Configurazione e risoluzione dei problemi di registrazione di telefoni IP wireless

Sommario

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

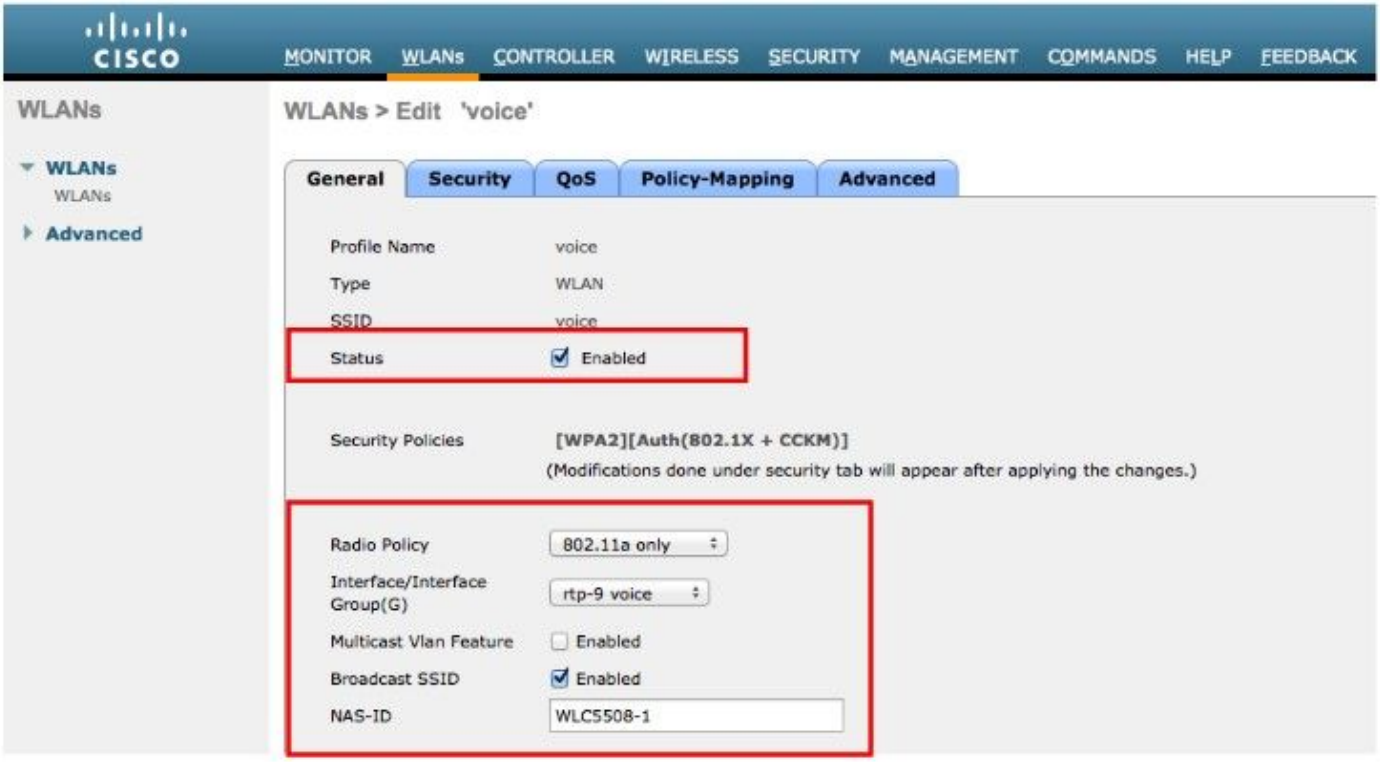
Impostazioni WLAN (Wireless Local Area Network)

Èconsigliabile 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.

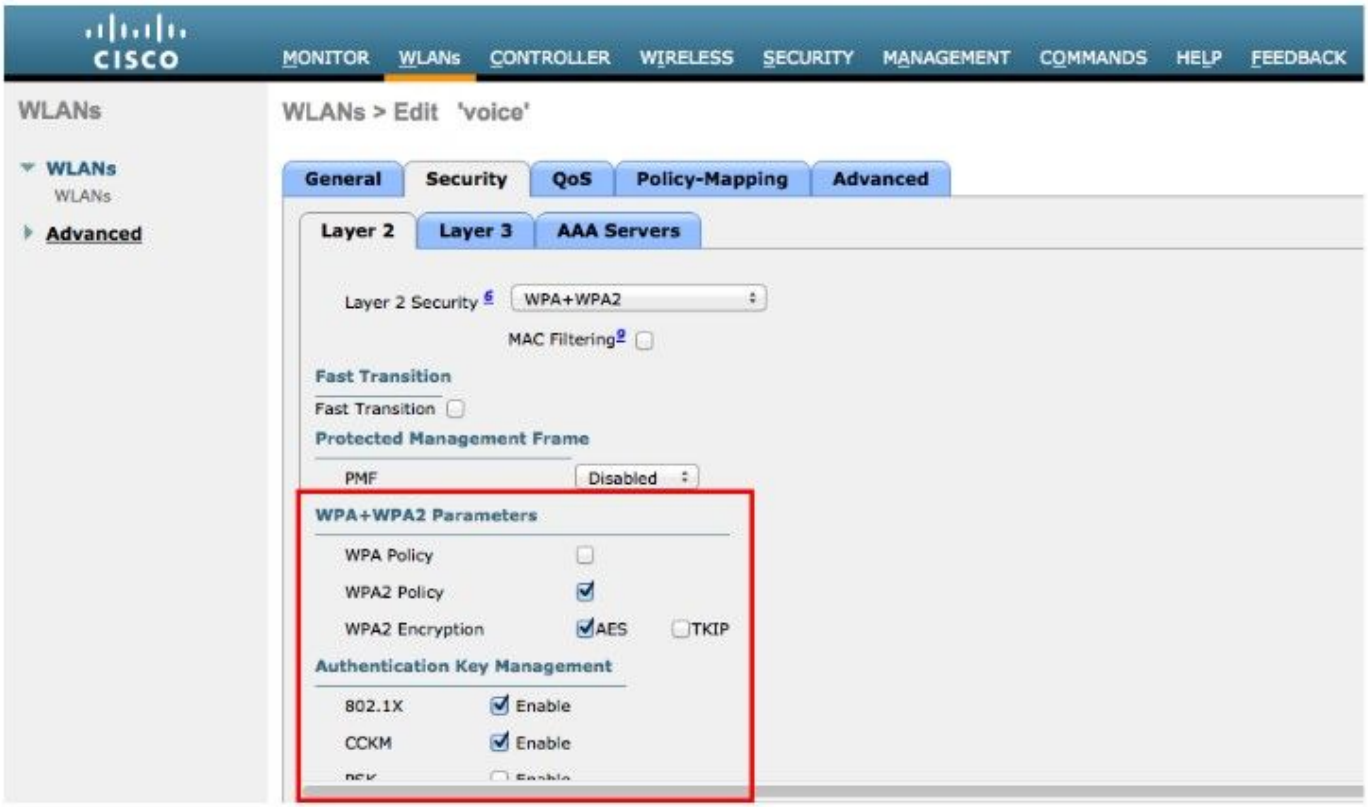
Si consiglia di far funzionare il telefono IP sulla banda dei 5 GHz in quanto ha molti canali disponibili e non così tanti interferitori come la banda dei 2.4 GHz.

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.

