VoIP-netwerken

Netwerkvereisten

Voor een succesvolle werking van de telefoon als een eindpunt in uw netwerk moet uw netwerk aan de volgende vereisten voldoen:

- VoIP-netwerk
  - VoIP is geconfigureerd op uw Cisco-routers en -gateways.
  - Cisco Unified Communications Manager is in uw netwerk geïnstalleerd en geconfigureerd voor het uitvoeren van gespreksverwerking.
- IP-netwerk dat DHCP of de handmatige toewijzing van IP-adres, gateway en subnetmasker ondersteunt

Opmerking De telefoon toont de datum en het tijdstip van de Cisco Unified Communications Manager. Als de gebruiker **Automatische datum en tijdstip** in de app Instellingen uitschakelt, is het tijdstip mogelijk niet langer gesynchroniseerd met de servertijd.

Netwerkprotocollen

De Cisco draadloze IP-telefoon 8821 en 8821-EX ondersteunt diverse industriestandaardprotocollen 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 1: Ondersteunde netwerkprotocollen

Netwerkprotocol	Doel	Opmerkingen over gebruik
Bluetooth	Bluetooth is een draadloos persoonlijk netwerk-protocol (WPAN) dat aangeeft hoe apparaten over korte afstand communiceren.	De telefoons ondersteunen Bluetooth 4.0.
Bootstrap Protocol (BootP)	BootP schakelt een netwerkapparaat, zoals Cisco IP-telefoon, in om bepaalde opstartgegevens te detecteren, zoals het IP-adres.	Geen
Cisco Audio Session Tunnel (CAST)	Het CAST-protocol stelt Cisco IP-telefoons en bijbehorende toepassingen in staat om externe IP-telefoons te detecteren en daarmee te communiceren zonder wijzigingen te vereisen in de traditionele signaleringscomponenten zoals Cisco Unified Communications Manager (CM) en gateways.	De telefoons gebruiken CAST als een interface tussen CUVA en de Cisco Unified Communications Manager met de 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.	De telefoons gebruiken CDP voor de communicatie van informatie zoals de hulp-VLAN-id, voedingsbeheerdetails per poort en QoS-configuratiegegeven (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.
Dynamic Host Configuration Protocol (DHCP)	DHCP wijst een IP-adres dynamisch toe aan netwerkapparaten. 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.	DHCP is standaard ingeschakeld. Als DHCP is uitgeschakeld, moet u het IP-adres, subnetmasker, gateway en TFTP-server lokaal handmatig op elke telefoon configureren. We adviseren om de aangepaste DHCP-optie 150 te gebruiken. Met deze methode configureert u het IP-adres van de TFTP-server als de optiewaarde. Voor meer informatie raadpleegt u de documentatie bij uw specifieke versie van Cisco Unified Communications Manager. **Opmerking** Als u de optie 150 niet kunt gebruiken, kunt u het proberen met de DHCP-optie 66.
Hypertext Transfer Protocol (HTTP)	HTTP is de standaardmanier voor informatie-overdracht en het verplaatsen van documenten over internet en het web.	De telefoons gebruiken HTTP voor XML-services en probleemoplossing.

Netwerkprotocol	Doel	Opmerkingen over gebruik
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. Telefoons die HTTPS ondersteunen, kiezen de HTTPS-URL.
IEEE 802,1X	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. 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.	De telefoons implementeren de IEEE 802.1X-standaard door ondersteuning te bieden voor de volgende verificatiemethoden: • EAP-FAST • EAP-TLS • PEAP-GTC • PEAP-MSCHAPV2
IEEE 802.11n/802.11ac	De IEEE 802.11-standaard geeft aan hoe apparaten communiceren via een draadloos LAN-netwerk (WLAN).	802.11n werkt binnen de 2.4 GHz- en 5 GHz-band. 802.11ac werkt binnen de 5 GHz-band.
Internet Protocol (IP)	IP is een berichtprotocol dat pakketten adresseert en verzendt via het netwerk.	Als netwerkapparaten willen communiceren met IP, moeten ze een toegewezen IP-adres, subnet en gateway hebben. IP-adressen, subnetten en gateway-id's worden automatisch toegewezen als u de telefoon gebruikt met Dynamic Host Configuration Protocol (DHCP). Als u DHCP niet gebruikt, moet u deze eigenschappen lokaal handmatig aan elke telefoon toewijzen. De telefoons bieden geen ondersteuning voor IPv6.
Real-Time Transport Protocol (RTP)	RTP is een standaardprotocol voor het transporteren van real-time gegevens, zoals interactieve spraak via gegevensnetwerken.	De 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.
Transmission Control Protocol (TCP)	TCP is een verbindingsgericht transportprotocol.	De telefoons gebruiken TCP om verbinding te maken met Cisco Unified Communications Manager en toegang te krijgen tot XML-services.
Transport Layer Security (TLS)	TLS is een standaardprotocol voor het beveiligen en verifiëren van communicatie.	Bij de implementatie van de beveiliging gebruiken de 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 door de telefoons gebruikt voor de signalering.

