-end gesprek te beheren. Cisco IP-telefoons ondersteunen het SIP-protocol wanneer de telefoons werken met alleen IPv6, alleen IPv4, of met zowel IPv4 als IPv6.
Transmission Control Protocol (TCP)	TCP is een verbindingsgericht transportprotocol.	Cisco IP-telefoons gebruiken TCP voor verbinding met Cisco Unified Communications Manager en toegang tot XML-services.
Transport Layer Security (TLS)	TLS is een standaardprotocol voor het beveiligen en verifiëren van communicatie.	Bij de implementatie van beveiliging gebruiken Cisco IP-telefoons het TLS-protocol bij het veilig registreren bij de Cisco Unified Communications Manager.
Trivial File Transfer Protocol (TFTP)	TFTP zorgt dat u bestanden over het netwerk kunt verzenden. Op de Cisco IP-telefoon kunt u met TFTP een configuratiebestand ophalen dat specifiek is voor het telefoontype.	TFTP vereist een TFTP-server in uw netwerk, die automatisch kan worden aangegeven door de DHCP-server. Als u wilt dat een telefoon een TFTP-server gebruikt die afwijkt van degene die is opgegeven door de DHCP-server, kunt u handmatig het IP-adres van de TFTP-server toewijzen via het menu Netwerkinstellingen op de telefoon. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.
User Datagram Protocol (UDP)	UDP is een verbindingsloos berichtenprotocol voor het leveren van gegevenspakketten.	UDP wordt alleen gebruikt voor RTP-stromen. SIP-signaling op de telefoons ondersteunt niet UDP.

Voor meer informatie over ondersteuning voor LLDP-MED raadpleegt u de whitepaper LLDP-MED and Cisco Discovery Protocol:

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

Verwante onderwerpen

[802.1X-verificatie](#)

[Netwerkinstellingen configureren](#)

[Verificatie opstarten telefoon](#)

[VLAN-interactie](#), op pagina 10

[Interactie Cisco Unified Communications Manager](#), op pagina 10

[Interactie Cisco Unified Communications Manager Express](#), op pagina 11

[Audio- en videoportbereik instellen](#)

VLAN-interactie

Cisco IP-telefoon bevat een interne Ethernet-switch, waarmee pakketten naar de telefoon kunnen worden doorgestuurd en naar de computer(toegangs)poort en de netwerkpoort op de achterkant van de telefoon.

Als een computer is aangesloten op de computer(toegangs)poort, delen de computer en de telefoon dezelfde fysieke koppeling met de switch en dezelfde poort op de switch. Deze gedeelde fysieke koppeling heeft de volgende implicaties voor de VLAN-configuratie op het netwerk:

- De huidige VLAN's kunnen worden geconfigureerd op een IP-subnetbasis. Er zijn mogelijk echter geen extra IP-adressen beschikbaar om de telefoon aan hetzelfde subnet toe te wijzen als andere apparaten die verbinding hebben met dezelfde poort.
- Door het gegevensverkeer dat aanwezig is op de telefoons op het VLAN kan de kwaliteit van het VoIP-verkeer afnemen.
- De netwerkbeveiliging kan aangeven dat het nodig is om het VLAN-spraakverkeer te scheiden van het VLAN-gegevensverkeer.

U kunt dit probleem oplossen door het spraakverkeer te isoleren op een aparte VLAN. De switchpoort waarmee de telefoon is verbonden, wordt geconfigureerd op afzonderlijke VLAN's voor het doorgeven van:

- Spraakverkeer naar en van de IP-telefoon (bijvoorbeeld hulp-VLAN op Cisco Catalyst 6000 Series)
- Gegevensverkeer naar en van de pc die verbinding heeft met de switch via de computer(toegangs)poort van de IP-telefoon (native VLAN)

Door het isoleren van de telefoon op een afzonderlijk hulp-VLAN wordt de kwaliteit van het spraakverkeer verhoogd en kan een groot aantal telefoons worden toegevoegd aan een bestaand netwerk dat onvoldoende IP-adressen voor elke telefoon heeft.