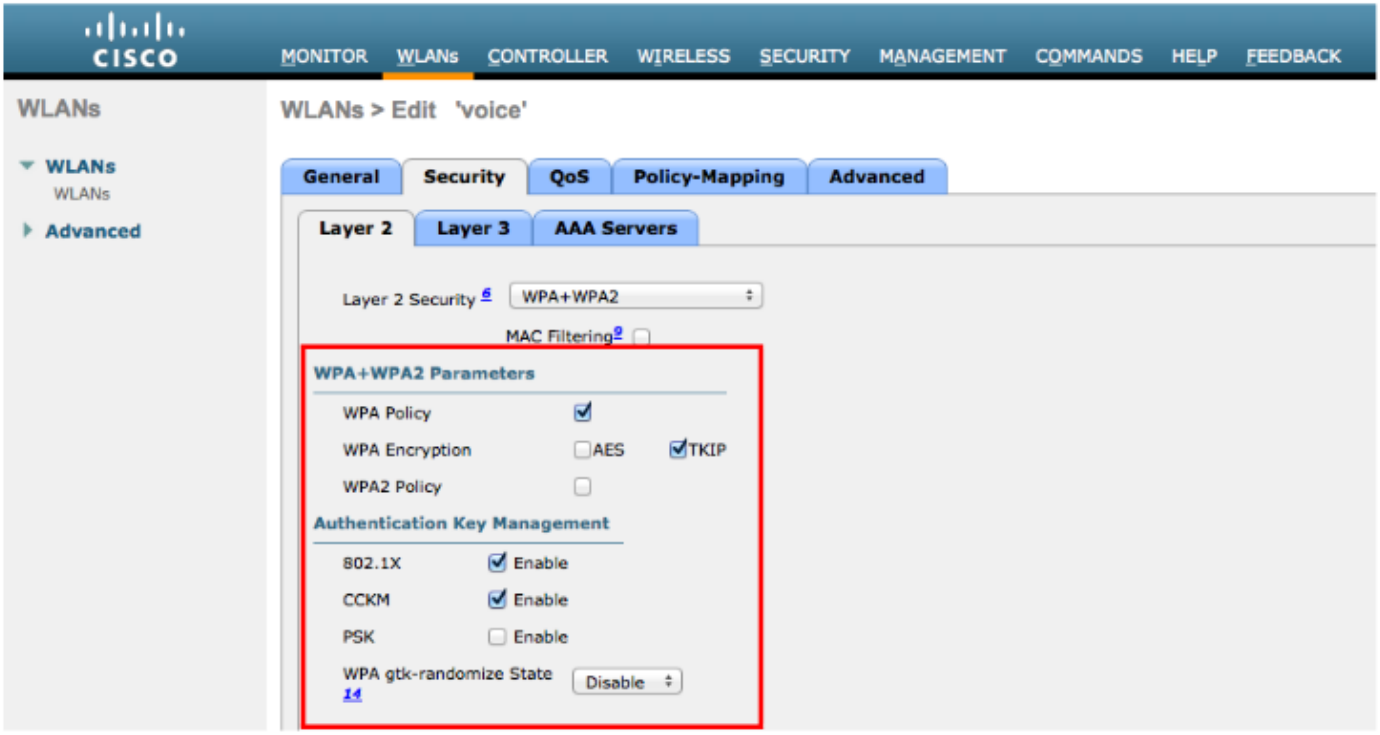


Per utilizzare la funzionalità Cisco Centralized Key Management (CCKM), abilitare la policy Wi-Fi Protected Access (WPA) 2 con la crittografia AES (Advanced Encryption Standard) e la crittografia

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.