Verwante onderwerpen

Het telefoonnetwerk handmatig instellen vanaf het menu Instellingen
Interactie Cisco Unified Communications Manager, op pagina 14
802.11-standaarden voor WLAN-communicatie, op pagina 9
Opstartsequentie

Implementatiehandleiding voor Cisco draadloze IP-telefoon 882x

De *implementatiehandleiding Cisco draadloze IP-telefoon 882x* bevat nuttige informatie over de draadloze telefoon in de Wi-Fi-omgeving. U vindt de implementatiehandleiding op de volgende locatie:

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

Draadloos LAN

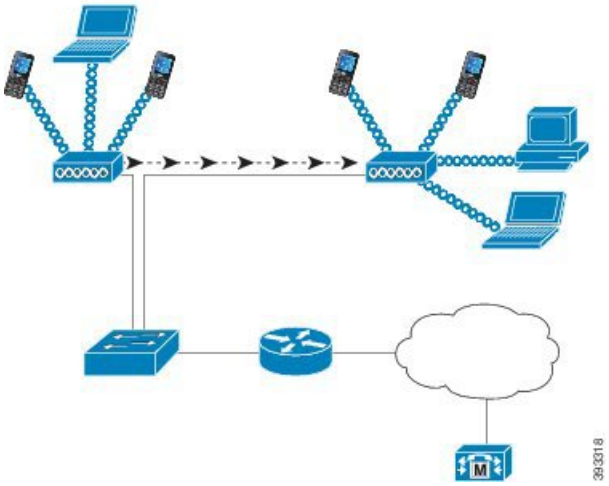
Opmerking Voor gedetailleerde Cisco draadloze IP-telefoon 8821 en 8821-EX implementatie- en configuratie-instructies, zie de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

Apparaten met een draadloze functionaliteit kunnen spraakcommunicatie binnen de WLAN van het bedrijf voorzien. Het apparaat is afhankelijk van en zorgt voor interactie met draadloze toegangspunten (AP) en belangrijke Cisco IP-telefoniecomponenten, inclusief Cisco Unified Communications Manager beheer, om een draadloze spraakcommunicatie te voorzien.

De draadloze telefoons hebben Wi-Fi-capaciteiten die 802.11a, 802.11b, 802.11g, en 802.11n Wi-Fi kunnen gebruiken.

De volgende afbeelding toont een typische WLAN-topologie die de draadloze overdracht van spraak voor draadloze IP-telefonie mogelijk maakt.

Figuur 1: Typische WLAN-topologie



Wanneer een telefoon wordt ingeschakeld, zoekt hij naar en wordt hij gekoppeld aan een AP als de draadloze toegang tot het apparaat is ingesteld op Aan. Als opgeslagen netwerken niet binnen het bereik liggen, kunt u een uitgezonden netwerk selecteren of handmatig een netwerk toevoegen.

Het AP gebruikt de verbinding met het bekabelde netwerk om gegevens en spraakpakketten van en naar de switches en routers te sturen. De spraaksignalen worden naar de gespreksbeheerserver overgedragen voor de verwerking en routering van gesprekken.

AP'sz zijn essentiële componenten in een WLAN aangezien ze voor de draadloze koppelingen of hotspots voor het netwerk zorgen. In sommige WLAN's heeft elke AP een bekabelde verbinding met een ethernetswitch zoals een Cisco Catalyst 3750 die op een LAN is geconfigureerd. De switch biedt toegang tot gateways en de gespreksbeheerserver om de draadloze IP-telefonie te ondersteunen.

