

Konfiguration und Fehlerbehebung bei der Registrierung von Wireless-IP-Telefonen

Inhalt

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Cisco Unified Wireless LAN Controller und Access Points](#)

[Einstellungen für Wireless Local Area Network \(WLAN\)](#)

[Controller-Einstellungen](#)

[802.11-Netzwerkeinstellungen](#)

[Konfigurieren des Cisco Unified IP-Telefons 9971](#)

[Wireless LAN-Einstellungen](#)

[Konfigurieren von Cisco Unified Communications Manager](#)

Einführung

In diesem Dokument wird beschrieben, wie die Registrierung von Wireless-IP-Telefonen beim Cisco Unified Communications Manager (CUCM) konfiguriert und Fehler bei diesen behoben werden.

Die Cisco Wireless IP-Telefone können an Benutzer angepasst werden, die die kabelgebundene Netzwerkverbindung trennen und weiterhin verbunden bleiben müssen.

Mitarbeiter: Luis Segnini und Kenny Araya, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Wireless-Architektur
- Konfiguration von Wireless-IP-Telefonen
- CUCM-Basiskonfiguration

Verwendete Komponenten

- Cisco Unified Communications Manager 8.6 oder höher
- Wireless IP-Telefonmodelle (792X, 9971, 8821)

Der folgende Leitfaden basiert auf dem Cisco Unified 9971 IP-Telefonmodell. Die Konfiguration kann je nach IP-Telefonmodell variieren.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Cisco Unified Wireless LAN Controller und Access Points

Einstellungen für Wireless Local Area Network (WLAN)

Es wird empfohlen, für das IP-Telefon einen separaten Service Set Identifier (SSID) zu verwenden. Wenn jedoch bereits ein vorhandener SSID für die Unterstützung sprachfähiger Cisco Wireless LAN-Endpunkte konfiguriert ist, kann dieses WLAN stattdessen verwendet werden.

Der vom IP-Telefon zu verwendende SSID kann so konfiguriert werden, dass er nur für einen bestimmten 802.11-Funktyp gilt.

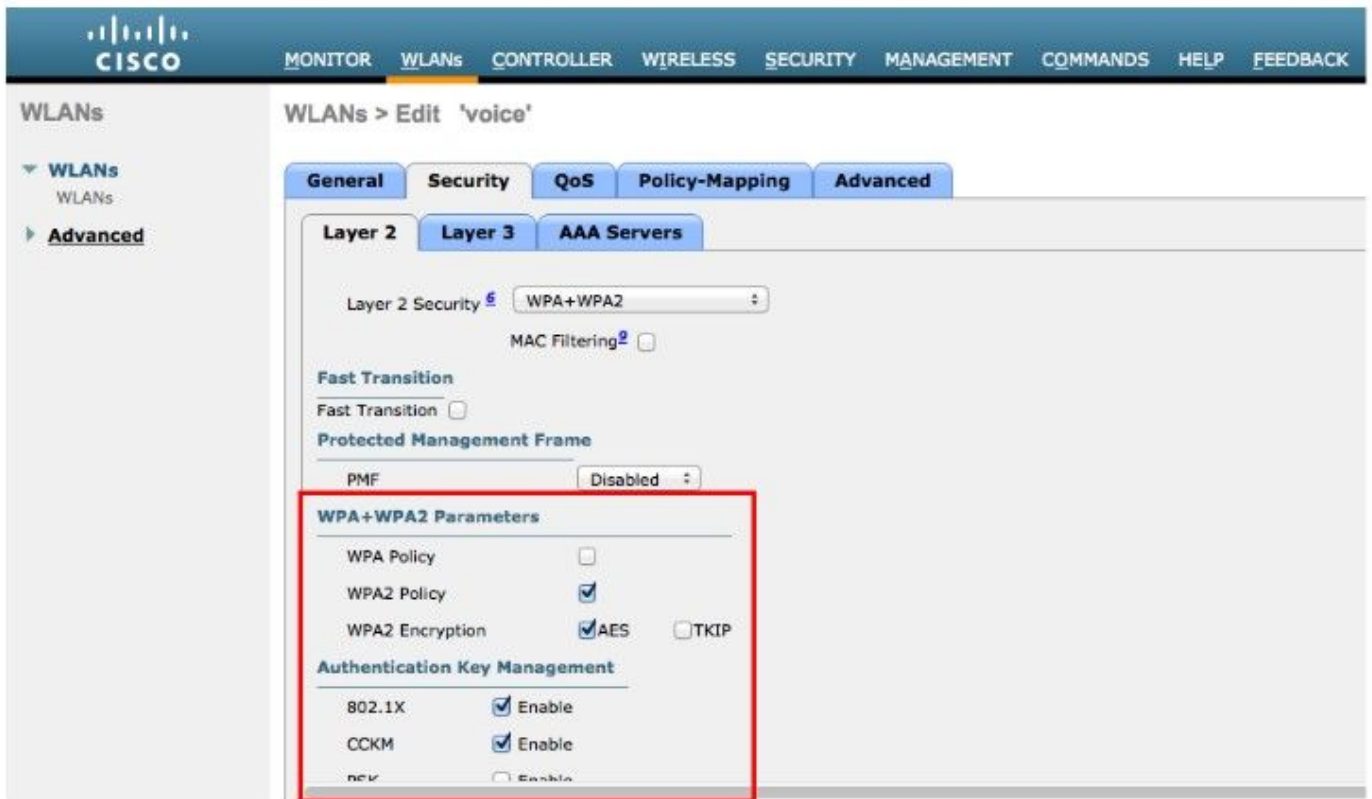
Es wird empfohlen, das IP-Telefon im 5-GHz-Band zu betreiben, da es viele Kanäle und nicht so viele Störquellen wie das 2,4-GHz-Band bietet.

Stellen Sie sicher, dass die ausgewählte SSID nicht von anderen WLANs verwendet wird, da dies zu Fehlern beim Einschalten oder beim Roaming führen könnte. vor allem dann, wenn ein anderer Sicherheitstyp verwendet wird.

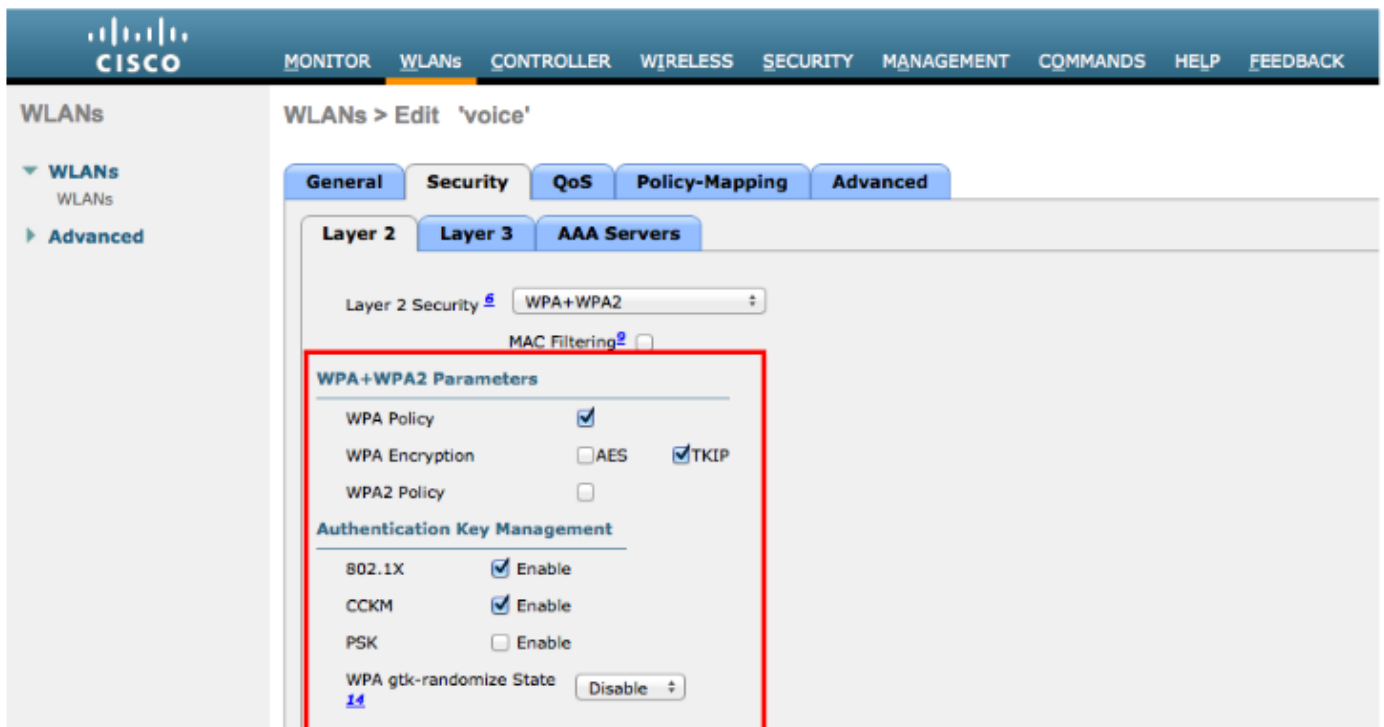
The screenshot shows the Cisco Unified Wireless LAN Controller configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', and 'FEEDBACK'. The main content area is titled 'WLANs > Edit 'voice'' and has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is active, showing the following configuration:

