VoIP-Netzwerke

Netzwerkanforderungen

Damit das Telefon als Endpunkt im Netzwerk funktioniert, muss das Netzwerk die folgenden Anforderungen erfüllen:

- VoIP-Netzwerk
  - VoIP ist auf Cisco Routern und Gateways konfiguriert.
  - Cisco Unified Communications Manager ist im Netzwerk installiert und konfiguriert, um Anrufe zu verarbeiten.
- IP-Netzwerk, das DHCP oder die manuelle Zuweisung von IP-Adresse, Gateway oder Subnetzmaske unterstützt.

Hinweis Das Telefon zeigt das Datum und die Uhrzeit von Cisco Unified Communications Manager an. Wenn der Benutzer die Option **Automatisches Datum und Uhrzeit** in der Anwendung „Einstellungen" ausschaltet, wird die Uhrzeit möglicherweise nicht mehr mit der Serverzeit synchronisiert.

Netzwerkprotokolle

Cisco schnurlos IP-Telefon 8821 und 8821-EX unterstützt verschiedene eigene und Industriestandard-konforme Netzwerkprotokolle, die für die Sprachkommunikation benötigt werden. Die folgende Tabelle enthält eine Übersicht der Netzwerkprotokolle, die von den Telefonen unterstützt werden.

Tabelle 1: Unterstützte Netzwerkprotokolle

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
Bluetooth	Bluetooth ist ein Kurzstrecken-Funkprotokoll (WPAN-Protokoll), das die Kommunikation zwischen Geräten über kurze Distanzen regelt.	Die Telefone unterstützen Bluetooth 4.0.
Bootstrap Protocol (BootP)	Mit BootP kann ein Netzwerkgerät, beispielsweise Cisco IP-Telefon, bestimmte Startinformationen (z. B. die IP-Adresse) abfragen.	Keine
Cisco Audio Session Tunnel (CAST)	Mit dem CAST-Protokoll können Cisco IP-Telefone und zugehörige Anwendungen entfernte IP-Telefone erkennen und mit diesen kommunizieren, ohne dass Änderungen an den herkömmlichen Komponenten zur Signalübertragung, beispielsweise dem Cisco Unified Communications Manager und den Gateways, erforderlich sind.	Die Telefone verwenden CAST als Schnittstelle zwischen CUVA und Cisco Unified Communications Manager mit Cisco IP-Telefone 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.	Die Telefone verwenden CDP, um Informationen, beispielsweise eine zusätzliche VLAN-ID, Details zur Energieverwaltung pro Port und QoS-Konfigurationsinformationen, mit dem Cisco Catalyst-Switch zu übertragen.
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.
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 benutzerdefinierte DHCP-Option 150 zu verwenden. Mit dieser Methode konfigurieren sie die IP-Adresse des TFTP- Servers als optionswert. 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.	Die Telefone nutzen HTTP für XML-Dienste und zur Fehlerbehebung.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
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. Die Telefone, 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 den Telefonen durch Unterstützung der Authentifizierungsmethoden: • EAP-FAST • EAP-TLS • PEAP-GTC • PEAP-MSCHAPV2
IEEE 802.11n/802.11ac	Der Standard IEEE 802.11 regelt die Kommunikation von Geräten in einem lokalen Funknetzwerk (WLAN).	802.11n funktioniert in den Bereichen 2,4 GHz und 5 GHz. 802.11ac funktioniert im Bereich 5 GHz.
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. IP-Adressen-, Subnetz- und Gateway-IDs werden automatisch zugewiesen, wenn Sie für das Telefon DHCP (Dynamic Host Configuration Protocol) nutzen. Wenn Sie DHCP nicht verwenden, müssen Sie diese Eigenschaften jedem Telefon manuell zuweisen. Die Telefone unterstützen IPv6 nicht.
Real-Time Transport Protocol (RTP)	RTP ist ein Protokoll zur Übertragung von Echtzeitdaten (z. B. interaktive Sprachübertragung) in Datennetzwerken.	Die Telefone verwenden das RTP-Protokoll zum Senden und Empfangen von Echtzeit-Sprachverkehrs an bzw. von anderen Telefonen und Gateways.
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.

Netzwerkprotokoll	Zweck	Anmerkungen zur Verwendung
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.
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.
Transmission Control Protocol (TCP)	TCP ist ein verbindungsorientiertes Transportprotokoll.	Die Telefone 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 die Telefone 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.	UDP wird von den Telefonen für die Signalisierung verwendet.