Sommige netwerken bevatten bekabelde componenten die draadloze componenten ondersteunen. De bekabelde componenten kunnen switches, routers en bruggen met speciale modules voor de draadloze mogelijkheden bevatten.

Voor meer informatie over draadloze Cisco Unified-netwerken, zie https://www.cisco.com/c/en/us/products/wireless/index.html.

Wi-Fi-netwerkcomponenten

De telefoon moet met verschillende netwerkcomponenten in de WLAN communiceren om succesvol gesprekken te kunnen voeren en ontvangen.

AP-kanaal- en -domeinrelaties

Toegangspunten (AP's) verzenden en ontvangen RF-signalen via kanalen binnen de frequentieband van 2.4 GHz of 5 GHz. Om een stabiele draadloze omgeving te voorzien en om de kanaalinterferentie te beperken, moet u voor elke AP niet-overlappende kanalen opgeven.

Voor meer informatie over de AP-kanaal- en -domeinrelaties, zie het deel “De draadloze LAN voor spraak ontwerpen” in de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

AP-interacties

Draadloze telefoons gebruiken dezelfde AP's als draadloze gegevensapparaten. Spraakverkeer via een WLAN vereist echter andere uitrustingsconfiguraties en -indelingen dan een WLAN die uitsluitend voor gegevensverkeer wordt gebruikt. Gegevensverkeer kan een hoger RF-geluidsniveau, pakketverlies en kanaalconflicten verdragen dan een spraakoverdracht. Pakketverlies tijdens de spraakoverdracht kan tot schokkerige of defecte audio leiden en kan het gesprek onhoorbaar maken. Pakketfouten kunnen ook tot blokkerige of bevroren video leiden.

Gebruikers van mobiele telefoons zijn mobiel en zwerven vaak doorheen een campus of tussen verdiepingen in een gebouw terwijl ze in gesprek zijn. Gebruikers van gegevens blijven daarentegen op één plaats of verplaatsen zich soms naar een andere locatie. De mogelijkheid om te roamen tijdens een gesprek is een van de voordelen van draadloze spraak. De RF-dekking moet dus trappen, liften, stille hoeken buiten conferentieruimtes en gangen omvatten.

Om een goede spraakkwaliteit en een optimale RF-signaaldekking te garanderen, moet u een siteonderzoek uitvoeren. Het siteonderzoek bepaalt de instellingen die geschikt zijn voor de draadloze spraak en helpt bij het ontwerp en de lay-out van de WLAN; bijvoorbeeld plaatsing van het AP, vermogensniveaus en kanaaltoewijzingen.

Na de implementatie en het gebruik van draadloze spraak moet siteonderzoeken na de installatie blijven uitvoeren. Wanneer u een groep nieuwe gebruikers toevoegt, meer uitrustingen installeert of grote hoeveelheden inventaris verzamelt, wijzigt u de draadloze omgeving. Een onderzoek na de installatie controleert of de AP-dekking nog steeds geschikt is voor optimale spraakcommunicatie.

Opmerking Pakketverlies komt voor tijdens het roamen; de beveiligingsmodus en de aanwezigheid van snelle roaming bepalen echter hoeveel pakketten er tijdens de overdracht verloren gaan. Cisco raadt de implementatie van Cisco Centralized Key Management (CCKM) aan om een snelle roaming mogelijk te maken.

Voor veer informatie over de QoS van de spraak in een draadloos netwerk, zie de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

Koppeling toegangspunt

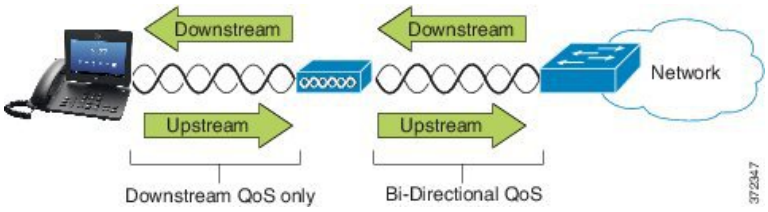
Bij het opstarten scant de telefoon voor AP's met SSID's en coderingstypes die worden herkend. De telefoon onderhoudt een lijst met geschikte AP's en selecteert het beste AP op basis van de huidige configuratie..