Profile Name	voice
Type	WLAN
SSID	voice
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X + CCKM)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11a only
Interface/Interface Group(G)	rtp-9 voice
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	WLC5508-1

Um Cisco Centralized Key Management (CCKM) zu verwenden, aktivieren Sie die Richtlinie Wi-Fi Protected Access (WPA) 2 mit AES-Verschlüsselung (Advanced Encryption Standard) und 802.1x + CCKM für den authentifizierten Schlüsselverwaltungstyp, wenn auf dem IP-Telefon Firmware-Version 9.1(1) oder höher ausgeführt wird, um schnelles sicheres sicheres sicheres Roaming zu ermöglichen.



Wenn auf dem IP-Telefon eine Firmware-Version vor 9.1(1) ausgeführt wird, aktivieren Sie die WPA-Richtlinie mit TKIP-Verschlüsselung (Temporal Key Integrity Protocol) und 802.1x + CCKM für den authentifizierten Schlüsselverwaltungstyp, um sicheres schnelles Roaming zu ermöglichen.



Die Wi-Fi Multimedia-Richtlinie (WMM) sollte nur dann auf "Erforderlich" gesetzt werden, wenn das IP-Telefon oder andere WMM-fähige Telefone diese SSID verwenden. Wenn im WLAN keine WMM-Clients vorhanden sind, wird empfohlen, diese Clients auf eine andere SSID/ein anderes WLAN zu setzen. Wenn andere WMM-Clients dieselbe SSID wie das IP-Telefon verwenden müssen, stellen Sie sicher, dass die WMM-Richtlinie auf "Zulassen" gesetzt ist.

Aktivieren Sie die Call Admission Control (CAC) für den 7920 Access Point (AP), um dem Client QoS (Basic Service Set) anzukündigen.

The screenshot shows the Cisco WLAN configuration interface for the 'voice' WLAN. The 'QoS' tab is selected. A red box highlights the 'Quality of Service (QoS)' section, which includes a dropdown menu set to 'Platinum (voice)', 'Application Visibility' checked and set to 'Enabled', 'AVC Profile' set to 'none', and 'Netflow Monitor' set to 'none'. Below this, there are sections for 'Override Per-User Bandwidth Contracts (kbps)' and 'Override Per-SSID Bandwidth Contracts (kbps)', each with input fields for Average Data Rate, Burst Data Rate, Average Real-Time Rate, and Burst Real-Time Rate, all currently set to 0.

The screenshot shows the Cisco WLAN configuration interface for the 'voice' WLAN, with the 'WMM' section highlighted by a red box. The 'WMM Policy' is set to 'Required'. Under '7920 AP CAC', '7920 Client CAC', and 'Media Stream', the 'Multicast Direct' option is checked and set to 'Enabled'. The '7920 AP CAC' and '7920 Client CAC' options are also checked and set to 'Enabled'. The 'Burst Real-Time Rate' section above shows input fields for DownStream and UpStream rates, all set to 0.

Konfigurieren Sie das Sitzungs-Timeout je nach Bedarf aktivieren.

Es wird empfohlen, die Sitzungs-Timeout-Einstellung zu deaktivieren oder die Zeitüberschreitung zu verlängern (z. B. 24 Stunden/86400 Sekunden), um mögliche Unterbrechungen bei

Audioanrufen zu vermeiden. Wenn die Option deaktiviert ist, werden alle möglichen Unterbrechungen vermieden, aber Sitzungs-Timeout kann dazu beitragen, die Client-Anmeldeinformationen regelmäßig zu überprüfen, um sicherzustellen, dass der Client gültige Anmeldeinformationen verwendet.

Aktivieren Sie Aironet Extensions (Aironet IE), Peer-to-Peer (P2P) Blocking Action muss deaktiviert werden. Konfigurieren Sie ggf. den Client-Ausschluss. Der Off-Channel-Scanverzögerung kann so eingestellt werden, dass die Prüfung für bestimmte Warteschlangen verzögert wird und die Abtastverzögerung erfolgt.

Die maximal zulässigen Clients pro AP-Funkmodul können bei Bedarf konfiguriert werden.

Die erforderliche DHCP-Adressenzuweisung (Dynamic Host Configuration Protocol) muss deaktiviert werden.

Der Management-Frame-Schutz muss auf "Optimal" oder "Deaktiviert" eingestellt sein.

Verwenden Sie für optimale Akkuleistung und -qualität einen Zeitraum von 2 DTIM (Delivery Traffic Indication Message) mit einer Beacon-Dauer von 100 ms.

Stellen Sie sicher, dass Client Load Balancing und Client Band Select deaktiviert sind.

The screenshot shows the Cisco WLAN configuration interface for a 'voice' WLAN. The 'Advanced' tab is selected, and several settings are highlighted with red boxes:

- Enable Session Timeout:** Checked, with a value of 86400 seconds.
- Aironet IE:** Checked and Enabled.
- P2P Blocking Action:** Set to Disabled.
- Client Exclusion:** Not checked.
- Maximum Allowed Clients Per AP Radio:** Set to 20.
- DHCP:** DHCP Server and DHCP Addr. Assignment are not checked.
- OEAP:** Split Tunnel (Printers) is not checked.
- Management Frame Protection (MFP):** MFP Client Protection is set to Optional.
- DTIM Period (in beacon intervals):** Set to 2 for both 802.11a/n and 802.11b/g/n.
- NAC:** NAC State is set to None.

The screenshot shows the Cisco WLAN configuration interface for a 'voice' WLAN, continuing from the previous one. The 'Advanced' tab is selected, and several settings are highlighted with red boxes:

- Off Channel Scanning Defer:** Scan Defer Priority is set to 0, 1, 2, 3, 4, 5, 6, 7. Scan Defer Time (msecs) is set to 100.
- FlexConnect:** FlexConnect Local Switching, FlexConnect Local Auth, Learn Client IP Address, and Vlan based Central Switching are all checked and Enabled.
- Load Balancing and Band Select:** Client Load Balancing and Client Band Select are not checked.
- Passive Client:** Passive Client is not checked.
- Voice:** Media Session Snooping, Re-anchor Roamed Voice Clients, and KTS based CAC Policy are all checked and Enabled.
- Radius Client Profiling:** DHCP Profiling and HTTP Profiling are not checked.
- Local Client Profiling:** DHCP Profiling and HTTP Profiling are not checked.
- PMIP:** No settings are visible.