Voor meer informatie raadpleegt u de documentatie bij de Cisco-switch. U vindt informatie over de switch via deze URL:

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

Interactie Cisco Unified Communications Manager

Cisco Unified Communications Manager is een open, industriestandaard gespreksverwerkingssysteem. De Cisco Unified Communications Manager-software brengt gesprekken tussen telefoons tot stand en beëindigt ze, waarbij de traditionele PBX-functionaliteit wordt geïntegreerd in het IP-bedrijfsnetwerk. Cisco Unified Communications Manager beheert de componenten van het telefoniesysteem, zoals de telefoon, de toegangsgateways en de resources die nodig zijn voor functies als conferentiegesprekken en routeplanning. Cisco Unified Communications Manager biedt ook:

- Firmware voor telefoons
- CTL- (Certificate Trust List) en ITL-bestanden (Identity Trust List) via de TFTP- en HTTP-services
- Telefoonregistratie

- Bewaren van gesprekken, zodat een mediasessie wordt voortgezet als de signalering tussen de primaire Communications Manager en een telefoon verloren gaat

Voor informatie over het configureren van Cisco Unified Communications Manager voor gebruik met telefoons zoals hier is beschreven, raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.

**Opmerking**

Als het telefoonmodel dat u wilt configureren niet wordt vermeld in de vervolgkeuzelijst Telefoontype in Cisco Unified Communications Manager Administration, installeert u het laatste apparaatpakket voor uw versie van Cisco Unified Communications Manager van Cisco.com.

Verwante onderwerpen

[Cisco Unified Communications Manager Documentatie](#)

Interactie Cisco Unified Communications Manager Express

Als uw telefoon werkt met Cisco Unified Communications Manager Express (Unified CME), moet deze in de CME-modus worden gezet.

Als een gebruiker de conferentiefunctie start, kan de telefoon met deze tag een lokale of een netwerkconferentiebrug gebruiken.

De telefoons ondersteunen de volgende acties niet:

- Doorverbinden: alleen ondersteund in het scenario voor verbonden gesprek doorverbinden.
- Conferentie: alleen ondersteund in het scenario voor verbonden gesprek doorverbinden.
- Deelnemen: ondersteund met de knop Conferentie of Hookflash-toegang.
- Wacht: ondersteund met de knop Wacht.
- Inbreken en samenvoegen: niet ondersteund.
- Direct doorverbinden: niet ondersteund.
- Selecteer: niet ondersteund.

De gebruikers kunnen geen conferentie tot stand brengen en gesprekken doorverbinden via verschillende lijnen.

Unified CME ondersteunt intercomgesprekken, ook wel bekend als Gefluisterde paging. Maar de page wordt tijdens een gesprek afgewezen door de telefoon.

Zowel de modus voor sessielijn als de modus voor een uitgebreide lijn worden ondersteund in de CME-modus.

Interactie Voicemailstelsysteem

In Cisco Unified Communications Manager kunt u verschillende voicemailsystemen integreren, met inbegrip van het Cisco Unity Connection voicemailstelsysteem. Omdat u verschillende systemen kunt integreren, moet u gebruikers voorzien van informatie over het gebruik van uw specifieke systeem.

Als u wilt inschakelen dat een gebruiker kan doorschakelen naar voicemail, stelt u een kiespatroon *xxxxx in en configureert u dit als Alle gesprekken doorschakelen naar voicemail. Voor meer informatie raadpleegt u de documentatie bij Cisco Unified Communications Manager.

Geef de volgende informatie op voor elke gebruiker:

- Hoe ze toegang krijgen tot het account voor het voicemailsysteem.
Zorg ervoor dat u Cisco Unified Communications Manager gebruikt voor het configureren van de knop Berichten op de Cisco IP-telefoon.
- Oorspronkelijk wachtwoord voor toegang tot het voicemailsysteem.
Configureer een standaardwachtwoord voor het voicemailsysteem voor alle gebruikers.
- Hoe de telefoon aangeeft dat er nieuwe berichten zijn.
Gebruik Cisco Unified Communications Manager om een indicator (MWI) voor nieuwe berichten in te stellen.

Overzicht telefoon opstarten

Wanneer u verbinding maakt met het VoIP-netwerk, volgen de Cisco IP-telefoons een standaard opstartprocedure. Afhankelijk van uw specifieke netwerkconfiguratie ziet u slechts een deel van deze stappen op uw Cisco IP-telefoon.