Verwandte Themen

Das Telefonnetzwerk manuell über das Einstellungsmenü konfigurieren
Cisco Unified Communications Manager-Interaktion, auf Seite 15
802.11-Standards für die WLAN-Kommunikation, auf Seite 9
Startsequenz

Anwendungsleitfaden für das Cisco schnurlos IP-Telefon 882x

Der *Anwendungsleitfaden für das Cisco schnurlos IP-Telefon 882x* enthält nützliche Informationen zum Schnurlostelefon in der Wi-Fi-Umgebung. Sie finden den Anwendungsleitfaden an diesem Speicherort:

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

Wireless LAN

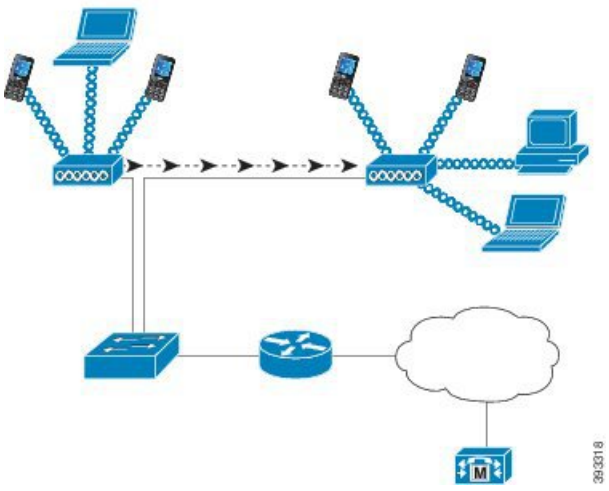
Hinweis Detaillierte Cisco schnurlos IP-Telefon 8821 und 8821-EX Bereitstellungs- und Konfigurationsanweisungen erhalten Sie unter *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

Geräte mit Wireless-Fähigkeit können Sprachkommunikation innerhalb des Unternehmens-WLANs bereitstellen. Das Gerät ist von drahtlosen Access Points (AP) und wichtigen Cisco IP Telephony-Komponenten abhängig, einschließlich Cisco Unified Communications Manager Administration zur Bereitstellung einer drahtlosen Sprachkommunikation.

Die Schnurlostelefone bieten Wi-Fi-Funktionen, die 802.11a, 802.11b, 802.11g, und 802.11n Wi-Fi verwenden können.

Die folgende Abbildung zeigt eine typische WLAN-Topologie, die eine drahtlose Übertragung von Sprache für drahtlose IP-Telefonielösungen ermöglicht.

Abbildung 1: Typische WLAN-Topologie



Wenn ein Telefon eingeschaltet wird, sucht es nach einem AP und wird diesem zugeordnet, falls der Wireless-Zugriff des Geräts auf Ein eingestellt ist. Wenn sich die gespeicherten Netzwerke nicht innerhalb der Reichweite befinden, können Sie eine Broadcast-Netzwerk auswählen oder ein Netzwerk manuell hinzufügen.

Der Access Point verwendet die Verbindung zum kabelgebundenen Netzwerk, um Daten- und Sprachpakete zu und von den Switches und Routern zu übertragen. Die Sprachsignalisierung wird an den Anrufsteuerungsserver zur Anrufverarbeitung und zum Routing übertragen.

APs sind wichtige Komponenten im WLAN, da sie die Wireless Links oder Hotspots zum Netzwerk bieten. Bei einigen WLANs hat jeder AP eine kabelgebundene Verbindung zu einem Ethernet-Switch, z. B. zu Cisco Catalyst 3750, der in einem LAN konfiguriert ist. Der Switch bietet Zugriff auf Gateways und auf den Anrufsteuerungsserver zur Unterstützung von drahtlosen IP-Telefonielösungen.

Einige Netzwerke enthalten kabelgebundene Komponenten, die drahtlose Komponenten zu unterstützen. Die verkabelten Komponenten können Switches, Router und Brücken mit speziellen Modulen, enthalten, die Wireless-Funktionen ermöglichen.

Weitere Informationen zu Cisco Unified Wireless Networks finden Sie unter https://www.cisco.com/c/en/us/products/wireless/index.html.

Wi-Fi-Netzwerkkomponenten

Das Telefon muss mit mehreren Netzwerkkomponenten im WLAN interagieren, um Anrufe erfolgreich zu tätigen und zu empfangen.

AP-Kanal- und Domänenbeziehungen

Access Points (APs) übertragen und empfangen HF-Signale über Kanäle im Frequenzbereich von 2,4 GHz bis 5 GHz. Um eine stabile drahtlose Umgebung bereitzustellen und Kanalstörungen zu reduzieren, müssen Sie die sich nicht überschneidenden Kanäle für jeden AP angeben.