Servicekwaliteit in een draadloos netwerk

Spraak- en videoverkeer op het draadloze LAN is net als gegevensverkeer vatbaar voor vertraging, jitter en pakketverlies. Deze problemen hebben geen invloed op de eindgebruiker van de gegevens, maar kunnen een spraak- of videogesprek wel ernstig beïnvloeden. Om te garanderen dat het spraak- en videoverkeer tijdig en betrouwbaar wordt behandeld met een geringe vertraging en jitter, moet u Quality of Service (QoS) gebruiken.

Door de apparaten in een spraak-VLAN te scheiden en spraakpakketten met hogere QoS te markeren, kunt u ervoor zorgen dat het spraakverkeer prioriteit krijgt boven gegevensverkeer. Dit leidt tot een geringere pakketvertragingen en minder pakketverliezen.

In tegenstelling tot bekabelde netwerken met specifieke bandbreedtes beschouwen draadloze LAN's de richting van het verkeer bij de implementatie van QoS. Het verkeer wordt geclassificeerd als upstream of downstream ten opzichte van het AP, zoals in de onderstaande afbeelding wordt weergegeven.



Het QoS-type Enhanced Distributed Coordination Function (EDCF) heeft tot acht wachtrijen voor downstream-QoS (richting de 802.11b/g clients). U kunt de wachtrijen toewijzen op basis van deze opties:

- Instellingen voor QoS of Differentiated Services Code Point (DSCP) voor de pakketten
- Toegangslijsten met Layer 2 of Layer 3
- VLAN's voor specifiek verkeer
- Dynamische registratie van apparaten

Hoewel er tot 8 wachtrijen op het AP kunnen worden ingesteld, is het aangeraden om er slechts drie te gebruiken voor spraak, video en signaalverkeer om de best mogelijke QoS te garanderen. Plaats spraak in de spraakwachtrij (UP6), video in de videowachtrij (UP5), signaalverkeer (SIP) in de videowachtrij (UP4) en gegevensverkeer in een best-effortwachtrij (UP0). Hoewel 802.11b/g EDCF niet garandeert dat het spraakverkeer tegen het gegevensverkeer wordt beschermd, zou u met dit wachtrijmodel de beste statistische resultaten moeten krijgen.

De wachtrijen zijn:

- Best Effort (BE) - 0, 3
- Achtergrond (BK) - 1, 2
- Video (VI) - 4, 5
- Spraak (VO) - 6, 7

Opmerking Het apparaat markeert de SIP-signaalpakketten met een DSCP-waarde van 24 (CS3) en RTP-pakketten met een DSCP-waarde van 46 (EF).

Opmerking Gesprekbeheer (SIP) wordt verzonden als UP4 (VI). Video wordt verzonden als UP5 (VI) wanneer Admission Control Mandatory (ACM) is uitgeschakeld voor video (Traffic Specification [TSpec] uitgeschakeld). Spraak wordt verzonden als UP6 (VO) wanneer ACM is uitgeschakeld voor spraak (TSpec uitgeschakeld).

De volgende tabel geeft een QoS-profiel op het AP dat prioriteit geeft aan spraak-, video- en gespreksbeheerverkeer.

Tabel 2: QoS-profiel- en interface-instellingen

Verkeerstype	DSCP	802.1p	WMM UP	Poortbereik
Spraak	EF (46)	5	6	UDP-16384-32767
Interactieve video	AF41 (34)	4	5	UDP-16384-32767
Gespreksbeheer	CS3 (24)	3	4	TCP 5060-5061

Om de betrouwbaarheid van spraakoverdrachten in een niet-deterministische omgeving te verbeteren, ondersteunt het apparaat de industriële standaard IEEE 802.11e en is het geschikt voor Wi-Fi Multimedia (WMM). WMM maakt gedifferentieerde services voor spraak-, video-, best-effortgegevens- en ander verkeer mogelijk. Opdat deze gedifferentieerde services voldoende QoS voor spraakpakketten voorziet, kan slechts een bepaalde bandbreedte tegelijkertijd op een kanaal worden onderhouden of toegestaan. Als het netwerk “N” spraakoproepen met een gereserveerde bandbreedte kan verwerken, wanneer de hoeveelheid van het spraakverkeer boven deze limiet stijgt (tot N+1 gesprekken), lijdt de kwaliteit van alle gesprekken hieronder.