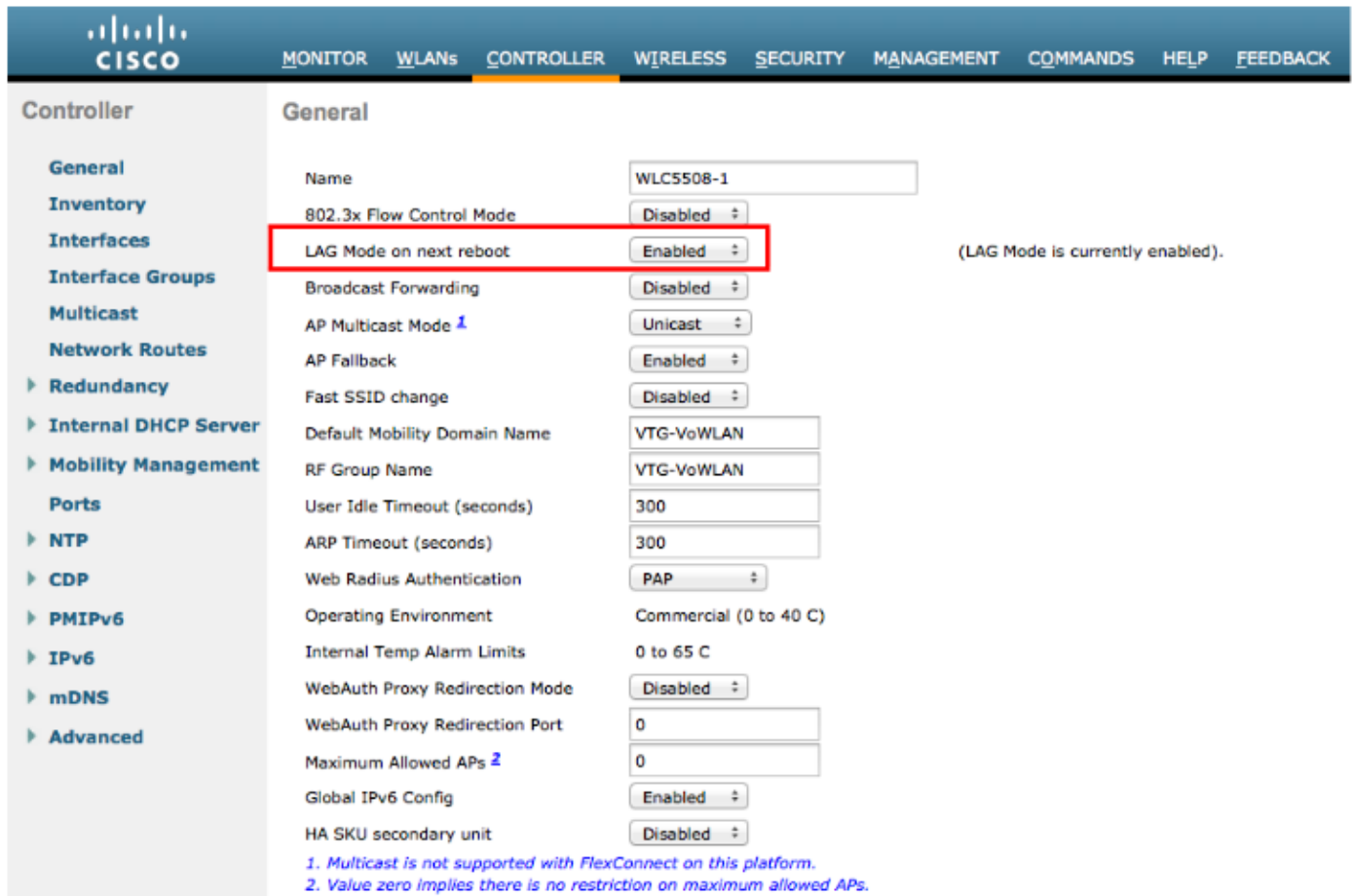
Controller-Einstellungen

Stellen Sie sicher, dass der Hostname des Cisco Unified Wireless LAN Controllers korrekt konfiguriert ist.

Aktivieren Sie die Link Aggregation (LAG), wenn Sie mehrere Ports des Cisco Unified Wireless LAN-Controllers verwenden.

Konfigurieren Sie den gewünschten AP-Multicast-Modus. In Versionen vor 6.0 wurde Aggressive Load Balancing in den allgemeinen Controller-Einstellungen konfiguriert. Ab 6.0 wird dies als

Client Load Balancing bezeichnet und kann unter der WLAN-Konfiguration (SSID-Einstellungen) konfiguriert werden.



The screenshot shows the Cisco Controller configuration page for a WLAN. The 'LAG Mode on next reboot' option is highlighted with a red box and set to 'Enabled'. A note indicates '(LAG Mode is currently enabled)'. Other settings include Name (WLC5508-1), 802.3x Flow Control Mode (Disabled), Broadcast Forwarding (Disabled), AP Multicast Mode (Unicast), AP Fallback (Enabled), Fast SSID change (Disabled), Default Mobility Domain Name (VTG-VoWLAN), RF Group Name (VTG-VoWLAN), User Idle Timeout (300), ARP Timeout (300), Web Radius Authentication (PAP), Operating Environment (Commercial), Internal Temp Alarm Limits (0 to 65 C), WebAuth Proxy Redirection Mode (Disabled), WebAuth Proxy Redirection Port (0), Maximum Allowed APs (0), Global IPv6 Config (Enabled), and HA SKU secondary unit (Disabled).

802.11-Netzwerkeinstellungen

Wenn Sie 5 GHz verwenden, stellen Sie sicher, dass der 802.11a-Netzwerkstatus "Enabled" (Aktiviert) lautet. Legen Sie den Beacon-Zeitraum auf 100 ms fest.

Stellen Sie sicher, dass die Unterstützung für Dynamic Transmit Power Control (DTPC) aktiviert ist. Wenn Sie Cisco 802.11n Access Points verwenden, stellen Sie sicher, dass ClientLink aktiviert ist. Bei den aktuellen Versionen können maximal zulässige Clients konfiguriert werden.

Es wird empfohlen, eine Rate von 12 Mbit/s als erforderliche (einfache) Übertragungsraten und eine Rate von 18-24 bzw. 18-54 Mbit/s als unterstützte Übertragungsraten (optional) festzulegen. In einigen Umgebungen kann es jedoch erforderlich sein, dass 6 Mbit/s als obligatorische (grundlegende) Option aktiviert werden. 36 - 54 Mbit/s können optional deaktiviert werden, wenn es keine Anwendungen gibt, die von diesen Raten profitieren können (z. B. Video).

Aktivieren Sie die CCX-Standortmessung.

The screenshot displays the Cisco Unified IP-Phone 9971 configuration interface for 802.11a Global Parameters. The interface is divided into several sections:

- General:**
 - 802.11a Network Status: Enabled
 - Beacon Period (milliseconds):
 - Fragmentation Threshold (bytes):
 - DTPC Support: Enabled
 - Maximum Allowed Clients:
 - RSSI Low Check: Enabled
 - RSSI Threshold (-60 to -90 dBm):
- Data Rates**:**
 - 6 Mbps:
 - 9 Mbps:
 - 12 Mbps:
 - 18 Mbps:
 - 24 Mbps:
 - 36 Mbps:
 - 48 Mbps:
 - 54 Mbps:
- CCX Location Measurement:**
 - Mode: Enabled
 - Interval (seconds):

Konfigurieren des Cisco Unified IP-Telefons 9971

Um die Wi - Fi-Einstellungen auf dem IP-Telefon zu konfigurieren, verwenden Sie die Tastatur und den Touchscreen, um zu Application Button > Administrator Settings > Network Setup > WLAN Setup zu navigieren.

Wireless LAN-Einstellungen

Verwenden Sie die folgenden Richtlinien, um das WLAN-Profil zu konfigurieren.

