

Configurazione e risoluzione dei problemi di registrazione di telefoni IP wireless

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Cisco Unified Wireless LAN Controller e Access Point](#)

[Impostazioni WLAN \(Wireless Local Area Network\)](#)

[Impostazioni controller](#)

[Impostazioni di rete 802.11](#)

[Configurazione di Cisco Unified 9971 IP Phone](#)

[Impostazioni LAN wireless](#)

[Configurazione di Cisco Unified Communications Manager](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi alla registrazione di telefoni IP wireless in Cisco Unified Communications Manager (CUCM).

I telefoni IP wireless Cisco sono adattabili agli utenti che devono poter scollegare la connessione alla rete cablata e rimanere connessi.

Contributo di Luis Segnini e Kenny Araya, tecnici Cisco TAC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Architettura wireless
- Configurazione di telefoni IP wireless
- Configurazione base CUCM

Componenti usati

- Cisco Unified Communications Manager 8.6 o versioni successive
- Modelli di telefoni IP wireless (792X, 9971, 8821)

La guida seguente è basata sul modello di telefono IP Cisco Unified 9971. La configurazione può variare a seconda del modello di telefono IP.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Cisco Unified Wireless LAN Controller e Access Point

Impostazioni WLAN (Wireless Local Area Network)

È consigliabile disporre di un SSID (Service Set Identifier) distinto per il telefono IP. Tuttavia, se esiste già un SSID configurato per supportare endpoint LAN wireless Cisco con funzionalità voce, è possibile utilizzare tale WLAN.

L'SSID che deve essere utilizzato dal telefono IP può essere configurato per essere applicato solo a un determinato tipo di radio 802.11.

Si consiglia di far funzionare il telefono IP sulla banda dei 5 GHz in quanto ha molti canali disponibili e non così tanti interferitori come la banda dei 2.4 GHz.

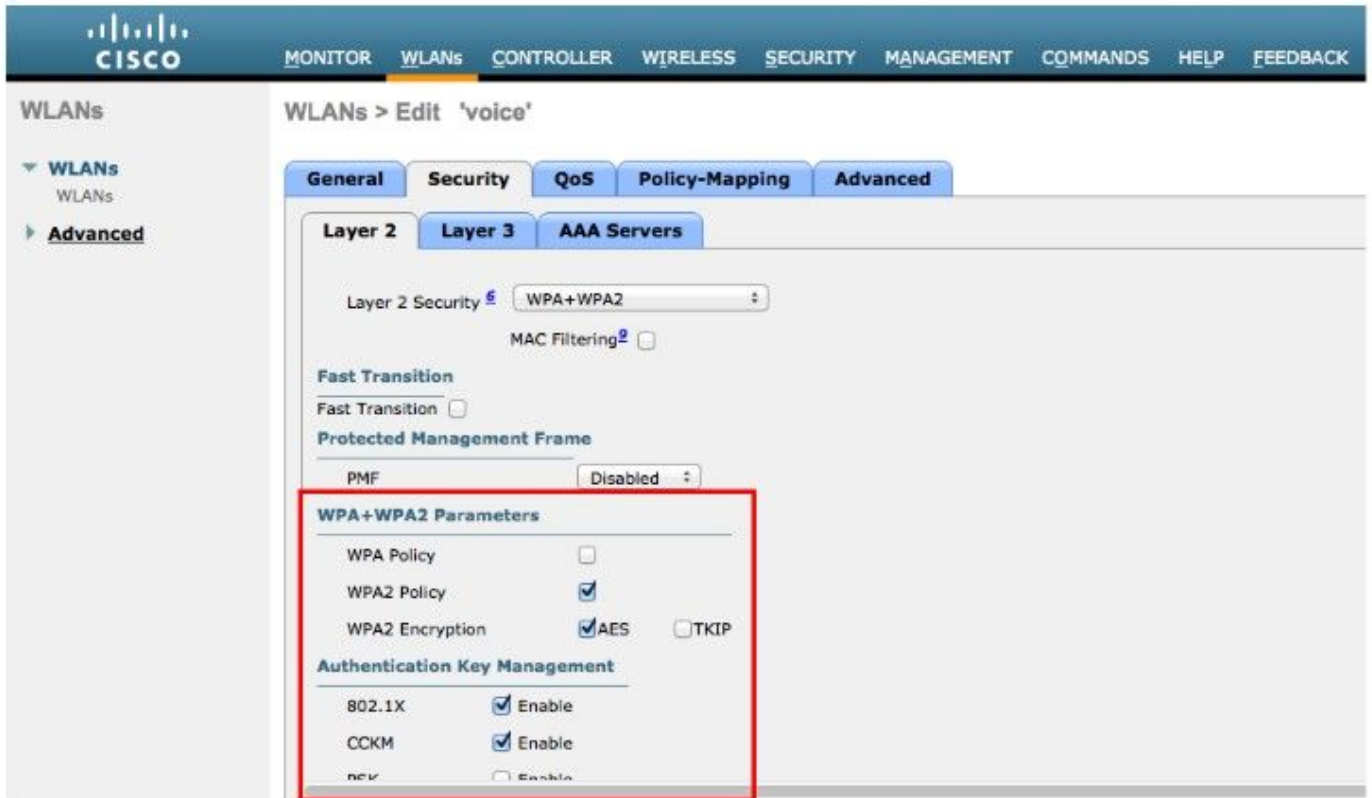
accertarsi che l'SSID selezionato non sia utilizzato da altre LAN wireless in quanto potrebbe causare guasti all'accensione o durante il roaming; in particolare se viene utilizzato un tipo di protezione diverso.