Om problemen met de gesprekskwaliteit op te lossen, is een initieel Call Admission Control-schema (CAC) vereist. Wanneer SIP CAC op de WLAN is ingeschakeld, wordt de QoS in een netwerkoverbelastingssituatie behouden door het aantal actieve spraakgesprekken te beperken zodat de configureerde limieten op het AP niet worden overschreden. Tijdens een verstopping van het netwerk behoudt het systeem een kleine bandbreedtereserve zodat clients van draadloze apparaten naar een naburige AP kunnen bewegen, zelfs wanneer de AP aan zijn “volledige capaciteit werkt.” Nadat de limiet van de spraakbandbreedte is bereikt, wordt het volgende gesprek gebalanceerd op een naburig AP geladen zodat de kwaliteit van de bestaande gesprekken op het kanaal niet wordt beïnvloed.

De telefoons gebruiken TCP voor SIP-communicatie en de registraties van het gespreksbeheersysteem kunnen mogelijk verloren gaan als een AP op volledige capaciteit werkt. Frames van of naar een client die niet via de CAC is "geautoriseerd", kunnen worden verwijderd waardoor de registratie van het gespreksbeheersysteem wordt geannuleerd. Daarom raden wij aan om SIP CAC uit te schakelen.

Flexibele DSCP instellen

Procedure

Stap 1 Ga in Cisco Unified Communications Manager Administration naar **Systeem** > **Serviceparameters**.

Stap 2 Stel in de Clusterparameters (Systeem - Locatie en regio) Bandbreedtepool voor immersieve videogesprekken in op **False**.

Stap 3 Stel in de Clusterparameters (Call Admission Control) QoS-markering videogesprek in op **Promoten naar immersief**.

Stap 4 Sla uw wijzigingen op.

802.11-standaarden voor WLAN-communicatie

Draadloze LAN's moeten de 802.11-standaarden van het Institute of Electrical and Electronics Engineers (IEEE) volgen die de protocollen definiëren die al het draadloze verkeer op basis van ethernet regelen. De draadloze telefoons ondersteunen de volgende standaarden:

- 802.11a: gebruikt de 5 GHz-band die meer kanalen en verbeterde datasnelheden voorziet door de OFDM-technologie te gebruiken. De Dynamic Frequency Selection (DFS) en Transmit Power Control (TPC) ondersteunen deze standaard.
- 802.11b: specificeert de radiofrequentie (RF) van 2,4 Ghz voor zowel de overdracht als de ontvangst van gegevens bij lagere gegevenssnelheden (1, 2, 5.5, 11 Mbps).
- 802.11d: hiermee kunnen toegangspunten hun momenteel ondersteunde radiokanalen en overdrachtsvermogensniveaus. De 802.11d-client gebruikt die informatie vervolgens om de te gebruiken kanalen en vermogens te bepalen. De telefoon vereist de Wereldmodus (802.11d) om te bepalen welke kanelen wettelijk voor een bepaald land zijn toegestaan. Zie de onderstaande tabel voor de ondersteunde kanalen. Zorg ervoor dat 802.11d correct is geconfigureerd op de Cisco IOS-toegangspunten of Cisco Unified Wireless LAN-controller.
- 802.11e: definieert een reeks verbeteringen aan de Quality of Service (QoS) voor draadloze LAN-toepassingen.
- 802.11g: gebruikt dezelfde niet-gelicentieerde 2.4 Ghz-band als 802.11b, maar breidt de gegevenssnelheden uit om betere prestaties te leveren door gebruik te maken van de Orthogonal Frequency Division Multiplexing-technologie (OFDM). OFDM is een coderingstechnologie voor de overdracht van signalen door middel van RF.
- 802.11h: ondersteunt het 5 GHz-spectrum en overdrachtsvermogensbeheer. Biedt DFS en TPC aan de 802.11a Media Access Control (MAC).
- 802.11i: specificeert beveiligingsmechanismen voor draadloze netwerken.
- 802.11n: gebruikt de radiofrequentie van 2,4 GHz of 5 GHz voor zowel de overdracht als de ontvangst van gegevens met snelheden tot 150 Mbps en verbetert de gegevensoverdracht door gebruik te maken van de technologie met meerdere ingangen en meerdere uitgangen (MIMO), kanaalverbinding en payloadoptimalisering.