Weitere Informationen zum AP-Kanal und zu Domänenbeziehungen erhalten Sie im Abschnitt „Wireless LAN für Sprache erstellen“ in *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

AP-Interaktionen

Schnurlostelefone verwenden dieselben APs wie drahtlose Datengeräte. Jedoch erfordert der Sprachverkehr über WLAN andere Konfigurationen und Layouts für Geräte als bei einem WLAN, das ausschließlich für den Datenverkehr verwendet wird. Eine Datenübertragung kann ein höheres Maß an Hochfrequenz-Rauschen, Paketverlusten und Kanalkonflikten tolerieren als eine Sprachübertragung. Ein Paketverlust während einer Sprachübertragung kann zu einem abgehackten und unterbrochenen Audio führen, sodass der Anruf nicht zu hören ist. Paketfehler können auch ein blockiertes oder eingefrorenes Video verursachen.

Benutzer von Schnurlostelefonen sind mobil und führen häufig ein Roaming auf einem Geländer oder zwischen Fluren in einem Gebäude durch, während sie mit einem Anruf verbunden sind. Im Gegensatz dazu bleiben Datenbenutzer an einem Ort oder wechseln gelegentlich an einen anderen Ort. Die Möglichkeit zum Roaming bei gleichzeitiger Beibehaltung des Anrufs ist einer der Vorteile von drahtlosen Sprachgeräten, daher muss die Funkfrequenzabdeckung Treppenhäuser, Aufzüge, ruhige Ecken außerhalb der Konferenzräume und Durchgänge umfassen.

Um eine gute Sprachqualität und eine optimale HF-Signalabdeckung sicherzustellen, müssen Sie eine Standortprüfung durchführen. Mit der Standortprüfung werden die Einstellungen bestimmt, die sich für drahtlose Sprachgeräte eignen sowie das Design und das Layout des WLAN unterstützen; z. B. AP-Platzierung, Leistungsstufen und Kanalzuordnungen.

Nach der Bereitstellung und Verwendung von drahtlosen Sprachgeräten, sollte Sie nach der Installation Standortprüfungen durchführen. Wenn Sie eine Gruppe von neuen Benutzern hinzufügen, weitere Geräte installieren oder große Mengen an Bestand stapeln, ändern Sie die drahtlose Umgebung. Mit einer Umfrage nach der Installation wird sichergestellt, dass der AP weiterhin für optimale Sprachkommunikationen ausreicht.

Hinweis Paketverlust tritt beim Roaming auf; allerdings legen der Sicherheitsmodus und ein schnelles Roaming fest, wie viele Pakete während der Übertragung verloren gegangen sind. Cisco empfiehlt die Implementierung des Cisco Centralized Key Management (CCKM), um schnelles Roaming zu aktivieren.

Weitere Informationen zum Sprach-QoS in einem drahtlosen Netzwerk erhalten Sie unter *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

Access Point-Zuordnung

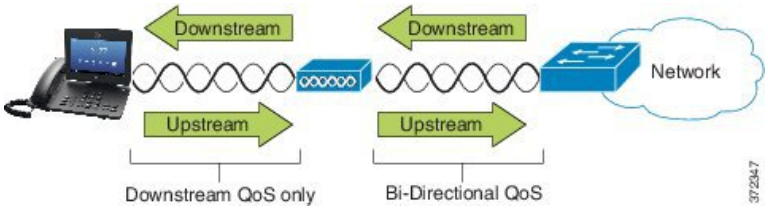
Beim Startvorgang scannt das Telefon APs mit SSIDs und Verschlüsselungstypen, die es erkennt. Das Telefon erstellt und verwaltet eine Liste der zulässigen Access Points und wählt den besten Access Point basierend auf der aktuellen Konfiguration aus.

QoS in einem drahtlosen Netzwerk

Der Sprach- und Videoverkehr im Wireless LAN wie Datenverkehr unterliegt Verzögerungen, Jitter und Paketverlusten. Diese Probleme wirken sich nicht auf die Benutzerdaten aus, können jedoch einen Sprach- oder Videoanruf nachhaltig beeinträchtigen. Um sicherzustellen, dass der Sprach- und Videoverkehr zeitnah und zuverlässig mit geringer Verzögerung und geringem Jitter verarbeitet wird, müssen Sie Quality of Service (QoS) verwenden.