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 left sidebar shows 'WLANs' with a sub-menu 'Advanced'. The main content area is titled 'WLANs > Edit 'voice'' and has tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'Security' tab is active. The configuration details are as follows:

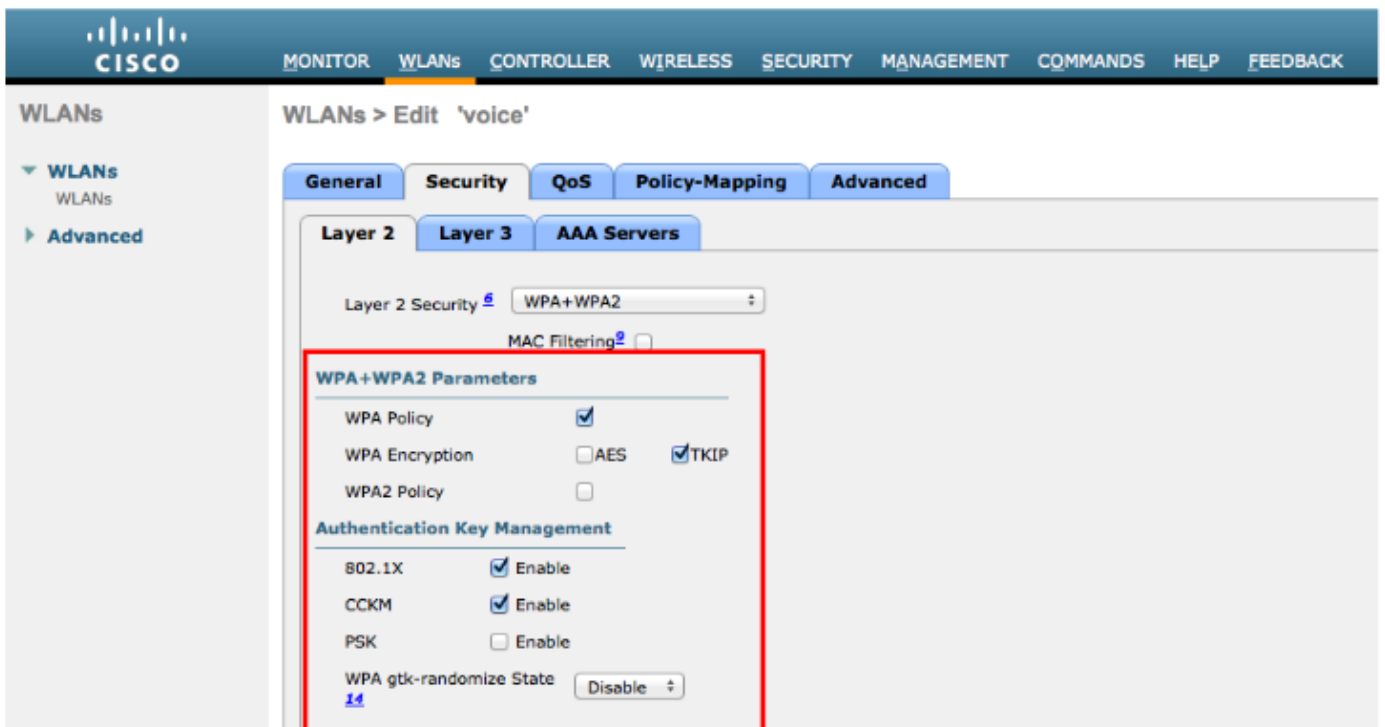
Profile Name	voice
Type	WLAN
SSID	voice
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X + CCKM)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	802.11a only
Interface/Interface Group(G)	rtp-9 voice
Multicast Vlan Feature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