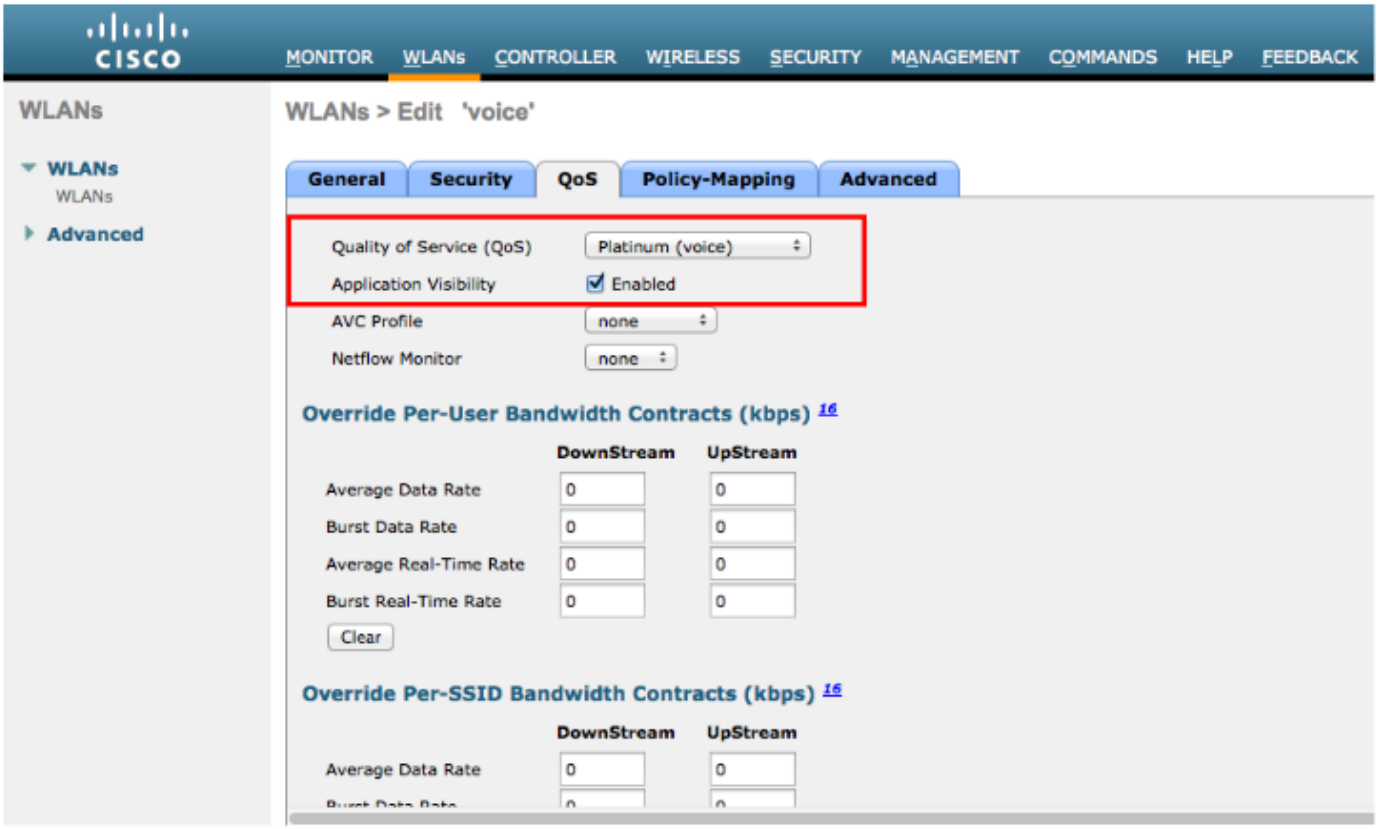


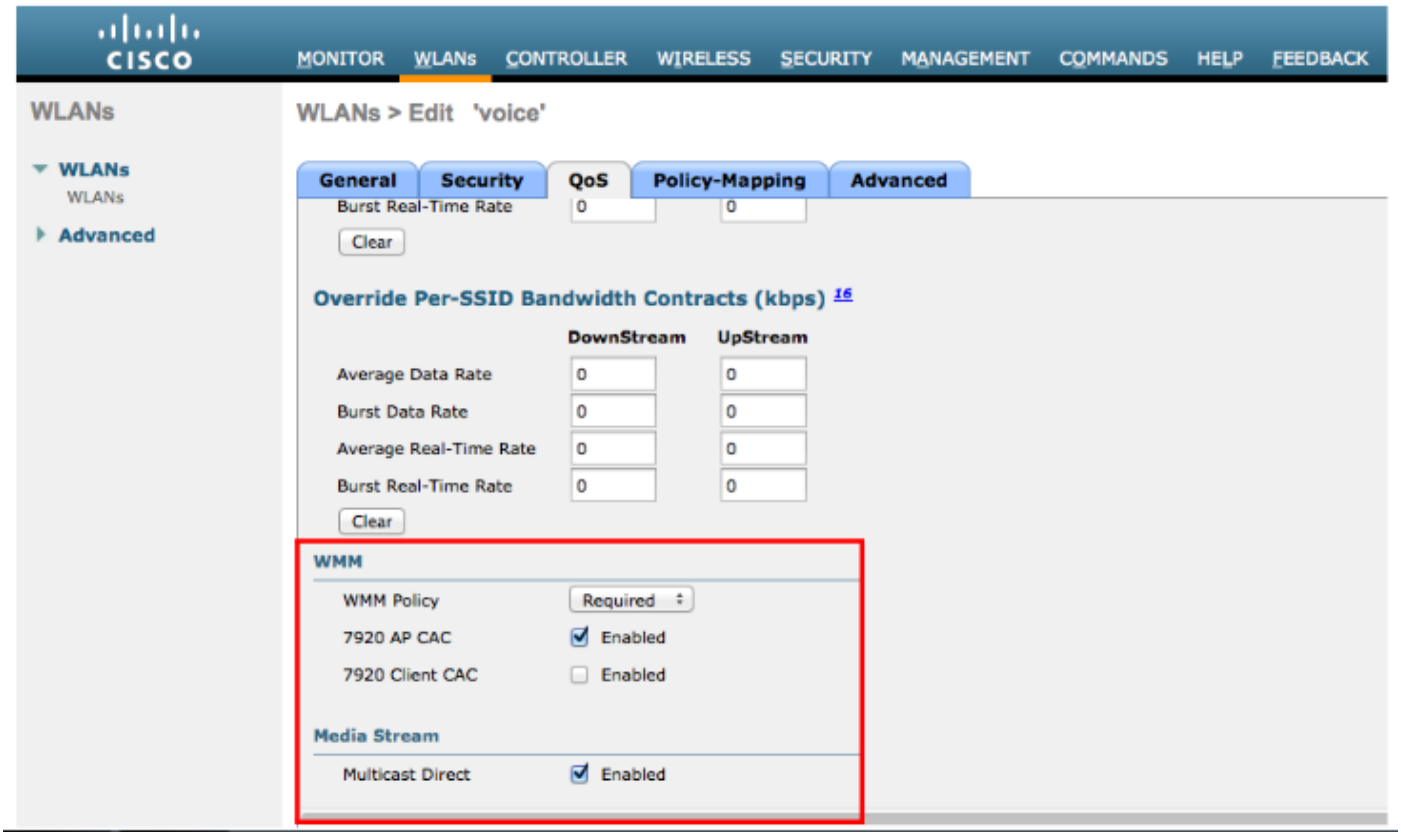
Se sul telefono IP è in esecuzione una versione firmware precedente alla 9.1(1), abilitare la policy WPA con crittografia TKIP (Temporal Key Integrity Protocol) e 802.1x + CCKM per il tipo di gestione delle chiavi autenticate per consentire un roaming veloce e sicuro.



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.





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.

Ènecessario 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.

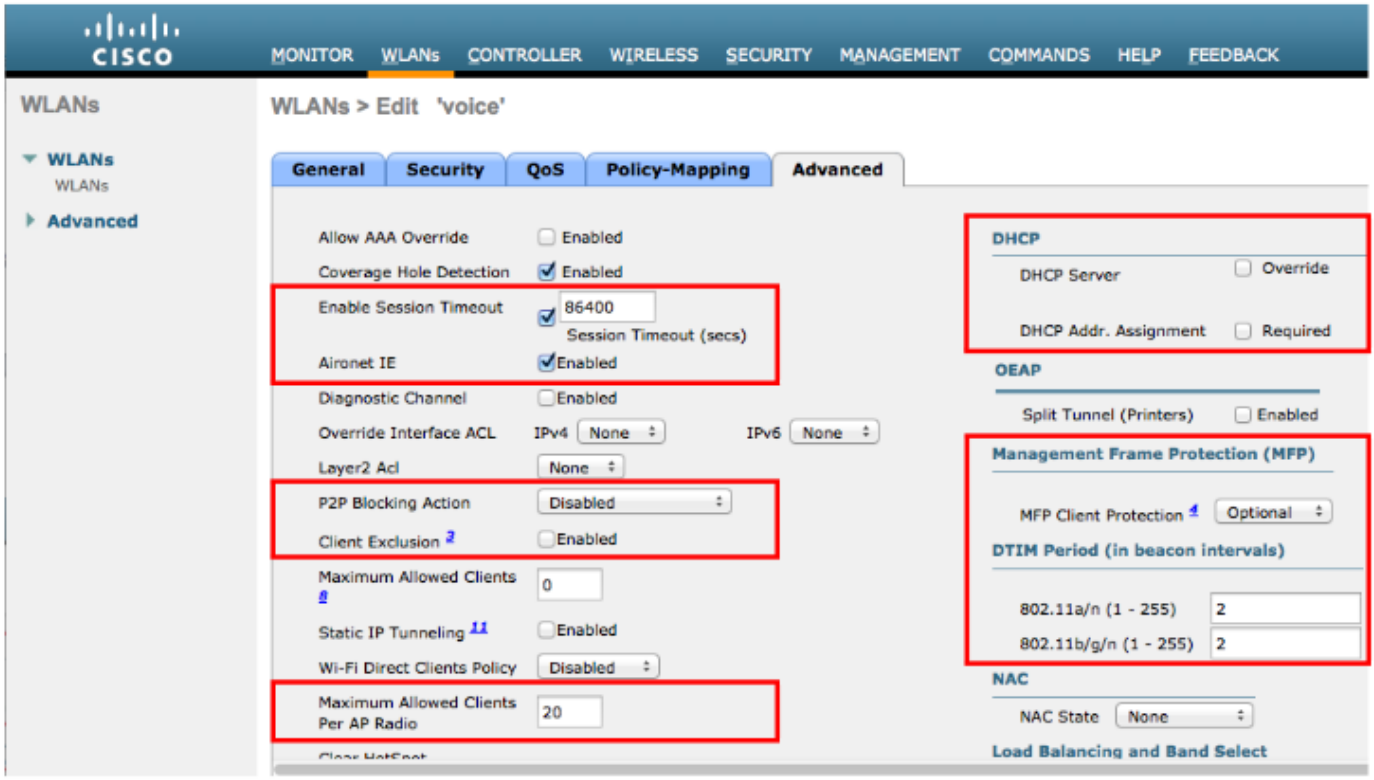
Èpossibile configurare il numero massimo di client consentiti per radio AP in base alle esigenze.