- Stellen Sie sicher, dass Wireless auf "Ein" eingestellt ist.
- Die WLAN-Anmeldung für den Zugriff kann auf On (Ein) gesetzt werden, um im Menü Applications (Anwendungen) einen Verknüpfungszugriff zu erhalten, um den Benutzernamen oder das Kennwort zu aktualisieren.
- Geben Sie die SSID für das Sprach-Wireless-LAN ein, wobei die Groß- und Kleinschreibung zu beachten ist.

Das Cisco Unified IP-Telefon 9971 unterstützt ein einzelnes WLAN-Profil, das eine einzelne SSID zulässt.

Es stehen drei verschiedene 802.11-Modi zur Verfügung.

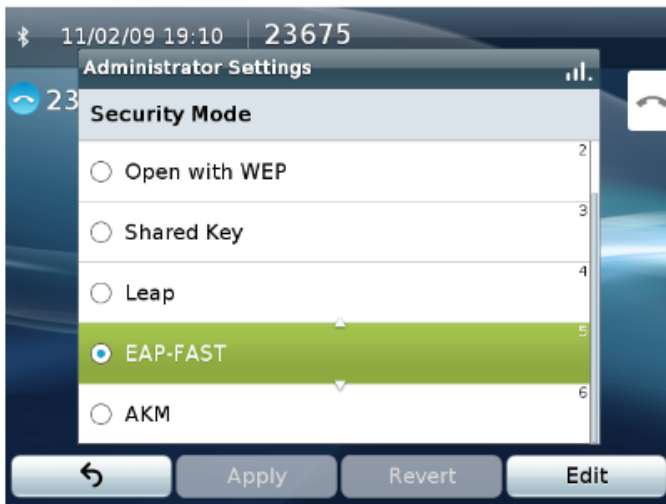
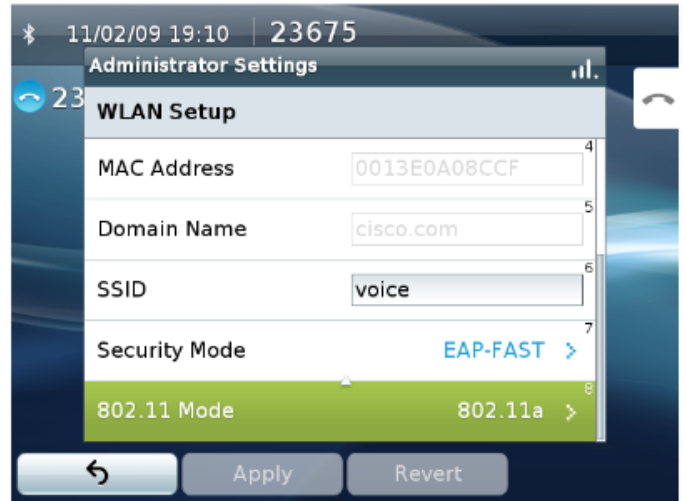
- Automatisch
- 802.11a
- 802.11b/g

Der automatische Modus scannt die 2,4- und 5-GHz-Kanäle und versucht, eine Verbindung zum Access Point herzustellen, wenn das konfigurierte Netzwerk verfügbar ist.

Der 802.11a-Modus scannt nur 5-GHz-Kanäle, und der 802.11b/g-Modus scannt nur 2,4-GHz-Kanäle und versucht dann, eine Verbindung zu einem Access Point herzustellen, wenn das konfigurierte Netzwerk verfügbar ist.

Konfigurieren Sie Ihr IP-Telefon so, dass es Open mit Wired Equivalent Privacy (WEP) oder Shared Key für den Sicherheitsmodus verwendet, und geben Sie die statischen WEP-Schlüsselinformationen ein, die der Konfiguration des Access Points entsprechen.

- Wählen Sie im IPv4-Setup aus, ob DHCP oder statische IP-Informationen konfiguriert werden sollen.
- Wenn Option 150 oder 66 nicht für die Bereitstellung der IP-Adresse des Trivial File Transfer Protocol (TFTP)-Servers über den DHCP-Bereich des Netzwerks konfiguriert ist, setzen Sie Alternate TFTP auf "Yes" (Ja), und geben Sie die IP-Adresse des TFTP-Servers ein.



Konfigurieren von Cisco Unified Communications Manager

Schritt 1: Konfigurieren Sie die entsprechende Telefontastenvorlage für das IP-Telefon.

Phone Button Template Information

Button Template Name * Cisco 7925G

Button Information

Button	Feature
1	Line **
2	Line
3	Speed Dial
4	Privacy
5	Service URL
6	Speed Dial BLF
	Call Park BLF
	Intercom
	Mobility
	Do Not Disturb
	None

Save Delete Copy Reset Add New

Schritt 2: Fügen Sie das IP-Telefon dem CUCM hinzu.

Schritt 3: Füllen Sie die erforderlichen Felder aus.

Schritt 4: Weisen Sie die neu erstellte Telefontastenvorlage und Softkey-Vorlage zu.

Schritt 5: Verwenden Sie ein nicht sicheres Profil für das IP-Telefon.

Sicherheitsprofile können verwendet werden, um den authentifizierten Modus oder den verschlüsselten Modus zu aktivieren, in dem die Verschlüsselung von Signalisierungs-, Medien- und Konfigurationsdateien aktiviert wird. Die CAPF (Certificate Authority Proxy Function) muss aktiv sein, um ein LSC (Locally Signed Certificate) mit einem Sicherheitsprofil zu verwenden. Das Cisco Unified Wireless IP-Telefon 7925G, 7925G - E X und 7926 G verfügen über ein MIC (Manufacturing Installed Certificate), das auch mit einem Sicherheitsprofil verwendet werden kann.

Überprüfung

Sammeln Sie Konsolenprotokolle vom IP-Telefon. Es werden die verschiedenen Nachrichten angezeigt, die zwischen dem IP-Telefon und dem Access Point ausgetauscht werden.

Das IP-Telefon scannt die Medien auf eine verfügbare SSID.

```
09039 08-10 09:33:32.750 649 668 INF wlanmgr : [1298@wm_drv_mrvl.c] State change(1542),
DISCONNECTED -> SCANNING
09040 08-10 09:33:32.750 685 2805 DEB LibWifi : wifi_wait_for_event(CTRL-EVENT-STATE-CHANGE id=0
state=3)
09041 08-10 09:33:32.750 685 2805 DEB LibWifi : wifi_wait_for_event()
09042 08-10 09:33:35.390 1063 2652 INF Unknown : VVMService: Waiting for 39961 ms before
attempting to reconnect.
09043 08-10 09:33:35.468 685 807 DEB StateMachine: handleMessage: E msg.what=401431
09044 08-10 09:33:35.468 685 807 DEB StateMachine: processMsg: AdapterConnectedState
09045 08-10 09:33:35.468 685 807 VBS EthernetStateMachine: AdapterConnectedState{ what=401431
when=-1ms }
09046 08-10 09:33:35.468 685 807 DEB StateMachine: handleMessage: X
09047 08-10 09:33:36.617 649 664 INF wlanmgr : [1298@wm_drv_mrvl.c] State change(1559), SCANNING
-> INACTIVE
09048 08-10 09:33:36.617 210 313 INF SWMAN : nl_ipThrd():recvmsg() len=56
09049 08-10 09:33:36.617 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x1002
```

```
09050 08-10 09:33:36.617 210 313 INF SWMAN : Got a messge NEW_LINK message!!!
09051 08-10 09:33:36.617 685 2805 DEB LibWifi : wifi_wait_for_event(CTRL-EVENT-STATE-CHANGE id=0
state=2)
09052 08-10 09:33:36.617 685 2805 DEB LibWifi : wifi_wait_for_event()
09053 08-10 09:33:36.617 685 804 DEB EthernetStateMachine: Interface mlan0 LinkStateChanged:
down
```