1. Sluit aan op de voeding van de switch. Als een telefoon geen externe voeding gebruikt, biedt de switch voeding via de Ethernet-kabel die is gekoppeld aan de telefoon.
2. (Voor de Cisco IP-telefoon 8861 en 8865 alleen in een draadloos LAN) Zoek naar een toegangspunt. De Cisco IP-telefoon 8861 en 8865 scant het dekkingsgebied voor radiofrequentie. De telefoon zoekt de netwerkprofielen en scant op toegangspunten die een overeenkomende SSID en verificatietype bevatten. De telefoon wordt gekoppeld aan het toegangspunt met de hoogste RSSI die met het netwerkprofiel overeenkomt.
3. (Voor de Cisco IP-telefoon 8861 en 8865 alleen in een draadloos LAN) Verifieer met het toegangspunt. De Cisco IP-telefoon begint het verificatieproces. In de volgende tabel wordt het verificatieproces beschreven:

Verificatietype	Opties sleutelbeheer	Beschrijving
Openen	Geen	Elk apparaat kan worden geverifieerd voor het toegangspunt. Voor extra veiligheid kan statische WEP-codering worden gebruikt.
Gedeelde sleutel	Geen	De telefoon codeert de identiteitsvraag met de WEP-sleutel en het toegangspunt moet de WEP-sleutel controleren die is gebruikt voor het coderen van de identiteitsvraag voordat toegang tot het netwerk beschikbaar is.
PEAP of EAP-FAST	Geen	Op de RADIUS-server worden de gebruikersnaam en het wachtwoord geverifieerd voordat toegang tot het netwerk beschikbaar is.

4. Laad opgeslagen afbeelding van de telefoon. Bij het opstarten wordt op de telefoon een bootstraploader uitgevoerd die de afbeelding van de telefoonfirmware laadt die is opgeslagen in flashgeheugen. Met deze afbeelding initialiseert de telefoon de software en hardware.
5. Configureer het VLAN. Als de Cisco IP-telefoon is aangesloten op een Cisco Catalyst-switch, informeert de switch vervolgens de telefoon over het spraak-VLAN dat is gedefinieerd op de switch. De telefoon moet weten wat het VLAN-lidmaatschap is voordat deze kan doorgaan met het DHCP-verzoek (Dynamic Host Configuration Protocol) voor een IP-adres.
6. Verkrijg een IP-adres. Als de Cisco IP-telefoon DHCP gebruikt om een IP-adres te verkrijgen, vraagt de telefoon de DHCP-server om dit op te halen. Als u niet DHCP in uw netwerk gebruikt, moet u statische IP-adressen lokaal aan elke telefoon toewijzen.
7. Vraag het CTL-bestand aan. Op de TFTP-server is het CTL-bestand opgeslagen. Dit bestand bevat de certificaten die nodig zijn voor het tot stand brengen van een beveiligde verbinding tussen de telefoon en Cisco Unified Communications Manager.

Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager.
8. Vraag het ITL-bestand aan. De telefoon vraagt om het ITL-bestand nadat een verzoek om het CTL-bestand is gedaan. Het ITL-bestand bevat de certificaten van de entiteiten die de telefoon kan vertrouwen. De certificaten worden gebruikt om een veilige verbinding te verifiëren met de servers of om een digitale handtekening te verifiëren die is ondertekend door de servers. Cisco Unified Communications Manager 8.5 en later ondersteunt het ITL-bestand.
9. Krijg toegang tot een TFTP-server. Naast het toewijzen van een IP-adres stuurt de DHCP-server de Cisco IP-telefoon door naar een TFTP-Server. Als de telefoon een statisch gedefinieerd IP-adres heeft, moet u de TFTP-server lokaal op de telefoon configureren: de telefoon neemt vervolgens rechtstreeks contact op met de TFTP-server.



Opmerking U kunt ook een alternatieve TFTP-server toewijzen in plaats van degene die DHCP toewijst.