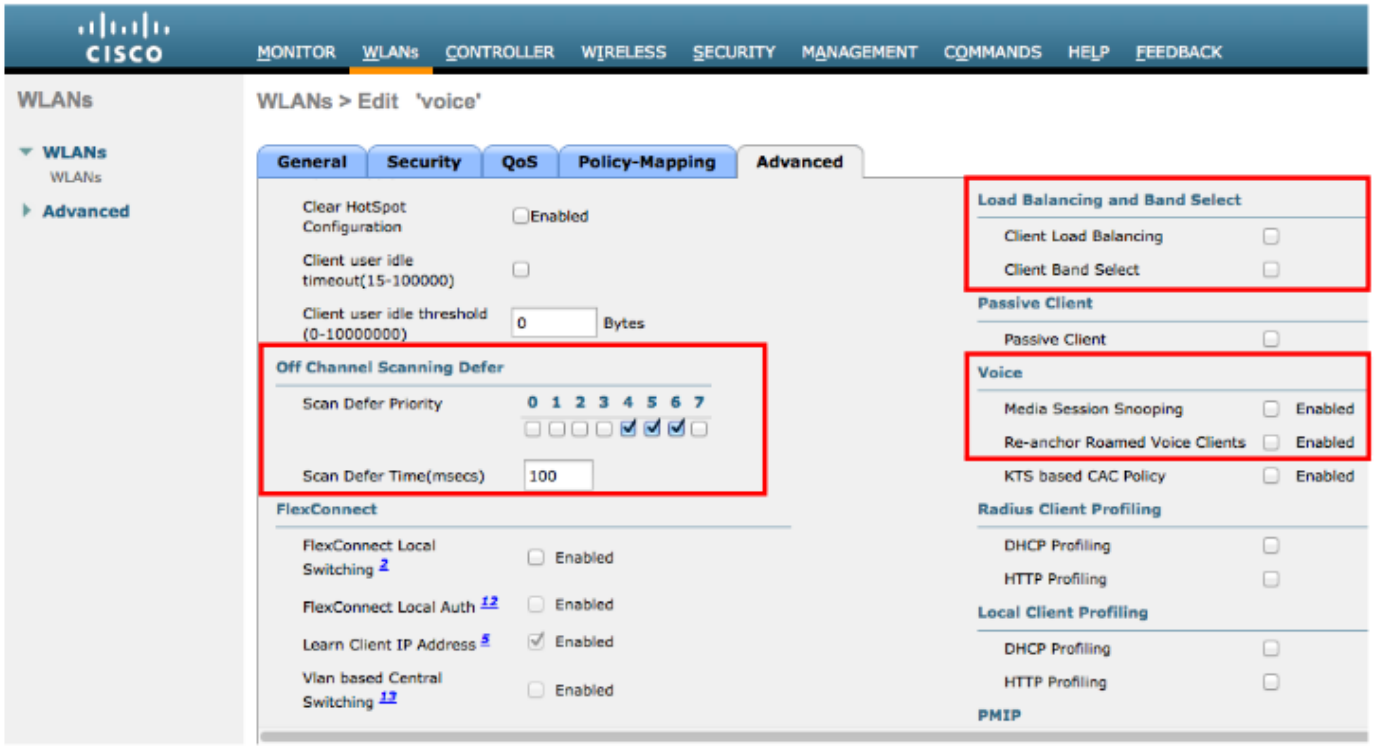
L'assegnazione degli indirizzi DHCP (Dynamic Host Configuration Protocol) richiesta deve essere disabilitata.

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.





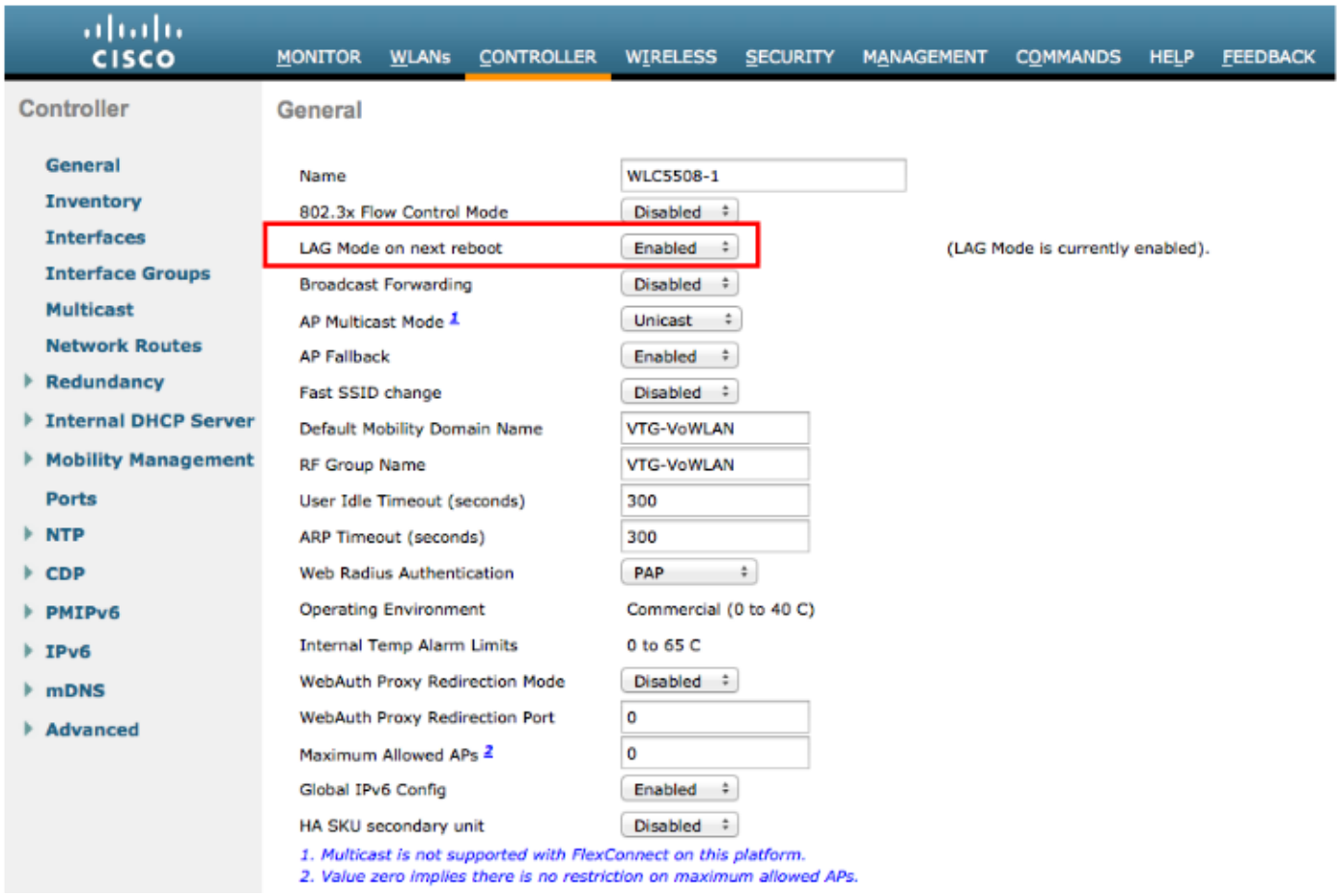
Impostazioni controller

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).