Opmerking De draadloze telefoons hebben een enkele antenne en gebruiken het systeem met enkele ingang en enkele uitgang (SISO) dat alleen MCS 0- tot MCS 7-gegevenssnelheden ondersteunt (72 Mbps met 20 MHz-kanalen en 150 Mbps met 40 MHz-kanalen). U kunt ook MCS 8 tot MCS 15 inschakelen als 802.11n-clients de MIMO-technologie gebruiken die voordeel kunnen halen uit deze hogere gegevenssnelheden.

- 802.11r: specificeert de vereisten voor een snelle en veilige roaming.
- 802.11ac: gebruikt de radiofrequentie van 5 GHz voor zowel de overdracht als de ontvangst van gegevens met snelheden tot 433 Mbps.

Tabel 3: Ondersteunde kanalen

Bandbereik	Beschikbare kanalen	Kanaal ingesteld	Kanaalbreedte
2,412 - 2,484 GHz	13	1 - 13	20 MHz
5,180 - 5,240 GHz	4	36, 40, 44, 48	20, 40, 80 MHz
5,260 - 5,320 GHz	4	52, 56, 60, 64	20, 40, 80 MHz
5. 500 - 5,700 GHz	11	100 - 140	20, 40, 80 MHz
5,745 - 5,825 GHz	5	149, 153, 157, 161, 165	20, 40, 80 MHz

Opmerking De kanalen 120, 124, 128 worden niet ondersteund in het Amerikaanse continent, Europa of Japan, maar mogelijk wel in andere regio's in de wereld.

Voor meer informatie over de ondersteunde gegevenssnelheden, Tx-kracht en Rx-gevoeligheid voor WLAN's, zie de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

Wereldmodus (802.11d)

De draadloze telefoons gebruiken 802.11d om te bepalen welke kanalen en overdrachtsniveaus moeten worden gebruikt. De telefoon neemt de clientconfiguratie over van het gekoppelde AP. Schakel de Wereldmodus (802.11d) ohet AP in om de telefoon in Wereldmodus te gebruiken.

Opmerking De inschakeling van de Wereldmodus (802.11d) is mogelijk niet nodig als de frequentie 2.4 GHz is en het huidige toegangspunt op een kanaal van 1 tot 11 verzendt.

Aangezien alle landen deze frequenties ondersteunen, kunt u proberen om deze kanalen te scannen, ongeacht de ondersteuning van de Wereldmodus (802.11d).

Voor meer informatie over de inschakeling van de Wereldmodus en de ondersteuning van 2.4 Ghz, zie de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

Schakel de Wereldmodus (802.11d) in voor het overeenkomstige land waarin het toegangspunt zich bevindt. De Wereldmodus is automatisch ingeschakeld voor de Cisco Unified Wireless LAN Controller.

Radiofrequentiebereiken

WLAN-communicaties gebruiken de volgende radiofrequentiebereiken (RF):

- 2.4 GHz: veel apparaten die 2.4 GHz gebruiken, kunnen de 802.11b/g-verbinding verstoren. De interferentie kan een Denial of Service-scenario (DoS) veroorzaken. Hierdoor kunnen succesvolle 802.11-transmissies worden vermeden.
- 5 GHz: dit bereik wordt verdeeld in verschillende secties, de zogenaamde Unlicensed National Information Infrastructure-banden (UNII). Elke band heeft vier kanalen. De kanalen hebben een tussenruimte van 20 MHz om niet-overlappende kanalen aan te bieden en meer kanalen te hebben dan 2.4 GHz.

Beveiliging voor communicatie in WLAN's

Omdat alle WLAN-apparaten die binnen het bereik zijn al het andere WLAN-verkeer kunnen ontvangen, is de beveiliging van spraakcommunicatie van cruciaal belang in WLAN's. Om ervoor te zorgen dat indringers het spraakverkeer niet manipuleren of onderscheppen, ondersteunt de Cisco SAFE Security-architectuur de draadloze telefoons en de Cisco Aironet-toegangspunten. Voor meer informatie over de beveiliging in netwerken, zie https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html.