Das IP-Telefon beginnt mit der Zuweisung zur SSID.

```
09054 08-10 09:33:36.718 649 668 INF wlanmgr : [1293@wm_drv_mrvl.c] State change(2221), "",
INACTIVE -> ASSOCIATING
09055 08-10 09:33:36.718 649 668 INF wlanmgr : [2226@wm_drv_mrvl.c] Connecting to "lcorrean
Wireless", a0:55:4f:c2:ec:eb, chan 56, rssi -56, load 4
09056 08-10 09:33:36.718 685 2805 DEB LibWifi : wifi_wait_for_event(CTRL-EVENT-STATE-CHANGE id=-
1 state=5)
09057 08-10 09:33:36.718 685 2805 DEB LibWifi : wifi_wait_for_event()
09058 08-10 09:33:36.734 2348 2348 VBS Settings.AccessPoint: refresh: for SSID lcorrean Wireless
09059 08-10 09:33:36.734 2348 2348 VBS Settings.CiscoWifiModifiable: Translating Wifi modifiable
state 0 for SSID: "lcorrean Wireless"
```

Das IP-Telefon ordnet dem Access Point erfolgreich zu.

```
09093 08-10 09:33:38.835 649 664 INF wlanmgr : [1293@wm_drv_mrvl.c] State change(2479),
"lcorrean Wireless", ASSOCIATING -> ASSOCIATED
09094 08-10 09:33:38.835 210 313 INF SWMAN : nl_ipThrd():recvmmsg() len=112
09095 08-10 09:33:38.835 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x1003
09096 08-10 09:33:38.835 210 313 INF SWMAN : Got a messge NEW_LINK message!!!
09097 08-10 09:33:38.835 210 313 INF SWMAN : nl_ipThrd():recvmmsg() len=80
09098 08-10 09:33:38.835 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x1003
09099 08-10 09:33:38.835 210 313 INF SWMAN : Got a messge NEW_LINK message!!!
09100 08-10 09:33:38.835 210 313 INF SWMAN : nl_ipThrd():recvmmsg() len=80
09101 08-10 09:33:38.835 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x1003
09102 08-10 09:33:38.835 210 313 INF SWMAN : Got a messge NEW_LINK message!!!
09103 08-10 09:33:38.835 210 313 INF SWMAN : nl_ipThrd():recvmmsg() len=132
09104 08-10 09:33:38.835 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x1003
09105 08-10 09:33:38.835 210 313 INF SWMAN : Got a messge NEW_LINK message!!!
09106 08-10 09:33:38.835 210 313 INF SWMAN : nl_ipThrd():recvmmsg() len=68
09107 08-10 09:33:38.835 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x1003
09108 08-10 09:33:38.835 210 313 INF SWMAN : Got a messge NEW_LINK message!!!
09109 08-10 09:33:38.835 685 804 DEB EthernetStateMachine: Interface mlan0 LinkStateChanged:
down
09110 08-10 09:33:38.843 685 804 DEB EthernetStateMachine: Interface mlan0 LinkStateChanged:
down
09111 08-10 09:33:38.843 685 2805 DEB LibWifi : wifi_wait_for_event(CTRL-EVENT-STATE-CHANGE id=1
state=6)
09112 08-10 09:33:38.843 685 804 DEB EthernetStateMachine: Interface mlan0 LinkStateChanged:
down
```

Das IP-Telefon startet die erweiterte Authentifizierung.

```
09146 08-10 09:33:39.039 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-
STARTED EAP authentication started
09147 08-10 09:33:39.039 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-
PROPOSED-METHOD vendor=0 method=25
09148 08-10 09:33:39.039 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-METHOD
EAP vendor 0 method 25 (PEAP) selected
09149 08-10 09:33:39.046 225 225 INF PAE : paeGetPort(): recvd macAddress: a0:55:4f:c2:ec:eb
09150 08-10 09:33:39.046 210 749 INF SWMAN : mdk_get_source_port(): mac = a0:55:4f:c2:ec:eb
09151 08-10 09:33:39.046 210 749 INF SWMAN : get_source_port(): START, MAC=0xa0554fc2eceb
09152 08-10 09:33:39.054 210 749 INF SWMAN : get_source_port(): DONE, cdk_port = -1, port = -1,
index = 2
```

```
09153 08-10 09:33:39.054 210 749 INF SWMAN : mdk_get_source_port(): rc = 0, port = -1
09154 08-10 09:33:39.054 225 225 INF PAE : paeGetPort(): 340 bytes rcvd from SWMAN, rcvLen: 340
09155 08-10 09:33:39.054 225 225 INF PAE : paeGetPort(): port obtained = -1
09156 08-10 09:33:39.054 225 225 WRN PAE : PAE rcv: msg received from unknown port, drop...
09157 08-10 09:33:39.125 225 225 INF PAE : paeGetPort(): recvd macAddress: a0:55:4f:c2:ec:eb
09158 08-10 09:33:39.125 2348 2348 VBS Settings.AccessPoint: refresh: for SSID lcorream Wireless
09159 08-10 09:33:39.125 2348 2348 VBS Settings.CiscoWifiModifiable: Translating Wifi modifiable
state 0 for SSID: "lcorream Wireless"
09160 08-10 09:33:39.125 2348 2348 VBS Settings.CiscoWifiModifiable: wifi configuration
modifiable state value= 0 internal string value: local
09161 08-10 09:33:39.125 210 749 INF SWMAN : mdk_get_source_port(): mac = a0:55:4f:c2:ec:eb
09162 08-10 09:33:39.125 210 749 INF SWMAN : get_source_port(): START, MAC=0xa0554fc2eceb
```

Das IP-Telefon überprüft das Serverzertifikat auf PEAP.

```
09163 08-10 09:33:39.132 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-PEER-
CERT depth=0 subject='/CN=CUCM-Srv-01.cucm.cotac.com'
09164 08-10 09:33:39.132 210 749 INF SWMAN : get_source_port(): DONE, cdk_port = -1, port = -1,
index = 2
09165 08-10 09:33:39.132 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-PEER-
CERT depth=0 subject='/CN=CUCM-Srv-01.cucm.cotac.com'
09166 08-10 09:33:39.132 210 749 INF SWMAN : mdk_get_source_port(): rc = 0, port = -1
09167 08-10 09:33:39.132 225 225 INF PAE : paeGetPort(): 340 bytes rcvd from SWMAN, rcvLen: 340
09168 08-10 09:33:39.132 225 225 INF PAE : paeGetPort(): port obtained = -1
09169 08-10 09:33:39.132 225 225 WRN PAE : PAE rcv: msg received from unknown port, drop...
09170 08-10 09:33:39.132 225 225 INF PAE : paeGetPort(): recvd macAddress: a0:55:4f:c2:ec:eb
09171 08-10 09:33:39.132 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-PEER-
CERT depth=0 subject='/CN=CUCM-Srv-01.cucm.cotac.com'
09172 08-10 09:33:39.140 210 749 INF SWMAN : mdk_get_source_port(): mac = a0:55:4f:c2:ec:eb
09173 08-10 09:33:39.140 210 749 INF SWMAN : get_source_port(): START, MAC=0xa0554fc2eceb
09174 08-10 09:33:39.148 210 749 INF SWMAN : get_source_port(): DONE, cdk_port = -1, port = -1,
index = 2
09175 08-10 09:33:39.148 210 749 INF SWMAN : mdk_get_source_port(): rc = 0, port = -1
09176 08-10 09:33:39.148 225 225 INF PAE : paeGetPort(): 340 bytes rcvd from SWMAN, rcvLen: 340
09177 08-10 09:33:39.148 225 225 INF PAE : paeGetPort(): port obtained = -1
```