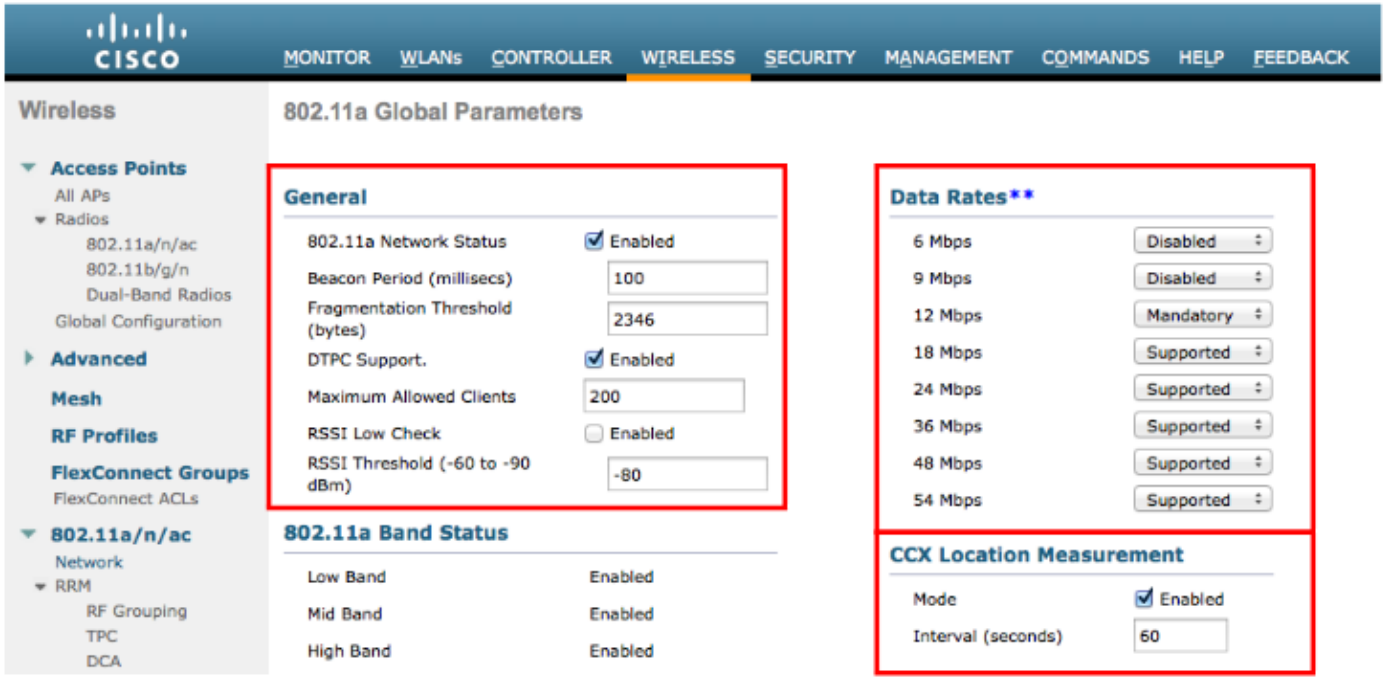
Impostazioni di rete 802.11

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.



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.

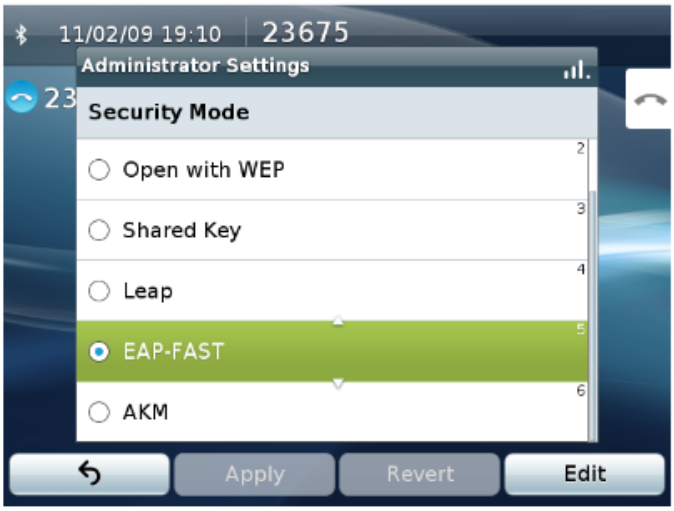
- Auto
- 802.11a
- 802.11b/g

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.

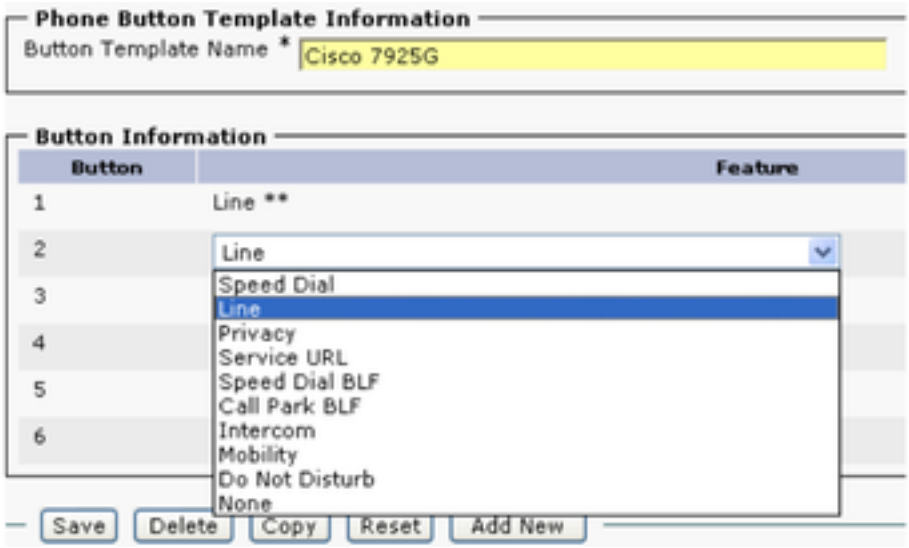
Configurare il telefono IP in modo che utilizzi Apri con WEP (Wired Equivalent Privacy) o Chiave condivisa per la modalità di protezione, immettere le informazioni della chiave WEP statica che corrispondono alla configurazione del punto di accesso.

- 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.



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():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
```

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 "lcorream
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 lcorream Wireless
09059 08-10 09:33:36.734 2348 2348 VBS Settings.CiscoWifiModifiable: Translating Wifi modifiable
state 0 for SSID: "lcorream 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),
"lcorream Wireless", ASSOCIATING -> ASSOCIATED
09094 08-10 09:33:38.835 210 313 INF SWMAN : nl_ipThrd():recvmsg() 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():recvmsg() 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():recvmsg() 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():recvmsg() 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():recvmsg() 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
```

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():recvmsg() 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: [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
```

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 dhcpcd : 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 dhcpcd : executing `/system/etc/dhcpcd/dhcpcd-run-hooks',
reason BOUND
09626 08-10 09:33:43.992 3246 3246 DEB dhcpcd : Enterning configure_env....
```

Il telefono IP riceve un messaggio di opzioni DHCP.

```
09627 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 1*: new_subnet_mask=255.255.255.0
09628 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 150*:
new_cisco_tftp_server=192.168.110.86
09629 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 3*: new_routers=192.168.110.1
09630 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 6*:
new_domain_name_servers=192.168.110.122 8.8.8.8
09631 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 15*: new_domain_name=cucm.cotac.com
09632 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 51*: new_dhcp_lease_time=600
09633 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 53*: new_dhcp_message_type=5
09634 08-10 09:33:43.992 3246 3246 DEB dhcpcd : option 54*:
new_dhcp_server_identifier=192.168.110.122
09635 08-10 09:33:44.257 3246 3246 DEB dhcpcd : configure: mlan0 adding IP address
192.168.110.236
09636 08-10 09:33:44.265 3246 3246 DEB dhcpcd : adding route to 0.0.0.0/0 via 192.168.110.1
09637 08-10 09:33:44.265 3246 3246 DEB dhcpcd : Writing lease file:
/dataRoot/.system/misc/dhcp/dhcpcd-mlan0.lease
09638 08-10 09:33:44.265 3246 3246 DEB dhcpcd : executing `/system/etc/dhcpcd/dhcpcd-run-hooks',
reason BOUND
09639 08-10 09:33:44.265 3246 3246 DEB dhcpcd : Enterning configure_env....
09640 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 1*: new_subnet_mask=255.255.255.0
09641 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 150*:
new_cisco_tftp_server=192.168.110.86
09642 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 3*: new_routers=192.168.110.1
09643 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 6*:
new_domain_name_servers=192.168.110.122 8.8.8.8
09644 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 15*: new_domain_name=cucm.cotac.com
09645 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 51*: new_dhcp_lease_time=600
09646 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 53*: new_dhcp_message_type=5
09647 08-10 09:33:44.265 3246 3246 DEB dhcpcd : option 54*:
new_dhcp_server_identifier=192.168.110.122
09648 08-10 09:33:44.265 214 241 INF NETSD : nl_ipThrd():recvmsg() len=60
09649 08-10 09:33:44.265 210 313 INF SWMAN : nl_ipThrd():recvmsg() 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
```