Indem Sie die Geräte in ein Sprach-VLAN aufteilen und Sprachpakete mit höherer QoS markieren, können Sie sicherstellen, dass der Sprachverkehr Vorrang vor dem Datenverkehr erhält, was zu einer geringeren Paketverzögerung und weniger Paketverlusten führt.

Im Gegensatz zu kabelgebundenen Netzwerken mit dedizierten Bandbreiten berücksichtigen Wireless LANs die Verkehrsrichtung bei der Implementierung von QoS. Der Datenverkehr wird im Verhältnis zum AP als vor- oder nachgeschaltet klassifiziert, wie in der folgenden Abbildung dargestellt.



Der Enhanced Distributed Coordination Function-(EDCF-)Typ des QoS besitzt bis zu acht Warteschalgen für den nachgeschalteten QoS (in Richtung der 802.11b/g-Clients). Sie können die Warteschlangen basierend auf diesen Optionen zuweisen:

- QoS- oder Differentiated Services Code Point-(DSCP-)Einstellungen für die Pakete
- Zugriffslisten für Ebene 2 oder Ebene 3
- VLANs für bestimmten Datenverkehr

- Dynamische Registrierung der Geräte

Obwohl bis zu acht Warteschlangen auf dem Access Point eingerichtet werden können, sollten Sie maximal drei Warteschlangen für Sprach-, Video- und Signaldatenverkehr einrichten, um den bestmöglichen QoS sicherzustellen. Platzieren Sie Sprache in der Sprach-Warteschlange (UP6), Video in der Video-Warteschlange (UP5), Signalisierungsverkehr (SIP) in der Video-Warteschlange (UP4) und Datenverkehr in einer Best Effort-Warteschlange (UP0). Obwohl 802. 11 b/g EDCF nicht garantiert, dass der Sprachverkehr vor Datenverkehr geschützt ist, erhalten Sie möglicherweise die besten Statistikergebnisse durch Verwendung dieses Warteschlangenmodells.

Die Warteschlangen sind:

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

Hinweis Das Gerät markiert die SIP-Signalübertragungspakete mit einem DSCP-Wert von 24 (CS3) und RTP-Pakete mit einem DSCP-Wert von 46 (EF).

Hinweis Die Anrufsteuerung (SIP) wird als UP4 (VI) gesendet. Video wird als UP5 (VI) gesendet, wenn Admission Control Mandatory (ACM) für Video (Traffic Specification [TSpec] disabled) deaktiviert ist. Sprache wird als UP6 (VO) gesendet, wenn ACM für Sprache deaktiviert ist (TSpec disabled).

Die folgende Tabelle enthält ein QoS-Profil auf dem Access Point, der den Sprach-, Video- und Anrufsteuerungs-Datenverkehr (SIP) priorisiert.

Tabelle 2: Einstellungen für QoS-Profil und Schnittstelle

Datenverkehrstyp	DSCP	802.1p	WMM UP	Port Range (Port-Bereich)
Voice	EF (46)	5	6	UDP 16384-32767
Interaktive Videofunktionen	AF41 (34)	4	5	UDP 16384-32767
Anrufsteuerung	CS3 (24)	3	4	TCP 5060-5061

Um die Zuverlässigkeit von Sprachübertragungen in einer nichtdeterministischen Umgebung zu verbessern, unterstützt das Gerät den Industriestandard IEEE 802.11e und ist Wi-Fi Multimedia-(WMM-)fähig. WMM ermöglicht differenzierte Dienste für Sprach-, Video-, Best-Effort-Daten- und anderen Verkehr. Damit diese differenzierten Dienste einen ausreichenden QoS für Sprachpakete bereitstellen, kann nur eine bestimmte Menge an Sprachbandbreite gleichzeitig auf einem Kanal bedient oder zugelassen werden. Falls das Netzwerk „N“-Sprachanrufe mit reservierter Bandbreite verarbeiten kann, verringert sich die Qualität aller Anrufe, wenn die Menge an Sprachverkehr über diese Begrenzung (auf N+1 Anrufe) hinausgeht.

Zur Behebung von Problemen mit der Anrufqualität ist ein CAC-Schema (Call Admission Control, Anrufzulassungssteuerung) erforderlich. Bei Aktivierung von SIP CAC im WLAN wird QoS in einem Szenario mit Netzwerküberlastung aufrechterhalten, indem die Anzahl an aktiven Sprachanrufen begrenzt wird, damit die konfigurierten Grenzwerte auf dem AP nicht überschritten werden. Bei einem überlasteten Netzwerk hält das System eine kleine Bandbreitenreserve aufrecht, damit drahtlose Geräte ein Roaming in das umliegende AP vornehmen können, selbst wenn der AP „voll ausgelastet“ ist. Nachdem das Sprachbandbreitenlimit erreicht ist, wird der nächste Anruf an einen benachbarten AP durch Lastausgleich übertragen, um die Qualität der vorhandenen Anrufe im Kanal nicht zu beeinträchtigen.