10. Vraag het configuratiebestand aan. De TFTP-server heeft configuratiebestanden, die de parameters definiëren voor het maken van verbinding met Cisco Unified Communications Manager en andere informatie voor de telefoon.
11. Neem contact op met Cisco Unified Communications Manager. Het configuratiebestand definieert hoe de Cisco IP-telefoon communiceert met Cisco Unified Communications Manager en voorziet een telefoon van de belasting-id. Nadat het bestand is verkregen van de TFTP-server, probeert de telefoon verbinding te maken met de Cisco Unified Communications Manager met de hoogste prioriteit in de lijst.

Als het beveiligingsprofiel van de telefoon is geconfigureerd voor beveiligd signaleren (gecodeerd of geverifieerd) en de Cisco Unified Communications Manager op de beveiligde modus is ingesteld, brengt de telefoon een TLS-verbinding tot stand. Anders wordt een niet-beveiligde TCP-verbinding tot stand gebracht.

Als de telefoon handmatig aan de database is toegevoegd, geeft Cisco Unified Communications Manager de identiteit van de telefoon aan. Als de telefoon niet handmatig is toegevoegd aan de database en autoregistratie in Cisco Unified Communications Manager is ingeschakeld, probeert de telefoon zichzelf te registreren in de Cisco Unified Communications Manager-database.

**Opmerking**

Autoregistratie wordt uitgeschakeld wanneer u de CTL-client configureert. In dit geval moet u de telefoon handmatig toevoegen aan de Cisco Unified Communications Manager-database.

Verwante onderwerpen

[Cisco Unified Communications Manager Documentatie](#)

Externe apparaten

We bevelen u aan externe apparaten van goede kwaliteit te gebruiken, die zijn afgeschermd tegen ongewenste radiofrequentie- en audiofrequentiesignalen. Externe apparaten zijn bijvoorbeeld headsets, kabels en connectors.

Niettemin kan, bijvoorbeeld als gevolg van de nabijheid van andere apparaten zoals mobiele telefoons en radio's met zender en ontvanger, een bepaalde mate van ruis hoorbaar zijn. In deze gevallen raden we u aan een of meer van de volgende stappen te ondernemen:

- Plaats het externe apparaat uit de buurt van de bron van de radio- of audiofrequentiesignalen.
- Leid de kabels van het externe apparaat weg van de bron van de radio- of audiofrequentiesignalen.
- Gebruik afgeschermd kabels voor het externe apparaat of gebruik kabels met een betere afscherming en connector.
- Maak de kabel van het externe apparaat korter.
- Plaats ferrieten of vergelijkbare oplossingen op de kabels van het externe apparaat.

Cisco kan geen garantie bieden voor de prestaties van externe apparaten, kabels en connectors.

**Voorzichtig**

In landen van de Europese Unie dient u alleen externe luidsprekers, microfoons en headsets te gebruiken die volledig voldoen aan de EMC-richtlijn [89/336/EEG].

Gegevens USB-poort

De Cisco IP-telefoons 8851, 8851NR, 8861, 8865 en 8865NR ondersteunen maximaal vijf apparaten die verbinding met elke USB-poort maken. Elk apparaat dat is verbonden met de telefoon, wordt meegeteld. Uw telefoon kan bijvoorbeeld vijf USB-apparaten op de poort aan de zijkant en vijf extra standaard USB-apparaten op de poort aan de achterkant ondersteunen. Veel USB-producten van derden tellen als meerdere USB-apparaten: een apparaat dat bijvoorbeeld een USB-hub en -hoofdtelefoon bevat, kan worden geteld als twee USB-apparaten. Zie de documentatie over USB-apparaten voor meer informatie.

**Opmerking**

- Hubs zonder voeding worden niet ondersteund en hubs met voeding met meer dan vier poorten worden niet ondersteund.
- USB-hoofdtelefoons die verbinding maken met de telefoon via een USB-hub worden niet ondersteund.

Elke toetsuitbreidingsmodule die verbinding maakt met de telefoon, telt als een USB-apparaat. Als er drie toetsuitbreidingsmodules met de telefoon zijn verbonden, worden deze geteld als drie USB-apparaten.