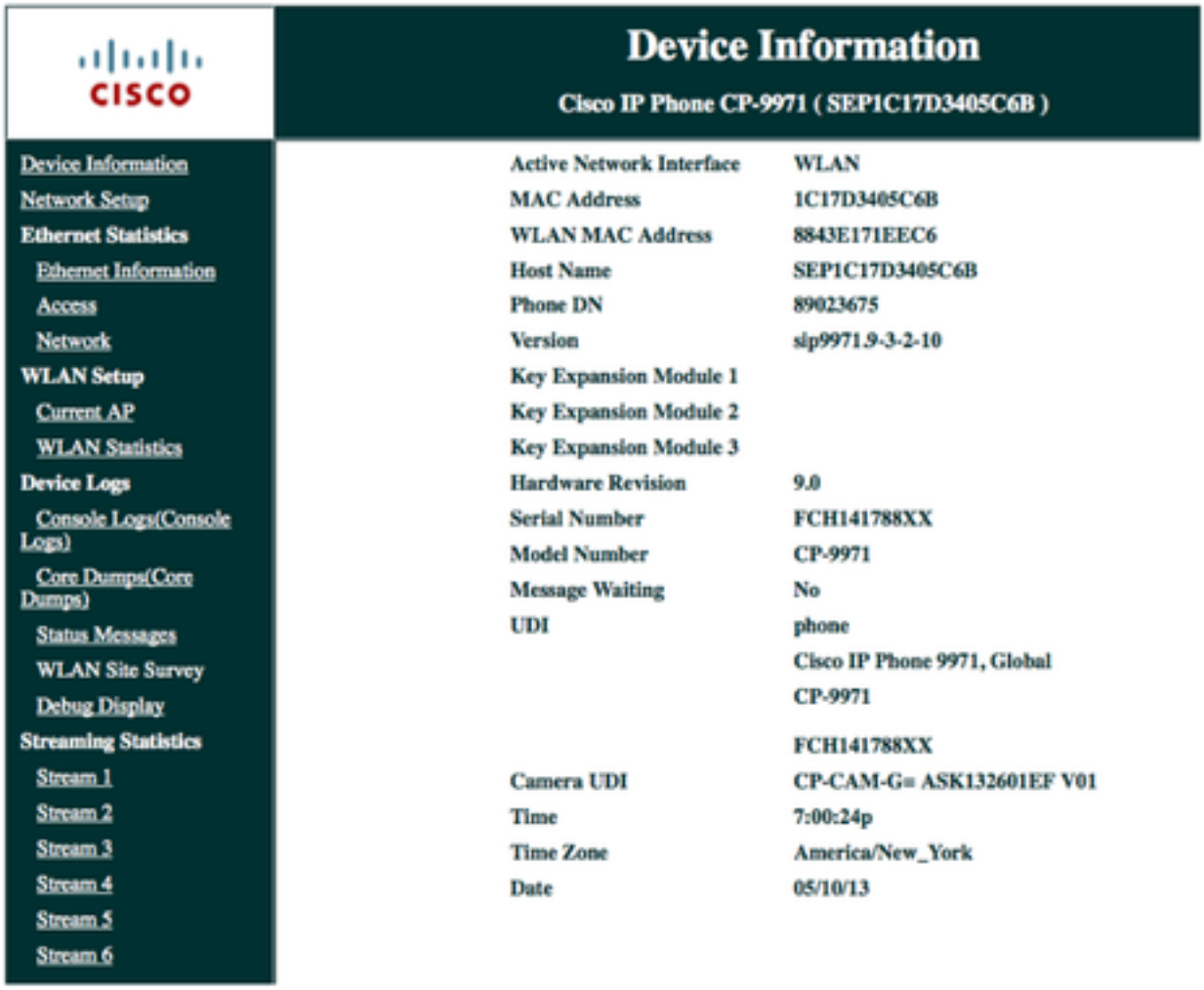
Il telefono IP cerca i server CUCM attivi per la registrazione.

```
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]
```

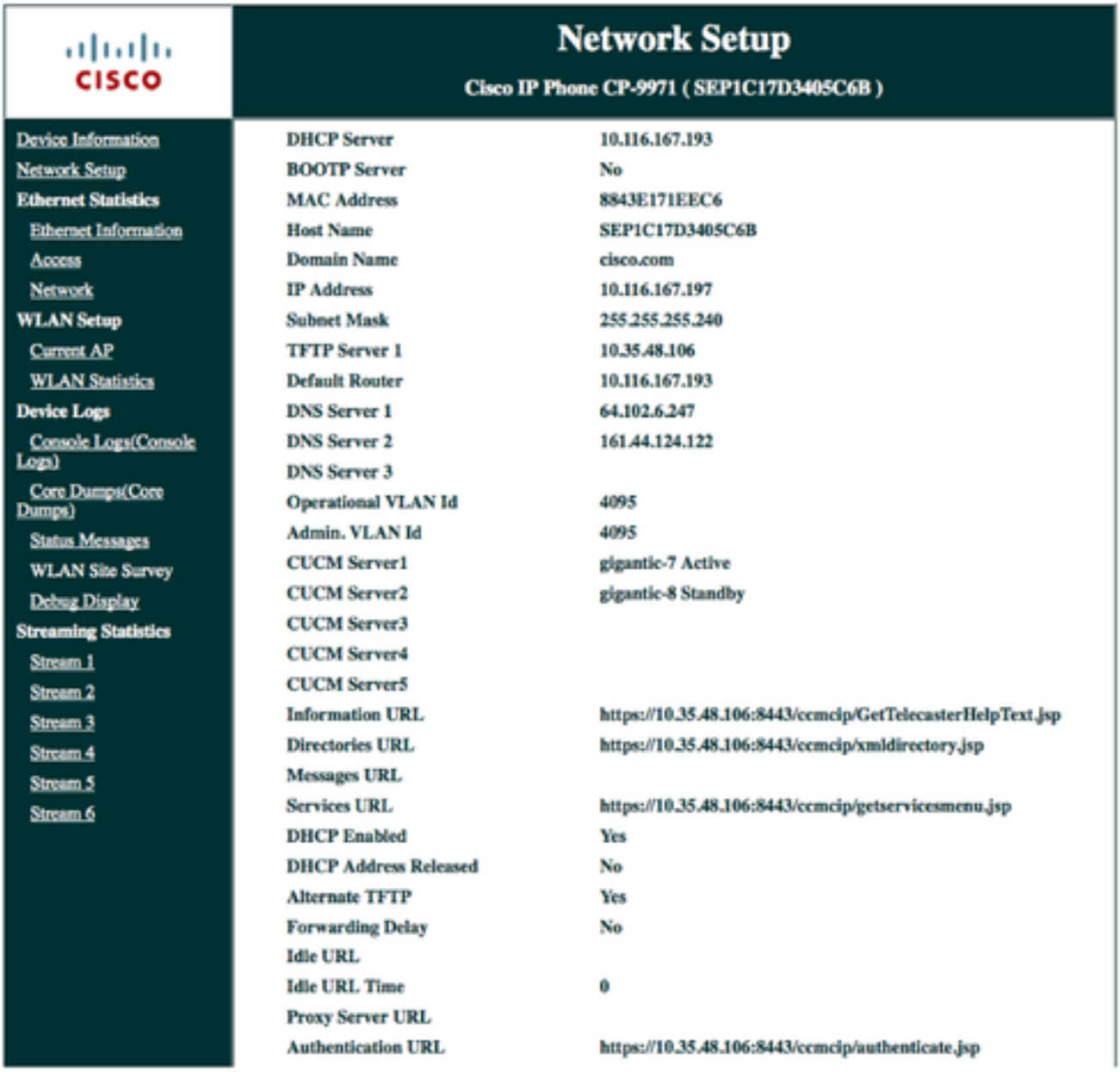
Risoluzione dei problemi

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.