Die Telefone verwenden TCP für die SIP-Kommunikation und die Registrierungen von Anrufsteuerungssystemen gehen möglicherweise verloren, wenn ein AP voll ausgelastet ist. Frames zu oder von einem Client, der nicht durch das CAC „autorisiert” wurde, können verloren werden, was zu einer Abmeldung des Anrufsteuerungssystems führt. Daher empfehlen wir die Deaktivierung von SIP CAC.

Flexibles DSCP einrichten

Prozedur

Schritt 1	Navigieren Sie in Cisco Unified Communications Manager Administration zu to **System** > **Dienstparameter**.
Schritt 2	Legen Sie in den clusterweiten Parametern (System – Standort und Region) die Option „Video-BandwidthPool für immersive Videoanrufe verwenden” auf **False** fest.
Schritt 3	Legen Sie in den clusterweiten Parametern (Anrufzulassungssteuerung) die Option „Videoanruf-QoS-Richtlinie” auf **Auf immersiv hochstufen** fest.
Schritt 4	Speichern Sie Ihre Änderungen.

802.11-Standards für die WLAN-Kommunikation

Wireless LANs müssen den Standards IEEE 802.11 des Institute of Electrical and Electronic Engineers (IEEE) entsprechen, die die Protokolle definieren, die für den gesamten Ethernet-basierten drahtlosen Datenverkehr gelten. Die Schnurlostelefone unterstützen die folgenden Standards:

- 802. 11A: Verwendet das 5-GHz-Band, das mehr Kanäle und verbesserte Datenraten durch Verwendung der OFDM-Technologie bietet. Dynamic Frequency Selection (DFS) und Transmit Power Control (TPC) unterstützen diesen Standard.
- 802.11b: Gibt die Funkfrequenz (HF) von 2,4 GHz für die Übertragung und den Empfang von Daten bei niedrigeren Datenraten (1, 2, 5,5, 11 Mbit/s) an.
- 802.11-d: Ermöglicht Access Points, ihre derzeit unterstützten Funkkanäle und Stufen zur Stromübertragung anzukündigen. Der 802.11d-fähige Client verwendet diese Informationen anschließend, um die zu verwendenden Kanäle und Stromversorgungen zu bestimmen. Das Telefon erfordert World-Modus (802.11 d), um zu bestimmen, welche Kanäle rechtlich für jedes angegebene Land zulässig sind. Informationen zu unterstützten Kanälen erhalten Sie in der Tabelle unten: Stellen Sie sicher, dass 802.11d ordnungsgemäß auf den Cisco IOS Access Points oder dem Cisco Unified Wireless LAN-Controller konfiguriert ist.
- 802.11E: Definiert eine Reihe von Quality of Service- (QoS-)Erweiterungen für WLAN-Anwendungen.

- 802. 11 g: Verwendet das gleiche nicht lizenzierte 2,4 Ghz-Band wie 802.11b, erweitert jedoch die Datenraten, um eine höhere Leistung durch Verwendung der OFDM-Technologie (Orthogonal Frequency Division Multiplexing) zu erreichen. OFDM ist eine Physical-Layer-Encoding-Technologie für die Übertragung von Signalen durch Verwendung von HF.
- 802.11 h: Unterstützt ein 5-GHz-Spektrum und die Verwaltung der Stromversorgungsübertragung. Stellt der 802.11a Media Access Control (MAC) DFS und TPC bereit.
- 802.11i: Gibt Sicherheitsmechanismen für drahtlose Netzwerke an.
- 802.11n: Verwendet die Funkfrequenz von 2,4 GHz oder 5 GHz für die Übertragung und den Empfang von Daten mit Geschwindigkeiten von bis zu 150 Mbit/s und verbessert die Datenübertragung durch die Verwendung von MIMO-Technologie (Multiple Input, Multiple Output), Kanalbündelung und Nutzlastoptimierung.