Verificatiemethodes

De Cisco Wireless IP-telefonieoplossing biedt draadloze netwerkbeveiliging die ongeautoriseerde aanmeldingen en verstoorde communicatie voorkomt door de volgende verificatiemethodes die door de draadloze telefoons worden ondersteund:

- WLAN-verificatie
  - WPA (802.1x-verificatie + TKIP- of AES-codering)
  - WPA2 (802.1x-verificatie + AES- of TKIP-codering)
  - WPA-PSK (vooraf gedeelde sleutel + TKIP-codering)
  - WPA2-PSK (vooraf gedeelde sleutel + AES-codering)
  - EAP-FAST (Extensible Authentication Protocol – Flexible Authentication via Secure Tunneling)
  - EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
  - PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 en GTC
  - CCKM (Cisco Centralized Key Management)
  - Open (geen)
- WLAN-codering

- AES (Advanced Encryption Scheme)
- TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
- WEP (Wired Equivalent Protocol) 40/64 en 104/128 bit

Opmerking Dynamische WEP met 802.1x-verificatie en verificatie met gedeelde sleutel worden niet ondersteund.

Voor meer informatie over verificatiemethodes, zie het gedeelte “Draadloze beveiliging” in de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

Verificatiesleutelbeheer

De volgende verificatieschema's gebruiken de RADIUS-server om verificatiesleutels te beheren:

- WPA/WPA2: gebruikt RADIUS-serverinformatie voor het genereren van unieke sleutels voor de verificatie. Omdat deze sleutels op de centrale RADIUS-server zijn gegenereerd, biedt WPA/WPA2 betere beveiliging dan de vooraf gedeelde WPA-sleutels die op het AP en het apparaat zijn opgeslagen.
- Cisco Centralized Key Management (CCKM): gebruikt de RADIUS-server en de gegevens van een draadloze domeinserver (WDS) voor het beheren en verifiëren van sleutels. De WDS maakt een cache met veiligheidsgegevens voor clientapparaten met CCKM-ondersteuning voor snelle en beveiligde verificatie.

Met WPA/WPA2 en CCKM worden coderingssleutels niet ingevoerd op het apparaat, maar automatisch afgeleid tussen het toegangspunt en het apparaat. Maar de EAP-gebruikersnaam en het wachtwoord die worden gebruikt voor de verificatie, moeten op elk apparaat worden ingevoerd.

Coderingsmethodes

Om ervoor te zorgen dat spraakverkeer veilig is, ondersteunen de draadloze telefoons de standaarden WEP, TKIP en AES (Advanced Encryption) voor codering. Als deze mechanismen voor de codering worden gebruikt, worden Real-Time Transport Protocol (RTP) spraakpakketten gecodeerd tussen het toegangspunt en het apparaat.

WEP

Als WEP in het draadloze netwerk wordt gebruikt, vindt de verificatie plaats via open of gedeelde sleutelverificatie op het toegangspunt. De WEP-sleutel die op de telefoon is ingesteld, moet voor geslaagde verbindingen overeenkomen met de WEP-sleutel die is geconfigureerd op het toegangspunt. De telefoons ondersteunen WEP-sleutels die gebruikmaken van 40-bits of 128-bits codering en blijven ongewijzigd op het apparaat en het toegangspunt.

TKIP

WPA en CCKM werken met TKIP-codering die verschillende verbeteringen heeft ten opzichte van WEP. TKIP biedt sleutelcodering per pakket en langere initialisatievectoren (IV's) die de codering versterken. Bovendien zorgt een Message Integrity Check (MIC) ervoor dat gecodeerde pakketten niet worden gewijzigd. TKIP voorkomt de voorspelbaarheid van WEP waarmee indringers de WEP-sleutel decoderen.

AES

Een coderingsmethode die wordt gebruikt voor WPA2-verificatie. Deze nationale standaard voor codering gebruikt een symmetrisch algoritme dat dezelfde sleutel voor codering en decodering heeft.

Voor meer informatie over coderingsmethodes, zie het gedeelte “Draadloze beveiliging” in de *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie*.