Die erweiterte Authentifizierung verläuft erfolgreich.

```
09226 08-10 09:33:39.312 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: EAP-
SUCCESS EAP authentication completed successfully
09227 08-10 09:33:39.312 210 749 INF SWMAN : mdk_get_source_port(): mac = a0:55:4f:c2:ec:eb
09228 08-10 09:33:39.312 210 749 INF SWMAN : get_source_port(): START, MAC=0xa0554fc2eceb
09229 08-10 09:33:39.320 649 664 INF wlanmgr : [3492@wm_drv_mrvl.c] Supplicant event: CONNECTED
- Connection to a0:55:4f:c2:ec:eb completed (auth) [id=0 id_str=]
```

Verbindung erfolgreich.

```
09230 08-10 09:33:39.320 649 664 INF wlanmgr : [1293@wm_drv_mrvl.c] State change(2592),
"lcorream Wireless", ASSOCIATED -> CONNECTED
09231 08-10 09:33:39.320 210 749 INF SWMAN : get_source_port(): DONE, cdk_port = -1, port = -1,
index = 2
09232 08-10 09:33:39.320 649 664 INF wlanmgr : [56@wm_util.c] Wifi connected[lcorream Wireless]:
a0:55:4f:c2:ec:eb, co-cucm, Ch: 56, RSSI: -57
09233 08-10 09:33:39.320 210 749 INF SWMAN : mdk_get_source_port(): rc = 0, port = -1
09234 08-10 09:33:39.320 225 225 INF PAE : paeGetPort(): 340 bytes rcvd from SWMAN, rcvLen: 340
09235 08-10 09:33:39.320 225 225 INF PAE : paeGetPort(): port obtained = -1
09236 08-10 09:33:39.320 225 225 WRN PAE : PAE rcv: msg received from unknown port, drop...
09237 08-10 09:33:39.320 225 225 INF PAE : paeGetPort(): recvd macAddress: a0:55:4f:c2:ec:eb
09238 08-10 09:33:39.320 685 804 DEB EthernetStateMachine: Interface mlan0 LinkStateChanged: up
09239 08-10 09:33:39.320 210 313 INF SWMAN : nl_ipThrd():rcvmsg() len=1012
09240 08-10 09:33:39.320 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x11043
```

09241 08-10 09:33:39.320 210 313 INF SWMAN : Got a messge NEW_LINK message!!!

Das IP-Telefon sucht nach einem DHCP-Lease.

```
09588 08-10 09:33:39.703 3246 3246 DEB dhcpcd : broadcasting for a lease of 192.168.110.236
09589 08-10 09:33:39.703 3246 3246 DEB dhcpcd : Starting to send message numberof message=0
09590 08-10 09:33:39.703 3246 3246 DEB dhcpcd : REQUESTING SENT
09591 08-10 09:33:39.703 3246 3246 DEB dhcpcd : STATE_RENEWING STATE_REBINDING mlan0
09592 08-10 09:33:39.703 3246 3246 DEB dhcpcd : *sending DHCP_REQUEST with xid 0xc89244e9, next
in 3.57 seconds
09593 08-10 09:33:39.703 3246 3246 DEB dhcpcd : get_tos_byte() = 96
09594 08-10 09:33:39.703 3246 3246 DEB dhcpcd : Set ToS byte for DHCP to configured value of
[96]
09595 08-10 09:33:39.703 2348 2348 VBS Settings.AccessPoint: onBindView: [lcorream Wireless]
modifiable state was empty, setting visibility to gone
09596 08-10 09:33:39.710 2348 2348 VBS Settings.AccessPoint: onBindView: [lcorream Wireless]
modifiable state was empty, setting visibility to gone
09597 08-10 09:33:39.718 2348 2348 VBS Settings.AccessPoint: onBindView: [lcorream Wireless]
modifiable state was empty, setting visibility to gone
09598 08-10 09:33:39.726 2348 2348 VBS Settings.AccessPoint: onBindView: [CUCM-PEAP] modifiable
state was empty, setting visibility to gone
09599 08-10 09:33:39.734 2348 2348 VBS Settings.AccessPoint: onBindView: [CUCM-LAB] modifiable
state was empty, setting visibility to gone
09600 08-10 09:33:39.742 2348 2348 VBS Settings.AccessPoint: onBindView: [Kemirand] modifiable
state was empty, setting visibility to gone
09601 08-10 09:33:39.750 2348 2348 VBS Settings.AccessPoint: onBindView: [Flex_Guest] modifiable
state was empty, setting visibility to gone
09603 08-10 09:33:39.765 2348 2348 VBS Settings.AccessPoint: onBindView: [ASA5506W-A] modifiable
state was empty, setting visibility to gone
09604 08-10 09:33:39.906 3246 3246 DEB dhcpcd : in handle_dhcp_packet...
09604 08-10 09:33:39.906 3246 3246 DEB dhcpcd :
09605 08-10 09:33:39.906 3246 3246 DEB dhcpcd : in handle_dhcp
```

Das IP-Telefon erhält eine Rückmeldung vom DHCP-Server.

```
09606 08-10 09:33:39.906 3246 3246 DEB dhcpcd : acknowledged 192.168.110.236 from
192.168.110.122.
09607 08-10 09:33:39.906 3246 3246 DEB dhcpcd : cont_init_retry = OLD:0 NEW:0
09608 08-10 09:33:39.976 3246 3246 DEB dhcpcd : handle_timeout:ifname mlan0 state: 9
09609 08-10 09:33:40.046 3246 3246 DEB dhcpcd : checking 192.168.110.236 is available on
attached networks
09610 08-10 09:33:40.046 3246 3246 DEB dhcpcd : DBG:checking 192.168.110.236 is available on
attached networks
```

Das IP-Telefon sendet ein unentgeltliches ARP, um zu bestätigen, dass die IP tatsächlich verfügbar ist.

```
09611 08-10 09:33:40.046 3246 3246 DEB dhcpcd : sending ARP probe (1 of 2), next in 1.94 seconds
09612 08-10 09:33:40.468 685 807 DEB StateMachine: handleMessage: E msg.what=401431
09613 08-10 09:33:40.468 685 807 DEB StateMachine: processMsg: AdapterConnectedState
09614 08-10 09:33:40.468 685 807 VBS EthernetStateMachine: AdapterConnectedState{ what=401431
when=-5ms }
09615 08-10 09:33:40.468 685 807 DEB StateMachine: handleMessage: X
09616 08-10 09:33:41.992 3246 3246 DEB dhcpcd : handle_timeout:ifname mlan0 state: 9
09617 08-10 09:33:41.992 3246 3246 DEB dhcpcd : sending ARP probe (2 of 2), next in 2.00 seconds
09618 08-10 09:33:43.992 3246 3246 DEB dhcpcd : handle_timeout:ifname mlan0 state: 9
09619 08-10 09:33:43.992 3246 3246 DEB dhcpcd : binding the DHCP IP address Probe=2
09620 08-10 09:33:43.992 3246 3246 DEB dhcpcd : startup 0 lease of 600
09621 08-10 09:33:43.992 3246 3246 DEB dhcpcd : get_option2addr: 2054072512
09622 08-10 09:33:43.992 3246 3246 DEB dhcpcd : get_option2addr: 134744072
09623 08-10 09:33:43.992 3246 3246 DEB dhcpcd : leased 192.168.110.122 for 600 seconds....server
```

```
192.168.110.122
09624 08-10 09:33:43.992 3246 3246 DEB dhcpd : Check values : state=3 mlan0 192.168.110.122
300/600 192.168.110.236
09625 08-10 09:33:43.992 3246 3246 DEB dhcpd : executing `'/system/etc/dhcpd/dhcpd-run-hooks',
reason BOUND
09626 08-10 09:33:43.992 3246 3246 DEB dhcpd : Entering configure_env....
```