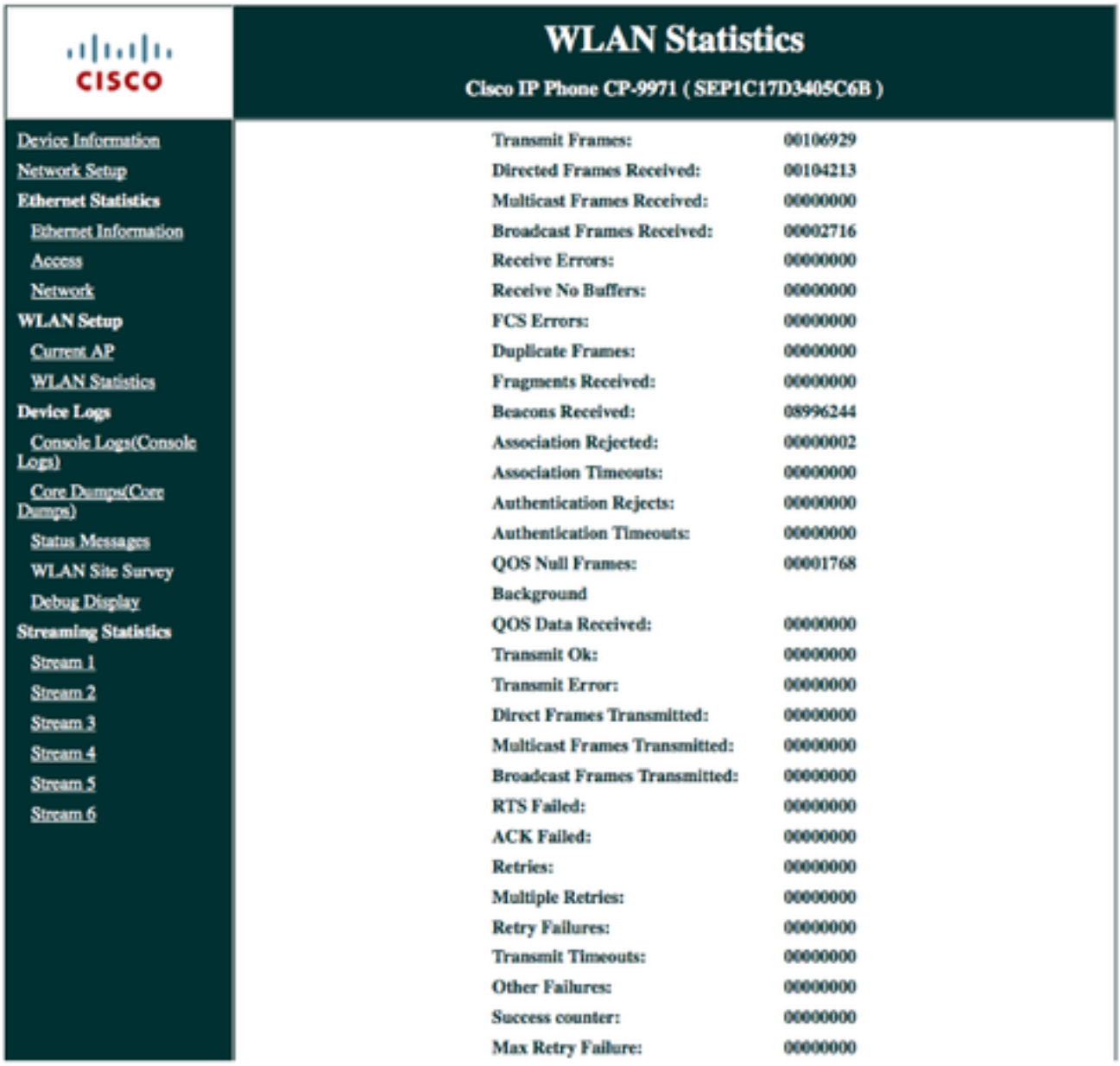
Informazioni dispositivo



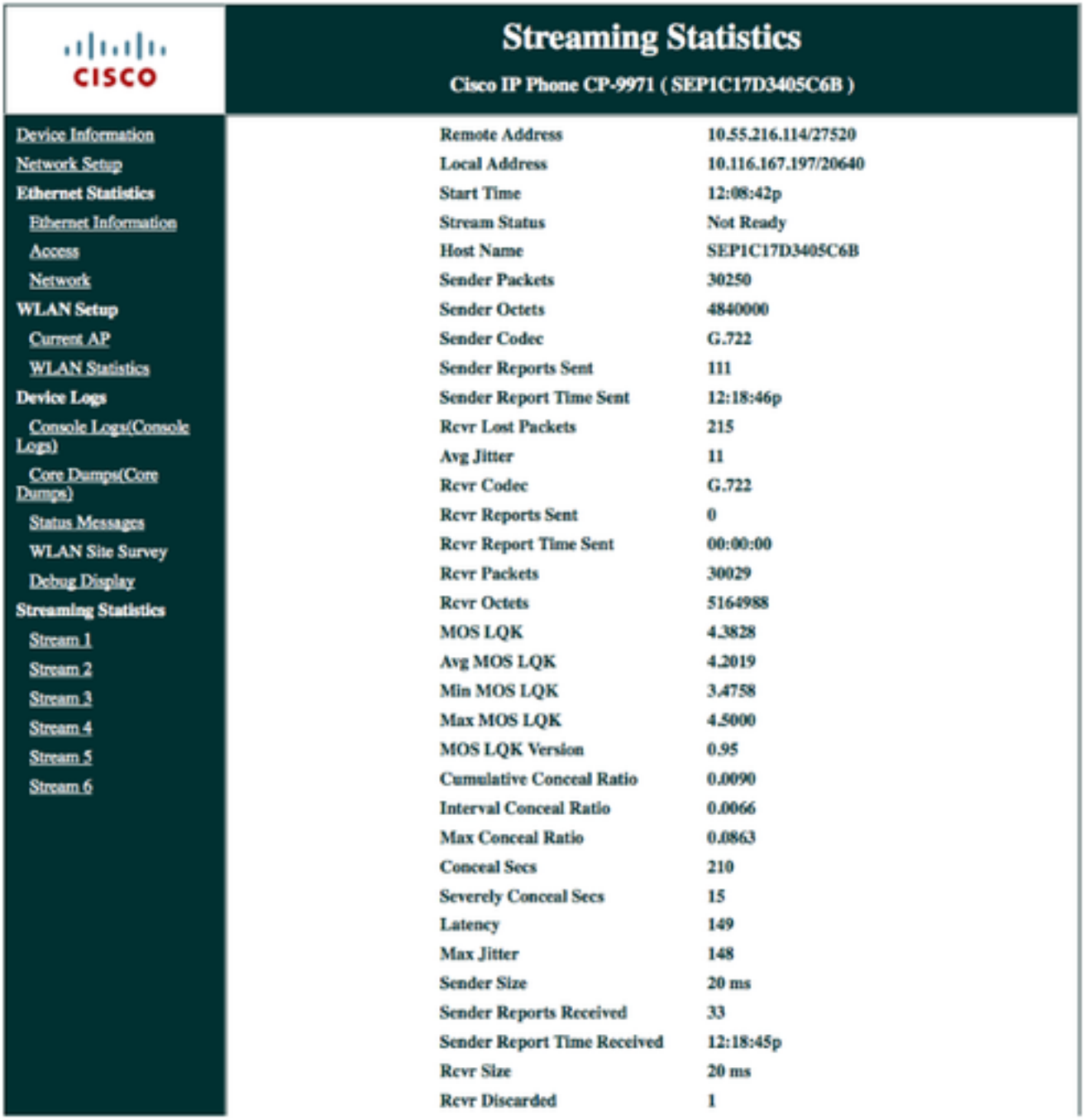
Installazione della rete



Statistiche WLAN

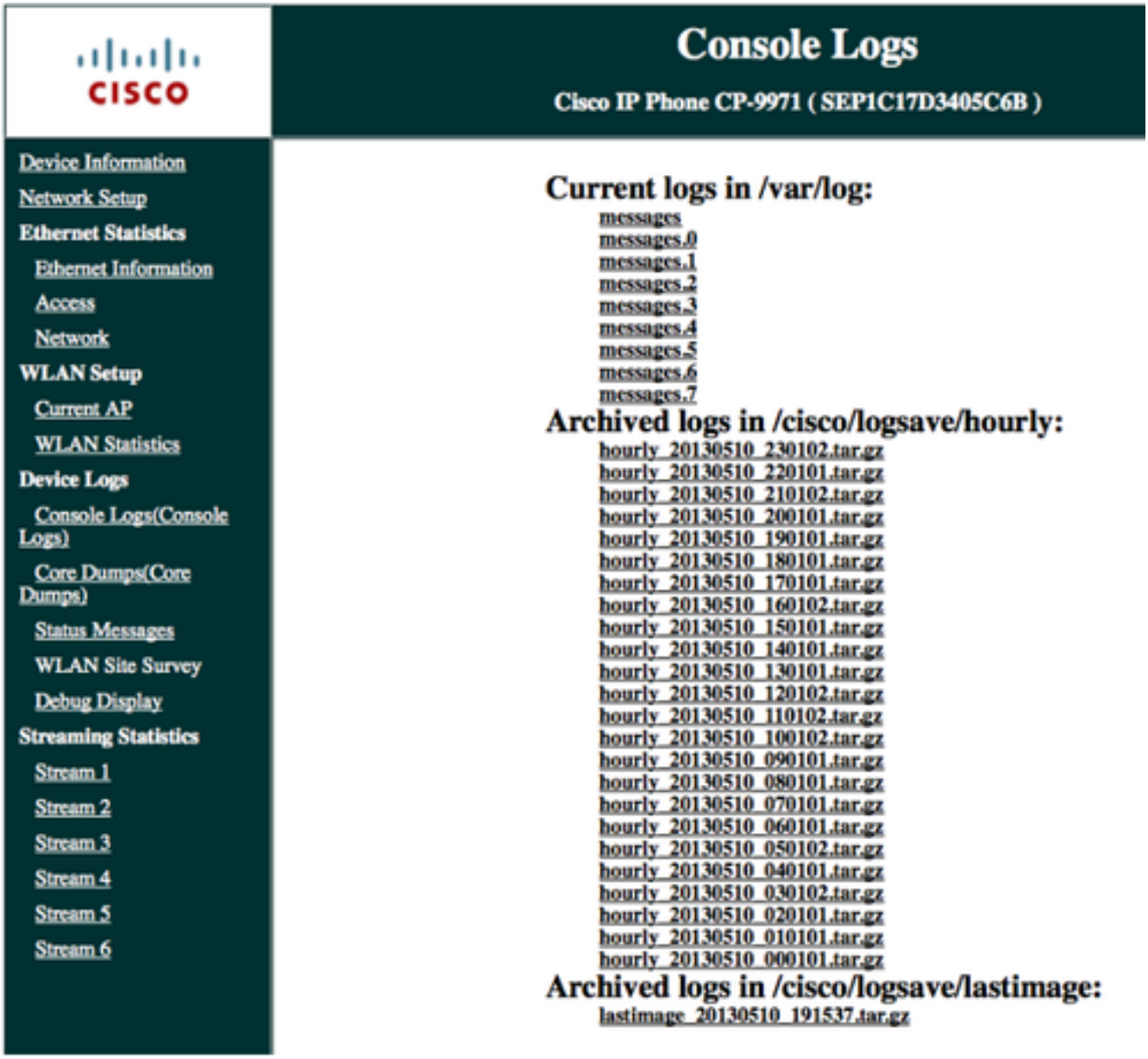