Verificatie- en coderingsopties voor AP

Verificatie en coderingschema's worden ingesteld binnen het draadloze LAN-netwerk. VLAN's zijn geconfigureerd in het netwerk en op de toegangspunten en geven verschillende verificatie- en coderingscombinaties. Een SSID wordt gekoppeld aan een VLAN en het specifieke verificatie- en coderingsschema. Voor een geslaagde verificatie van draadloze telefoons moet u dezelfde SSID's configureren met de verificatie- en coderingschema's op de toegangspunten en op de telefoon.

Opmerking

- Wanneer u vooraf gedeelde WPA-sleutels of vooraf gedeelde WPA2-sleutels gebruikt, moet de vooraf gedeelde sleutel statisch zijn ingesteld op de telefoon. Deze sleutels moeten overeenkomen met de sleutels op het toegangspunt.
- De draadloze telefoons bieden geen ondersteuning voor automatische EAP-onderhandeling. Als u de EAP-FAST-modus wilt gebruiken, moet u deze opgeven.

De volgende tabel bevat een lijst met verificatie- en coderingschema's die zijn geconfigureerd op de Cisco Aironet-toegangspunten die door de telefoons worden ondersteund. De tabel geeft de netwerkconfiguratie-optie weer voor het appaaat die met de toegangspuntconfiguratie overeenkomt.

Tabel 4: Verificatie- en coderingschema's

Cisco WLAN-configuratie			**Telefoonconfiguratie**
Verificatie	**Sleutelbeheer**	**Algemene codering**	**Verificatie**
Openen	Geen	Geen	Geen
Statisch WEP	Geen	WEP	WEP
EAP-FAST	WPA of WPA2 met optionele CCKM	TKIP of AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA of WPA2 met optionele CCKM	TKIP of AES	802.1x EAP > PEAP > MSCHAPV2
PEAP-GTC	WPA of WPA2 met optionele CCKM	TKIP of AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA of WPA2 met optionele CCKM	TKIP of AES	802.1 x EAP > TLS
WPA/WPA2-PSK	WPA-PSK of WPA2-PSK	TKIP of AES	WPA/WPA2 PSK

Raadpleeg *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie* voor meer informatie.

Certificaten

De telefoons ondersteunen de volgende certificaten.

- X.509 digitaal certificaat voor EAP-TLS of voor het inschakelen van PEAP + servervalidatie voor WLAN-verificatie
- Simple Certificate Enrollment Protocol (SCEP) voor registratie en automatisch vernieuwen van certificaten
- 1024, 2048, 4096 bits
- Handtekeningstypen SHA-1 en SHA-256
- Coderingstypen DER en Base-64 (PEM)
- Door de gebruiker geïnstalleerd certificaat in PKCS #12-indeling (.p12- of .pfx-extensie), dat ook de persoonlijke sleutel bevat
- Servercertificaat (Root CA) met .crt- of .cer-extensie

U kunt op één van de volgende manieren certificaten installeren op uw telefoon:

- Met de Beheer-webpagina. Zie Beheerpagina Cisco IP-telefoon voor meer informatie.
- Met een SCEP-server voor het beheren en installeren van certificaten. Voor meer informatie zie SCEP instellen

Als uw gebruikers hun telefoons zelf instellen en ze hebben certificaten nodig voor hun telefoons, dient u hen het type van het certificaat te geven, samen met de andere configuratie-instellingen. Als u geen SCEP gebruikt voor het installeren van certificaten, dan dient u de certificaten zelf te installeren.

WLAN's en roaming

De draadloze telefoons ondersteunen Cisco Centralized Key Management (CCKM), een gecentraliseerd sleutelbeheerprotocol dat een cache met sessiereferenties op de draadloze domeinserver (WDS) voorziet.

Voor meer informatie over CCKM, zie de *Cisco-nota over een snelle en veilige roamingtoepassing* op:

http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_technical_reference09186a00801c5223.html

De telefoons ondersteunen ook 802.11r. Raadpleeg *Implementatiehandleiding Cisco draadloze IP-telefoons 8821-serie* voor meer informatie.

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.

Interactie Voicemailsysteem

In Cisco Unified Communications Manager kunt u verschillende voicemailsystemen integreren, met inbegrip van het Cisco Unity Connection voicemailsysteem. 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.
- 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.

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.