Per utilizzare la funzionalità Cisco Centralized Key Management (CCKM), abilitare la policy Wi-Fi Protected Access (WPA) 2 con la crittografia AES (Advanced Encryption Standard) e la crittografia

802.1x + CCKM per il tipo di gestione delle chiavi autenticate quando il telefono IP esegue la versione firmware 9.1(1) o successive, al fine di abilitare il roaming veloce e sicuro.



Se sul telefono IP è in esecuzione una versione firmware precedente alla 9.1(1), abilitare la policy WPA con crittografia TKIP (Temporal Key Integrity Protocol) e 802.1x + CCKM per il tipo di gestione delle chiavi autenticate per consentire un roaming veloce e sicuro.



Il criterio Wi-Fi Multimedia (WMM) deve essere impostato su "Obbligatorio" solo se il telefono IP o altri telefoni abilitati per WMM utilizzeranno questo SSID. Se nella WLAN non sono presenti client WMM, si consiglia di collocarli su un altro SSID/WLAN. Se client WMM diversi devono utilizzare lo stesso SSID del telefono IP, verificare che il criterio WMM sia impostato su "Consentito".

Abilitare 7920 Access Point (AP) Call Admission Control (CAC) per annunciare QoS Basic Service Set (QoS) al client.

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 '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 for both DownStream and UpStream directions.

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 the 'WMM' section, '7920 AP CAC' is checked and 'Enabled', while '7920 Client CAC' is unchecked. Below the WMM section, the 'Media Stream' section has 'Multicast Direct' checked and 'Enabled'. The 'QoS' tab is still selected, and the 'Burst Real-Time Rate' input fields are visible at the top of the configuration area.

Configurare Abilita timeout sessione in base alle proprie esigenze.

Si consiglia di disattivare il timeout della sessione o di estenderlo (ad esempio, 24 ore / 86400 secondi) per evitare possibili interruzioni durante le chiamate audio. Se disabilitata, evita qualsiasi

potenziale interruzione, ma il timeout della sessione può aiutare a riconvalidare periodicamente le credenziali del client per garantire che il client utilizzi credenziali valide.

È necessario disabilitare l'azione di blocco Enable Aironet Extensions (Aironet IE) e Peer to Peer (P2P). Configurare l'esclusione del client in base alle esigenze, è possibile impostare il posticipo scansione off-channel per posticipare la scansione di determinate code e il tempo di posticipo della scansione.

È possibile configurare il numero massimo di client consentiti per radio AP in base alle esigenze.

L'assegnazione degli indirizzi DHCP (Dynamic Host Configuration Protocol) richiesta deve essere disabilitata.

Management Frame Protection deve essere impostato su "Optimal" o "Disabled".

Per prestazioni ottimali della batteria e qualità ottimale, utilizzare un periodo DTIM (Delivery Traffic Indication Message) di 2 con un periodo di beacon di 100 ms.

Assicurarsi che le opzioni Bilanciamento carico e Selezione banda client siano disattivate.

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:** Unchecked.
- Maximum Allowed Clients Per AP Radio:** Set to 20.
- DHCP:** DHCP Server Override is unchecked, and DHCP Address Assignment Required is unchecked.
- Management Frame Protection (MFP):** MFP Client Protection is set to Optional. DTIM Period for 802.11a/n and 802.11b/g/n is set to 2.