Das IP-Telefon erhält eine Nachricht mit DHCP-Optionen.

```
09627 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 1*: new_subnet_mask=255.255.255.0
09628 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 150*:
new_cisco_tftp_server=192.168.110.86
09629 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 3*: new_routers=192.168.110.1
09630 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 6*:
new_domain_name_servers=192.168.110.122 8.8.8.8
09631 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 15*: new_domain_name=cucm.cotac.com
09632 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 51*: new_dhcp_lease_time=600
09633 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 53*: new_dhcp_message_type=5
09634 08-10 09:33:43.992 3246 3246 DEB dhcpd : option 54*:
new_dhcp_server_identifizier=192.168.110.122
09635 08-10 09:33:44.257 3246 3246 DEB dhcpd : configure: mlan0 adding IP address
192.168.110.236
09636 08-10 09:33:44.265 3246 3246 DEB dhcpd : adding route to 0.0.0.0/0 via 192.168.110.1
09637 08-10 09:33:44.265 3246 3246 DEB dhcpd : Writing lease file:
/dataRoot/.system/misc/dhcp/dhcpd-mlan0.lease
09638 08-10 09:33:44.265 3246 3246 DEB dhcpd : executing `'/system/etc/dhcpd/dhcpd-run-hooks',
reason BOUND
09639 08-10 09:33:44.265 3246 3246 DEB dhcpd : Entering configure_env....
09640 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 1*: new_subnet_mask=255.255.255.0
09641 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 150*:
new_cisco_tftp_server=192.168.110.86
09642 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 3*: new_routers=192.168.110.1
09643 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 6*:
new_domain_name_servers=192.168.110.122 8.8.8.8
09644 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 15*: new_domain_name=cucm.cotac.com
09645 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 51*: new_dhcp_lease_time=600
09646 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 53*: new_dhcp_message_type=5
09647 08-10 09:33:44.265 3246 3246 DEB dhcpd : option 54*:
new_dhcp_server_identifizier=192.168.110.122
09648 08-10 09:33:44.265 214 241 INF NETSD : nl_ipThrd():recvmmsg() len=60
09649 08-10 09:33:44.265 210 313 INF SWMAN : nl_ipThrd():recvmmsg() len=56
09650 08-10 09:33:44.265 210 313 INF SWMAN : NL event: 16 found; device idx:6 flag :0x11043
09651 08-10 09:33:44.265 210 313 INF SWMAN : Got a message NEW_LINK message!!!
09652 08-10 09:33:44.265 685 2805 DEB LibWifi : wifi_wait_for_event(CTRL-EVENT-SCAN-RESULTS
Ready)
09653 08-10 09:33:44.265 685 2805 DEB LibWifi : wifi_wait_for_event()
09654 08-10 09:33:44.265 685 804 DEB EthernetStateMachine: Interface mlan0 LinkStateChanged: up
09655 08-10 09:33:44.398 685 3245 INF dhcp_utils: DHCP is started OK
09656 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 IP
address = 192.168.110.236
09657 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4
Gateway = 192.168.110.1
09658 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 DNS 1
= 192.168.110.122
09659 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 DNS 2
= 8.8.8.8
09660 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 Server
Address = 192.168.110.122
09661 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 Vendor
Info =
09662 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 Domain
Name = cucm.cotac.com
09663 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 TFTP 1
```

```
= 192.168.110.86
09664 08-10 09:33:44.398 685 3245 DEB NetUtils: android_net_utils_runDhcpCommon() Ipver:4 TFTP 2
=
09665 08-10 09:33:44.398 685 3245 DEB DhcpStateMachine: DHCP succeeded on mlan0 IPv4
09666 08-10 09:33:44.398 685 3245 DEB DhcpStateMachine: RunningState: 4
```

Das IP-Telefon fordert zunächst Dateien für Identity Trust List (ITL) und Certificate Trust List (CTL) an.

```
10276 08-10 09:33:47.632 3329 3329 INF dgetfile: GETXXTP
[GT3329][src=CTLSEP00CCFC4ACCD2.tlv][dest=/data/data/cip.cfg/app_cip.tftp/CTLSEP00CCFC4ACCD2.tlv
][serv=][serv6=][sec=0]
10277 08-10 09:33:47.632 3329 3329 INF dgetfile: In normal mode, call - > makeXXTPrequest (...)
10278 08-10 09:33:47.632 3329 3329 INF dgetfile: DTRACE [GT3329]makeXXTPrequest
10279 08-10 09:33:47.632 3329 3329 INF dgetfile: DTRACE [GT3329]parseEMCCConfig
10280 08-10 09:33:47.632 3329 3329 INF dgetfile: EMCC mode is false
10281 08-10 09:33:47.632 3329 3329 INF dgetfile: DTRACE [GT3329]parseDhcpInfoIntoTftpList
10282 08-10 09:33:47.632 3329 3329 INF dgetfile: Using WIRELESS interface for dhcp properties:
ok
10283 08-10 09:33:47.632 3329 3329 INF dgetfile: cisco_tftp_server2 unavailable:
10284 08-10 09:33:47.632 927 1611 ERR SQLiteLog: (1) table 'device' already exists
```

Das IP-Telefon sucht nach aktiven CUCM-Servern, auf denen sich diese registrieren können.

```
10361 08-10 09:33:47.640 1095 1540 INF ccservice-j: TelephonyManagerData: : fetchCallServerInfos
svrHndls[1]=1584903492 mode=CCM status=ACTIVE CallServerInfo=[192.168.110.86, CCM, ACTIVE]
10362 08-10 09:33:47.640 1095 1540 DEB ccservice: SIPCC-SIP_CC_PROV: 0x5e77b5bc,
CCAPI_DeviceInfo_getCallServerName: returned ipv4 192.168.110.84
10363 08-10 09:33:47.640 1095 1540 DEB ccservice: SIPCC-SIP_CC_PROV: 0x5e77b5bc,
CCAPI_DeviceInfo_getCallServerMode: returned 02
10364 08-10 09:33:47.640 1095 1540 DEB ccservice: SIPCC-SIP_CC_PROV: 0x5e77b5bc,
CCAPI_DeviceInfo_getCallServerStatus: returned 00
10365 08-10 09:33:47.640 1095 1540 INF ccservice-j: TelephonyManagerData: : fetchCallServerInfos
svrHndls[2]=1584903612 mode=NONCCM status=NONE CallServerInfo=[192.168.110.84, NONCCM, NONE]
```

Fehlerbehebung

Das Cisco Unified IP-Telefon 9971 stellt Geräteinformationen bereit, in denen Netzwerkstatus, MAC-Adresse, Versionsinformationen, Unified Communications, Stream Statistics und WLAN-Statistiken angezeigt werden. Navigieren Sie zur Webschnittstelle (<http://x.x.x.x>) des IP-Telefons, und wählen Sie die Informationen aus, die Sie überprüfen möchten.

Geräteinformationen



Device Information

Cisco IP Phone CP-9971 (SEP1C17D3405C6B)

Device Information

Network Setup

Ethernet Statistics

Ethernet Information

Access

Network

WLAN Setup

Current AP

WLAN Statistics

Device Logs

Console Logs(Console Logs)

Core Dumps(Core Dumps)

Status Messages

WLAN Site Survey

Debug Display

Streaming Statistics

Stream 1

Stream 2

Stream 3

Stream 4

Stream 5

Stream 6

Active Network Interface	WLAN
MAC Address	1C17D3405C6B
WLAN MAC Address	8843E171EEC6
Host Name	SEP1C17D3405C6B
Phone DN	89023675
Version	slp9971.9-3-2-10
Key Expansion Module 1	
Key Expansion Module 2	
Key Expansion Module 3	
Hardware Revision	9.0
Serial Number	FCH141788XX
Model Number	CP-9971
Message Waiting	No
UDI	phone Cisco IP Phone 9971, Global CP-9971 FCH141788XX
Camera UDI	CP-CAM-G= ASK132601EF V01
Time	7:00:24p
Time Zone	America/New_York
Date	05/10/13

Netzwerkeinrichtung



Network Setup

Cisco IP Phone CP-9971 (SEP1C17D3405C6B)