Configuratiebestanden telefoon

Configuratiebestanden voor een telefoon worden opgeslagen op de TFTP-server en definiëren de parameters voor het maken van verbinding met Cisco Unified Communications Manager. Als u een wijziging aanbrengt in Cisco Unified Communications Manager die vereist dat de telefoon wordt gereset, wordt de wijziging in het algemeen automatisch aangebracht in het telefoonconfiguratiebestand.

Configuratiebestanden bevatten ook informatie over welke geladen afbeelding de telefoon moet uitvoeren. Als deze geladen afbeelding afwijkt van de huidige op een telefoon, maakt de telefoon contact met de TFTP-server om de vereiste laadbestanden aan te vragen.

Als u de beveiligingsinstellingen configureert in Cisco Unified Communications Manager Administration, bevat het telefoonconfiguratiebestand vertrouwelijke informatie. Om te zorgen voor de privacy van een configuratiebestand moet u dit configureren voor codering. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager. Een telefoon vraagt een configuratiebestand aan wanneer deze wordt gereset en geregistreerd met Cisco Unified Communications Manager.

Een telefoon opent het standaardconfiguratiebestand XmlDefault.cnf.xml van de TFTP-server wanneer aan de volgende voorwaarden is voldaan:

- U hebt autoregistratie ingeschakeld in Cisco Unified Communications Manager
- De telefoon is niet toegevoegd aan de Cisco Unified Communications Manager-database
- De telefoon wordt voor het eerst geregistreerd

Verwante onderwerpen

[Cisco Unified Communications Manager Documentatie](#)

Telefoongedrag tijdens netwerkcongestie

Alle factoren die de netwerkprestaties verslechteren, kunnen invloed hebben op de audio- en videokwaliteit van de telefoon. In sommige gevallen kan een gesprek zelfs wegvallen. Bronnen van netwerkverslechtering zijn onder andere de volgende activiteiten:

- Beheertaken, zoals een interne poortscan of een beveiligingsscan.
- Aanvallen die zich voordoen op uw netwerk, zoals een Denial of Service-aanval.

Het gedrag van de telefoon op een netwerk met twee netwerkrouers

De Cisco IP-telefoon 8800-serie maakt gebruik van een firewall om bescherming te bieden tegen cybergevaaren, zoals man-in-the-middle-aanval Deze firewall kan niet worden uitgeschakeld. Maar de firewall kan het verkeer

op een telefoon stoppen, als uw netwerk is geconfigureerd met twee netwerkroueters in hetzelfde subnet en met IP-omleiding.

De telefoonfirewall stopt verkeer omdat deze netwerkinstelling vergelijkbaar met een man-in-the-middle-aanval. De telefoon ontvangt omleidingspakketten voor andere bestemmings-IP's in een ander subnet van de telefoon. De telefoon bevindt zich op een netwerk met meerdere routers en de standaardrouter verzendt verkeer naar een tweede router.

Bekijk de logboeken als u vermoedt dat de firewall verkeer tegenhoudt. Zoek naar een foutcode 1-melding van het besturingssysteem wanneer dit probeert een verbinding tot stand te brengen. Een van de handtekeningen is

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

Een netwerk met twee netwerkroueters in hetzelfde subnet en IP-omleiding is niet een algemene configuratie. Als u deze netwerkinstellingen gebruikt, kunt u overwegen om slechts één router op een subnet te gebruiken. Maar als u twee netwerkroueters nodig hebt op hetzelfde subnet, schakel dan de IP-omleiding uit op de router en start de telefoon opnieuw.

Application Programming Interface

Cisco ondersteunt het gebruik van telefoon-API's door toepassingen van andere fabrikanten die via Cisco door de toepassingsontwikkelaar van de andere fabrikant zijn getest en gecertificeerd. Alle telefoonproblemen die verband houden met niet-gecertificeerde toepassingsinteractie, moeten door de andere fabrikant worden opgelost, dus niet door Cisco.

Raadpleeg de website van het [Cisco Solution Partner Program](#) voor meer informatie over toepassingen/oplossingen van andere fabrikanten die door Cisco zijn gecertificeerd.

Over de vertaling

Cisco biedt voor sommige gebieden lokalisatie aan voor deze content. De vertalingen worden echter alleen aangeboden ter informatie. Als er sprake is van inconsistentie, heeft de Engelse versie van de content de voorkeur.