Statistiche di streaming



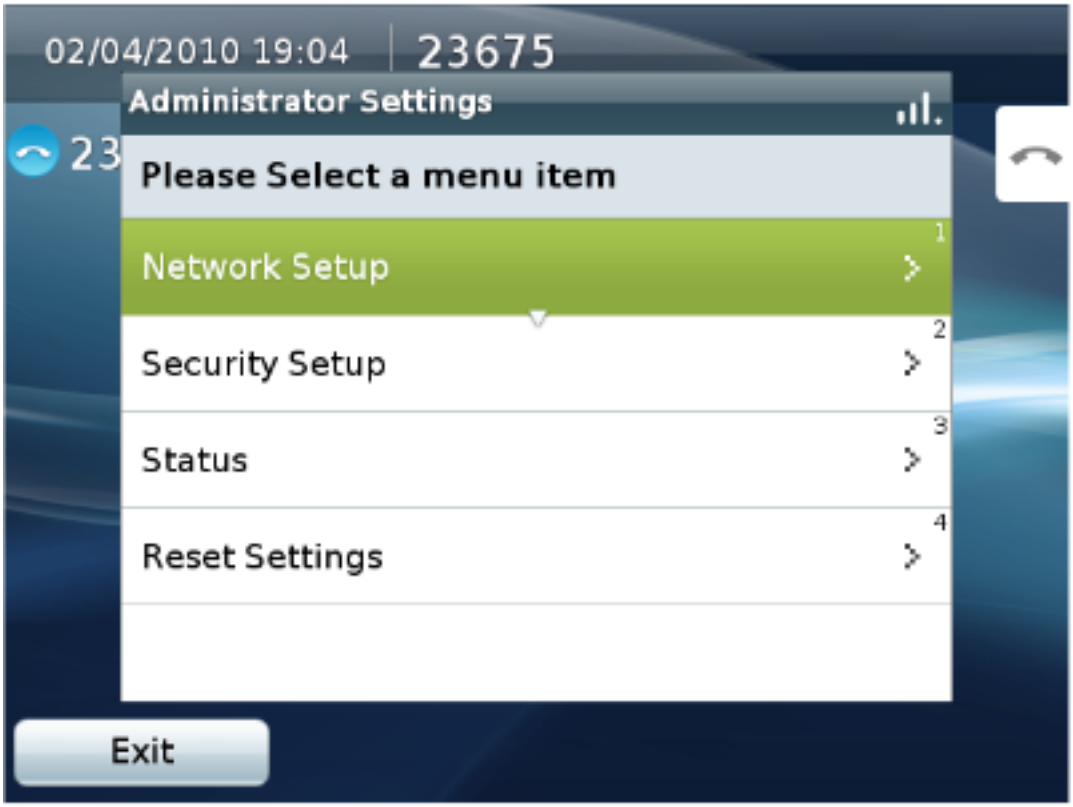
Registri dispositivo

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.



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