Hinweis Die Schnurlostelefone verfügen über eine einzige Antenne und verwenden das SISO-System (Single Input Single Output), das nur Datenraten von MCS 0 bis MCS 7 unterstützt (72 Mbit/s mit 20-MHz-Kanälen und 150 Mbit/s mit 40-MHz-Kanälen). Optional können Sie MCS 8 bis MCS 15 aktivieren, wenn 802.11n-Clients die MIMO-Technologie verwenden, die diese höheren Datenraten nutzen kann.

- 802.11r: Gibt die Anforderungen für sicheres schnelles Roaming an.
- 802.11ac: Verwendet die Funkfrequenz von 5 GHz für die Übertragung und den Empfang von Daten mit Geschwindigkeiten von bis zu 433 Mbit/s.

Tabelle 3: Unterstützte Kanäle

Band-Bereich	Verfügbare Kanäle	Kanalsatz	Channel Width (Kanalbandbreite)
2,412–2,472 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

Hinweis Die Kanäle 120, 124, 128 werden in Amerika, Europa oder Japan nicht unterstützt, können jedoch möglicherweise in anderen Regionen der Welt eingesetzt werden.

Informationen zu unterstützten Datenraten und zur Empfindlichkeit beim Senden und Empfangen für WLANs finden Sie unter *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

World-Modus (802.11 d)

Die Schnurlostelefone verwenden 802.11d, um die Kanäle festzulegen und die zu verwendenden Leistungsstufen zu übertragen. Das Telefon übernimmt die Client-Konfiguration vom zugewiesenen AP. Aktivieren Sie den Weltmodus (802.11d) auf dem AP, um das Telefon im Weltmodus zu verwenden.

Hinweis Die Aktivierung des Weltmodus (802.11d) ist möglicherweise nicht erforderlich, wenn die Frequenz 2,4 GHz beträgt und der aktuelle Access Point auf einem Kanal von 1 bis 11 überträgt.

Da alle Länder diese Frequenzen unterstützen, können Sie versuchen, diese Kanäle ungeachtet der Unterstützung des Weltmodus (802.11d) zu scannen.

Weitere Informationen zum Aktivieren der Welt Modus und zur 2,4-GHz-Unterstützung finden Sie in *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

Aktivieren Sie den Weltmodus (802.11d) für das entsprechende Land, in dem sich der Access Point befindet. Der Weltmodus wird automatisch für den Cisco Unified Wireless LAN Controller aktiviert.

Funkbereiche

Bei WLAN-Kommunikationen werden die folgenden Hochfrequenzbereiche verwendet:

- 2,4 GHz – Bei vielen Geräten, die 2,4 GHz verwenden, können potenzielle Störungen bei der 802.11b/g-Verbindung auftreten. Eine Störung kann ein Denial of Service-(DoS-)Szenario auslösen, das möglicherweise erfolgreiche 802.11-Übertragungen verhindert.
- 5 GHz – Dieser Bereich ist in verschiedene Abschnitte mit der Bezeichnung Unlicensed National Information Infrastructure-(UNII-)Bereiche unterteilt. Diese Abschnitte enthalten jeweils vier Kanäle. Die Kanäle weisen einen Abstand von 20 MHz auf, um sich nicht überschneidende Kanäle und weitere Kanäle bereitzustellen als mit 2,4 GHz.

Sicherheit für Kommunikationen in WLANs

Da alle WLAN-Geräte, die sich innerhalb der Reichweite befinden, den gesamten anderen WLAN-Datenverkehr empfangen können, ist die Sicherheit der Sprachkommunikation in einem WLAN besonders wichtig. Um zu verhindern, dass der Sprachverkehr von Angreifern manipuliert oder abgefangen wird, unterstützt die Cisco SAFE-Sicherheitsarchitektur Schnurlostelefone und Cisco Aironet Access Points. Weitere Informationen zur Sicherheit in Netzwerken finden Sie unter https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/index.html.

Authentifizierungsmethoden

Die Cisco Wireless IP-Telefonielösung bietet Sicherheit für drahtlose Netzwerke, die nicht autorisierte Anmeldungen und kompromittierte Kommunikation mithilfe der folgenden Authentifizierungsmethoden verhindert, die von Schnurlostelefonen unterstützt werden:

- WLAN-Authentifizierung
  - WPA (802.1x-Authentifizierung + TKIP- oder AES-Verschlüsselung)

- WPA2 (802.1x-Authentifizierung + AES- oder TKIP-Verschlüsselung)
- WPA-PSK (vorab bereitgestellter Schlüssel + TKIP-Verschlüsselung)
- WPA2-PSK (vorab bereitgestellter Schlüssel + AES-Verschlüsselung)
- EAP-FAST (Extensible Authentication Protocol – Flexible Authentifizierung durch sicheres Tunneling)
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security)
- PEAP (Protected Extensible Authentication Protocol) MS-CHAPv2 und GTC
- CCKM (Cisco Centralized Key Management)
- Offen (Keine)

- WLAN-Verschlüsselung
  - AES (Advanced Encryption Scheme)
  - TKIP / MIC (Temporal Key Integrity Protocol / Message Integrity Check)
  - WEP (Wired Equivalent Protocol) 40/64 und 104/128 Bit

Hinweis Dynamisches WEP mit 802.1x-Authentifizierung und Authentifizierung über einen gemeinsamen Schlüssel werden nicht unterstützt.