Device Information	DHCP Server	10.116.167.193
Network Setup	BOOTP Server	No
Ethernet Statistics	MAC Address	8843E171EEC6
Ethernet Information	Host Name	SEP1C17D3405C6B
Access	Domain Name	cisco.com
Network	IP Address	10.116.167.197
WLAN Setup	Subnet Mask	255.255.255.240
Current AP	TFTP Server 1	10.35.48.106
WLAN Statistics	Default Router	10.116.167.193
Device Logs	DNS Server 1	64.102.6.247
Console Logs(Console Logs)	DNS Server 2	161.44.124.122
Core Dumps(Core Dumps)	DNS Server 3	
Status Messages	Operational VLAN Id	4095
WLAN Site Survey	Admin. VLAN Id	4095
Debug Display	CUCM Server1	gigantic-7 Active
Streaming Statistics	CUCM Server2	gigantic-8 Standby
Stream 1	CUCM Server3	
Stream 2	CUCM Server4	
Stream 3	CUCM Server5	
Stream 4	Information URL	https://10.35.48.106:8443/ccmclp/GetTelecasterHelpText.jsp
Stream 5	Directories URL	https://10.35.48.106:8443/ccmclp/xmldirectory.jsp
Stream 6	Messages URL	
	Services URL	https://10.35.48.106:8443/ccmclp/getservicesmenu.jsp
	DHCP Enabled	Yes
	DHCP Address Released	No
	Alternate TFTP	Yes
	Forwarding Delay	No
	Idle URL	
	Idle URL Time	0
	Proxy Server URL	
	Authentication URL	https://10.35.48.106:8443/ccmclp/authenticate.jsp

WLAN-Statistiken



WLAN Statistics

Cisco IP Phone CP-9971 (SEP1C17D3405C6B)

Device Information

Network Setup

Ethernet Statistics

Ethernet Information

Access

Network

WLAN Setup

Current AP

WLAN Statistics

Device Logs

Console Logs(Console Logs)

Core Dumps(Core Dumps)

Status Messages

WLAN Site Survey

Debug Display

Streaming Statistics

Stream 1

Stream 2

Stream 3

Stream 4

Stream 5

Stream 6

Transmit Frames:	00106929
Directed Frames Received:	00104213
Multicast Frames Received:	00000000
Broadcast Frames Received:	00002716
Receive Errors:	00000000
Receive No Buffers:	00000000
FCS Errors:	00000000
Duplicate Frames:	00000000
Fragments Received:	00000000
Beacons Received:	08996244
Association Rejected:	00000002
Association Timeouts:	00000000
Authentication Rejects:	00000000
Authentication Timeouts:	00000000
QOS Null Frames:	00001768
Background	
QOS Data Received:	00000000
Transmit Ok:	00000000
Transmit Error:	00000000
Direct Frames Transmitted:	00000000
Multicast Frames Transmitted:	00000000
Broadcast Frames Transmitted:	00000000
RTS Failed:	00000000
ACK Failed:	00000000
Retries:	00000000
Multiple Retries:	00000000
Retry Failures:	00000000
Transmit Timeouts:	00000000
Other Failures:	00000000
Success counter:	00000000
Max Retry Failure:	00000000

Streaming-Statistiken



Streaming Statistics

Cisco IP Phone CP-9971 (SEP1C17D3405C6B)

Device Information	Remote Address	10.55.216.114/27520
Network Setup	Local Address	10.116.167.197/20640
Ethernet Statistics	Start Time	12:08:42p
Ethernet Information	Stream Status	Not Ready
Access	Host Name	SEP1C17D3405C6B
Network	Sender Packets	30250
WLAN Setup	Sender Octets	4840000
Current AP	Sender Codec	G.722
WLAN Statistics	Sender Reports Sent	111
Device Logs	Sender Report Time Sent	12:18:46p
Console Logs(Console Logs)	Rcvr Lost Packets	215
Core Dumps(Core Dumps)	Avg Jitter	11
Status Messages	Rcvr Codec	G.722
WLAN Site Survey	Rcvr Reports Sent	0
Debug Display	Rcvr Report Time Sent	00:00:00
Streaming Statistics	Rcvr Packets	30029
Stream 1	Rcvr Octets	5164988
Stream 2	MOS LQK	4.3828
Stream 3	Avg MOS LQK	4.2019
Stream 4	Min MOS LQK	3.4758
Stream 5	Max MOS LQK	4.5000
Stream 6	MOS LQK Version	0.95
	Cumulative Conceal Ratio	0.0090
	Interval Conceal Ratio	0.0066
	Max Conceal Ratio	0.0863
	Conceal Secs	210
	Severely Conceal Secs	15
	Latency	149
	Max Jitter	148
	Sender Size	20 ms
	Sender Reports Received	33
	Sender Report Time Received	12:18:45p
	Rcvr Size	20 ms
	Rcvr Discarded	1

Geräteprotokolle

Konsolenprotokolle, Core Dumps und Statusmeldungen zur Fehlerbehebung können über die Webschnittstelle des IP-Telefons abgerufen werden. Navigieren Sie zur Webschnittstelle (<http://x.x.x.x>) des IP-Telefons, und wählen Sie dann die erforderlichen Menüoptionen unter Geräteprotokolle aus, um diese Informationen anzuzeigen.



Console Logs

Cisco IP Phone CP-9971 (SEP1C17D3405C6B)

- Device Information
- Network Setup
- Ethernet Statistics
 - Ethernet Information
 - Access
 - Network
- WLAN Setup
 - Current AP
 - WLAN Statistics
- Device Logs
 - Console Logs(Console Logs)
 - Core Dumps(Core Dumps)
 - Status Messages
 - WLAN Site Survey
 - Debug Display
- Streaming Statistics
 - Stream 1
 - Stream 2
 - Stream 3
 - Stream 4
 - Stream 5
 - Stream 6

Current logs in /var/log:

[messages](#)
[messages.0](#)
[messages.1](#)
[messages.2](#)
[messages.3](#)
[messages.4](#)
[messages.5](#)
[messages.6](#)
[messages.7](#)

Archived logs in /cisco/logsave/hourly:

[hourly_20130510_230102.tar.gz](#)
[hourly_20130510_220101.tar.gz](#)
[hourly_20130510_210102.tar.gz](#)
[hourly_20130510_200101.tar.gz](#)
[hourly_20130510_190101.tar.gz](#)
[hourly_20130510_180101.tar.gz](#)
[hourly_20130510_170101.tar.gz](#)
[hourly_20130510_160102.tar.gz](#)
[hourly_20130510_150101.tar.gz](#)
[hourly_20130510_140101.tar.gz](#)
[hourly_20130510_130101.tar.gz](#)
[hourly_20130510_120102.tar.gz](#)
[hourly_20130510_110102.tar.gz](#)
[hourly_20130510_100102.tar.gz](#)
[hourly_20130510_090101.tar.gz](#)
[hourly_20130510_080101.tar.gz](#)
[hourly_20130510_070101.tar.gz](#)
[hourly_20130510_060101.tar.gz](#)
[hourly_20130510_050102.tar.gz](#)
[hourly_20130510_040101.tar.gz](#)
[hourly_20130510_030102.tar.gz](#)
[hourly_20130510_020101.tar.gz](#)
[hourly_20130510_010101.tar.gz](#)
[hourly_20130510_000101.tar.gz](#)

Archived logs in /cisco/logsave/lastimage:

[lastimage_20130510_191537.tar.gz](#)

WLAN-Signalanzeige

Ab Version 9.0(2) wird die WLAN-Statusanzeige in allen Menüs in den Administratoreinstellungen angezeigt. In der ersten Version war die WLAN-Signalanzeige nur im Menü "WLAN Setup" (WLAN-Einrichtung) sichtbar.

02/04/2010 19:04 | 23675

Administrator Settings



23

Please Select a menu item

Network Setup



1

Security Setup



2

Status



3

Reset Settings



4

Exit