The screenshot shows the Cisco WLAN configuration interface for a 'voice' WLAN, continuing from the previous view. 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. The Scan Defer Time is set to 100 msec.
- FlexConnect:** FlexConnect Local Switching, FlexConnect Local Auth, and Learn Client IP Address are all checked and Enabled.
- Load Balancing and Band Select:** Client Load Balancing and Client Band Select are both unchecked.
- Voice:** Media Session Snooping, Re-anchor Roamed Voice Clients, and KTS based CAC Policy are all checked and Enabled.

Impostazioni controller

Verificare che il nome host del controller Cisco Unified Wireless LAN sia configurato correttamente.

Abilitare il LAG (Link Aggregation) se si utilizzano più porte sul Cisco Unified Wireless LAN Controller.

Configurare la modalità multicast AP desiderata. Nelle versioni precedenti alla 6.0, il bilanciamento del carico aggressivo era configurato nelle impostazioni del controller generale. Nella versione 6.0

e successive, questo processo è noto come bilanciamento del carico del client ed è configurabile nella configurazione WLAN (impostazioni SSID).

The screenshot shows the Cisco Controller configuration interface. The 'General' tab is selected, and the 'LAG Mode on next reboot' option is highlighted with a red box. The value is set to 'Enabled', and 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 (seconds): 300, ARP Timeout (seconds): 300, Web Radius Authentication: PAP, Operating Environment: Commercial (0 to 40 C), 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, HA SKU secondary unit: Disabled.

Impostazioni di rete 802.11

Se si utilizzano 5 GHz, verificare che lo stato della rete 802.11a sia "Abilitato". Impostare il periodo beacon su 100 ms.

Verificare che il supporto DTPC (Dynamic Transmit Power Control) sia abilitato. Se si utilizzano punti di accesso Cisco 802.11n, verificare che ClientLink sia abilitato. Nelle versioni correnti è possibile configurare il numero massimo di client autorizzati.

si consiglia di impostare 12 Mbps come velocità obbligatoria (di base) e 18 - 24 o 18 - 54 Mbps come velocità supportata (opzionale); tuttavia, alcuni ambienti potrebbero richiedere l'attivazione di 6 Mbps come obbligatorio (standard). 36 - 54 Mbps può essere disabilitato, se non vi sono applicazioni che possono beneficiare di queste velocità (ad esempio video).

Abilitare CCX Location Measurement.

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
- Mesh
- RF Profiles
- FlexConnect Groups
 - FlexConnect ACLs
- 802.11a/n/ac
 - Network
 - RRM
 - RF Grouping
 - TPC
 - DCA

Configurazione di Cisco Unified 9971 IP Phone

Per configurare le impostazioni Wi - Fi sul telefono IP, usare il tastierino e lo schermo tattile per selezionare Applications Button > Administrator Settings > Network Setup > WLAN Setup.

Impostazioni LAN wireless

Per configurare il profilo LAN wireless, attenersi alle seguenti linee guida.

- Assicurarsi che Wireless sia impostato su "On".
- L'opzione Accesso WLAN può essere impostata su On per fornire l'accesso rapido nel menu Applications per aggiornare il nome utente o la password.
- Immettere l'SSID per la LAN wireless vocale, che fa distinzione tra maiuscole e minuscole.

Cisco Unified 9971 IP Phone supporta un singolo profilo LAN wireless che consente un singolo SSID.

Sono disponibili tre diverse modalità 802.11.

- Auto
- 802.11a
- 802.11b/g

La modalità automatica esegue la scansione dei canali a 2,4 e 5 GHz e tenta di associare il punto di accesso con un segnale a 5 GHz se la rete configurata è disponibile.

La modalità 802.11a esegue la scansione solo dei canali a 5 GHz e la modalità 802.11b/g esegue la scansione solo dei canali a 2,4 GHz; quindi, se la rete configurata è disponibile, tenta di associarsi a un punto di accesso.

Configurare il telefono IP in modo che utilizzi Apri con WEP (Wired Equivalent Privacy) o Chiave condivisa per la modalità di protezione, immettere le informazioni della chiave WEP statica che corrispondono alla configurazione del punto di accesso.