Weitere Informationen zu Authentifizierungsmethoden finden Sie im Abschnitt „Wireless-Sicherheit“ in *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

Authentifizierte Schlüsselverwaltung

Folgende Authentifizierungsschemata verwenden den RADIUS-Server, um Authentifizierungsschlüssel zu verwalten:

- WPA/WPA2: Verwendet RADIUS-Serverinformationen, um eindeutige Authentifizierungsschlüssel zu generieren. Da diese Schlüssel auf dem zentralen RADIUS-Server generiert werden, bietet WPA/WPA2 eine höhere Sicherheit als die vorinstallierten WPA-Schlüssel, die am Access Point und auf dem Gerät gespeichert sind.
- CCKM (Cisco Centralized Key Management): Verwendet RADIUS-Serverinformationen und WDS-Informationen (Wireless Domain Server), um Schlüssel zu verwalten und zu authentifizieren. Der WDS erstellt einen Cache mit Sicherheitsanmeldedaten für CCKM-fähige Client-Geräte, um eine schnelle und sichere erneute Authentifizierung zu ermöglichen.

Bei WPA/WPA2 und CCKM werden die Verschlüsselungsschlüssel nicht auf dem Gerät eingegeben, sondern zwischen dem Access Point und dem Gerät automatisch abgeleitet. Der EAP-Benutzername und das Kennwort, die zur Authentifizierung verwendet werden, müssen jedoch auf jedem Gerät eingegeben werden.

Verschlüsselungsmethoden

Um die Sicherheit des Sprachverkehrs sicherzustellen, unterstützt das Schnurlostelefon die Verschlüsselung mit WEP, TKIP und AES (Advanced Encryption Standard). Wenn diese Mechanismen für die Verschlüsselung verwendet werden, sind Sprachpakete RTP (Real-Time Transport Protocol) zwischen dem Access Point und dem Gerät verschlüsselt.

WEP

Bei Verwendung von WEP in einem Wireless-Netzwerk erfolgt die Authentifizierung am Access Point mit offener Authentifizierung oder Authentifizierung über einen gemeinsamen Schlüssel. Der auf dem Telefon eingerichtete WEP-Schlüssel muss mit dem am Access Point konfigurierten WEP-Schlüssel übereinstimmen, um erfolgreiche Verbindungen zu ermöglichen. Die Telefone unterstützen die WEP-Schlüssel, die 40- oder 128-Bit-Verschlüsselung verwenden und auf dem Gerät und am Access Point statisch bleiben.

TKIP

WPA und CCKM verwenden die TKIP-Verschlüsselung. Dabei handelt es sich um eine Methode, die im Vergleich zu WEP mehrere Verbesserungen aufweist. TKIP ermöglicht die Verschlüsselung einzelner Paket und bietet längere Initialisierungsvektoren (IVs), um die Sicherheit der Verschlüsselung zu erhöhen. Darüber hinaus stellt eine Nachrichtenintegritätsprüfung sicher, dass die verschlüsselten Pakete nicht geändert werden. TKIP besitzt nicht die Vorhersehbarkeit von WEP, die es Angreifern ermöglicht, den WEP-Schlüssel zu entschlüsseln.

AES

Eine Verschlüsselungsmethode, die für die WPA2-Authentifizierung verwendet wird. Dieser nationale Verschlüsselungsstandard verwendet einen symmetrischen Algorithmus, bei dem die Schlüssel für Ver- und Entschlüsselung identisch sind.

Weitere Informationen zu Verschlüsselungsmethoden finden Sie im Abschnitt „Wireless-Sicherheit“ in *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

AP-Authentifizierungs- und Verschlüsselungsoptionen

Authentifizierungs- und Verschlüsselungsschemata werden innerhalb des Wireless LAN eingerichtet. VLANs werden im Netzwerk und an den Access Points konfiguriert und geben verschiedene Kombinationen von Authentifizierung und Verschlüsselung an. Eine SSID wird einem VLAN und dem spezifischen Authentifizierungs- und Verschlüsselungsschema zugeordnet. Damit Schnurlostelefone erfolgreich authentifiziert werden können, müssen Sie an den Access Points und auf dem Telefon die gleichen SSIDs mit ihren Authentifizierungs- und Verschlüsselungsschemata konfigurieren.

Hinweis

- Wenn Sie WPA Pre-shared Key oder WPA2 Pre-shared Key verwenden, muss der vorinstallierte Schlüssel auf dem Telefon statisch festgelegt werden. Diese Schlüssel müssen mit den Schlüsseln am Access Point übereinstimmen.
- Die Schnurlostelefone unterstützen die automatische EAP-Aushandlung nicht. Wenn der EAP-FAST-Modus verwendet werden soll, müssen Sie diesen festlegen.

Die folgende Tabelle enthält eine Liste der Authentifizierungs- und Verschlüsselungsschemata, die auf den vom Telefon unterstützten Cisco Aironet Access Points konfiguriert werden können. Die Tabelle zeigt die Netzwerkkonfigurationsoption für das Gerät, die der Konfiguration des Access Points entspricht.

Tabelle 4: Authentifizierungs- und Verschlüsselungsschemata

Cisco WLAN-Konfiguration			Telefonkonfiguration
Authentifizierung	**Schlüsselverwaltung**	**Allgemeine Verschlüsselung**	**Authentifizierung**
Offen	Keine	Keine	Keine
Statisches WEP	Keine	WEP	WEP
EAP-FAST	WPA oder WPA2 mit optionalem CCKM	TKIP oder AES	802.1x EAP > EAP-FAST
PEAP-MSCHAPv2	WPA oder WPA2 mit optionalem CCKM	TKIP oder AES	802.1x EAP > PEAP > MSCHAPV2
PEAP-GTC	WPA oder WPA2 mit optionalem CCKM	TKIP oder AES	802.1x EAP > PEAP > GTC
EAP-TLS	WPA oder WPA2 mit optionalem CCKM	TKIP oder AES	802.1x EAP > TLS
WPA/WPA2-PSK	WPA-PSK oder WPA2-PSK	TKIP oder AES	WPA/WPA2 PSK

Weitere Informationen finden Sie im Abschnitt *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

Zertifikate

Das Telefon unterstützt die folgenden Zertifikate.

- Digitales X.509-Zertifikat für EAP-TLS oder zum Aktivieren von PEAP und Servervalidierung für die WLAN-Authentifizierung
- SCEP (Simple Certificate Enrollment Protocol) für die Registrierung und automatische Erneuerung von Zertifikaten
- 1024-, 2048-, 4096-Bit-Schlüssel
- SHA-1 und SHA-256 Signaturtypen
- DER und Base-64 (PEM) Verschlüsselungstypen
- Vom Benutzer installiertes Zertifikat im PKCS 12-Format (Erweiterung .p12 oder .pfx), das auch den privaten Schlüssel enthält
- Serverzertifikat (Stammzertifizierungsstelle) mit der Erweiterung .crt oder .cer

Installieren Sie die Zertifikate wie folgt auf den Telefonen:

- Verwenden Sie die Verwaltungswebseite. Weitere Informationen hierzu finden Sie unter Verwaltungsseite für das Cisco IP-Telefon.

- Verwenden Sie einen SCEP-Server, um die Zertifikate zu installieren und zu verwalten. Weitere Informationen hierzu finden Sie unter SCEP-Konfiguration

Wenn die Benutzer ihre Telefone selbst konfigurieren und Zertifikate erforderlich sind, müssen Sie den Benutzern den Zertifikatstyp mit den anderen Konfigurationseinstellungen mitteilen. Wenn Sie SCEP nicht für die Installation von Zertifikaten verwenden, müssen Sie die Zertifikate manuell installieren.

WLANs und Roaming

Die Schnurlostelefone unterstützen das Cisco Centralized Key Management (CCKM), ein zentralisiertes Protokoll zur Schlüsselverwaltung, das einem Cache die Sitzungsanmeldeinformationen auf dem Wireless Domain Server (WDS) bereitstellt.

Einzelheiten zu CCKM erhalten Sie in *Cisco Fast Secure Roaming Application Note* unter:

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

Die Telefone unterstützen auch 802.11r. Weitere Informationen finden Sie im Abschnitt *Bereitstellungshandbuch für die Cisco schnurlos IP-Telefon 8821-Serie*.

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.

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.
- 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.

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.