- Nella configurazione IPv4, selezionare se usare DHCP o configurare le informazioni IP statiche.
- Se le opzioni 150 o 66 non sono configurate per fornire l'indirizzo IP del server Trivial File Transfer Protocol (TFTP) tramite l'ambito DHCP della rete, impostare Alternate TFTP su "Sì" e immettere l'indirizzo IP del server TFTP.



Configurazione di Cisco Unified Communications Manager

Passaggio 1. Configurare il modello del pulsante Telefono appropriato per il telefono IP.

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

Passaggio 2. Aggiungere il telefono IP a CUCM.

Passaggio 3. Completare i campi obbligatori.

Passaggio 4. Assegnare il nuovo modello di pulsante telefonico e il nuovo modello di tasto softkey.

Passaggio 5. Utilizzare un profilo non sicuro per il telefono IP.

I profili di sicurezza possono essere utilizzati per abilitare la modalità autenticata o crittografata, in cui la segnalazione, i supporti e la crittografia dei file di configurazione sono abilitati. La funzione CAPF (Certification Authority Proxy Function) deve essere operativa per utilizzare un certificato con firma locale (LSC, Locally Signed Certificate) con un profilo di sicurezza. I Cisco Unified 7925G, 7925G - E X e 7926 G dispongono di un certificato di fabbricazione installato (MIC), che può essere utilizzato anche con un profilo di sicurezza.

Verifica

Raccogliere i registri della console dal telefono IP. Vediamo i diversi messaggi scambiati tra il telefono IP e il punto di accesso.

Il telefono IP avvia la ricerca di un SSID disponibile nel supporto.

```
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():recvmmsg() 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 wlan0 LinkStateChanged:
down
```

Il telefono IP inizia l'associazione con il 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"
```

Il telefono IP viene associato correttamente al punto di accesso.

```
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 wlan0 LinkStateChanged:
down
09110 08-10 09:33:38.843 685 804 DEB EthernetStateMachine: Interface wlan0 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 wlan0 LinkStateChanged:
down
```

Il telefono IP avvia l'autenticazione estesa.

```
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
```

Il telefono IP controlla il certificato del server per 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
```

Passaggio autenticazione estesa completato.

```
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=]
```

Connessione riuscita.

```
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!!!

Il telefono IP cerca un lease DHCP.

```
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: [lcorrearn Wireless]
modifiable state was empty, setting visibility to gone
09596 08-10 09:33:39.710 2348 2348 VBS Settings.AccessPoint: onBindView: [lcorrearn Wireless]
modifiable state was empty, setting visibility to gone
09597 08-10 09:33:39.718 2348 2348 VBS Settings.AccessPoint: onBindView: [lcorrearn 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
```

Il telefono IP riceve una risposta dal server DHCP.

```
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
```

Il telefono IP invia un ARP gratuito per confermare che il IP è effettivamente disponibile.

```
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....
```

Il telefono IP riceve un messaggio di opzioni DHCP.

```
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_identififier=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_identififier=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 messge 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
```

Il telefono IP inizia a richiedere i file dell'elenco di identità attendibili (ITL) e dell'elenco di certificati attendibili (CTL).

```
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
```

Il telefono IP cerca i server CUCM attivi per la registrazione.

```
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]
```

Risoluzione dei problemi

Cisco Unified 9971 IP Phone fornisce informazioni sui dispositivi, tra cui stato della rete, indirizzo MAC, informazioni sulla versione, comunicazioni unificate, statistiche di flusso e statistiche WLAN. Accedere all'interfaccia Web (<http://x.x.x.x>) del telefono IP e selezionare le informazioni da controllare.

Informazioni dispositivo



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

Installazione della rete



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

Statistische WLAN



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

Statistiche di streaming



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

Registri dispositivo

I registri della console, i dump di base, i messaggi di stato per la risoluzione dei problemi possono essere ottenuti dall'interfaccia Web del telefono IP. Selezionare l'interfaccia Web (<http://x.x.x.x>) del telefono IP, quindi selezionare le voci di menu necessarie in Registri dispositivi per visualizzare queste informazioni.



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](#)

Indicatore del segnale WLAN

a partire dalla versione 9.0(2), l'indicatore di stato WLAN sarà visibile in tutti i menu di Impostazioni amministratore. Nella versione iniziale, l'indicatore del segnale WLAN era visibile solo nel menu WLAN Setup.

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

