APPENDIX D

トラブルシューティング

この付録では、Cisco Unified Wireless Network Solution インターフェイスに表示されるシステム メッセージのリストと、コントローラと Lightweight アクセス ポイントの LED パターンに関する情報を示し、コントローラのトラブルシューティングに使用できる CLI コマンドについて説明します。この章の内容は、次のとおりです。

LED の解釈

コントローラの LED の解釈

LED パターンの情報については、特定のコントローラのクイック スタート ガイドを参照してください。これらのガイドには、次の URL からアクセスできます。

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

Lightweight アクセス ポイント LED の解釈

LED パターンの情報については、特定のアクセス ポイントのハードウェア インストレーション ガイドを参照してください。これらのガイドには、次の URL からアクセスできます。

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

システム メッセージ

表 D-1 は、一般的なシステム メッセージとその説明の一覧です。システム メッセージの一覧は、『Cisco Wireless LAN Controller System Message Guide, Release 5.0』を参照してください。

表 D-1　システム メッセージとその説明

エラー メッセージ	説明
apf_utils.c 680:Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	クライアントは保護ビットが 0 に設定された、セキュリティが有効になっている WLAN 上でアソシエーション要求を送信しています（アソシエーション要求の Capability フィールドで）。設計されたとおりに、コントローラはアソシエーション要求を却下し、クライアントにはアソシエーション エラーが表示されます。
dtl_arp.c 480:Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	コントローラの Network Processing Unit（NPU）はタイムアウト メッセージを CPU に送信し、特定のクライアントがタイムアウトまたは期限切れであることを知らせます。これは通常、CPU が内部データベースから無線クライアントを削除したことを NPU に通知していない場合に起こります。クライアントは NPU データベースにとどまるため、ネットワーク プロセッサで期限切れになり、CPU に通知されます。CPU はデータベースにないクライアントを検出して、このメッセージを送信します。
STATION_DISASSOCIATE	クライアントが使用を意図的に中断したか、サービスの中断を受けた可能性があります。
STATION_DEAUTHENTICATE	クライアントが使用を意図的に中断したか、認証上の問題があることを示しています。
STATION_AUTHENTICATION_FAIL	設定の有効性、キーの不一致、またはその他の問題を確認します。
STATION_ASSOCIATE_FAIL	Cisco Radio 上の負荷または信号の品質に問題がないか確認します。
LRAD_ASSOCIATED	アソシエートされた Lightweight アクセス ポイントがこのコントローラで管理されるようになりました。
LRAD_DISASSOCIATED	Lightweight アクセス ポイントが他のコントローラにアソシエートされているか、完全に接続不可能になっている可能性があります。
LRAD_UP	Lightweight アクセス ポイントは正常に動作しています。処理は必要ありません。
LRAD_DOWN	Lightweight アクセス ポイントに問題があるか、管理上無効にされています。
LRADIF_UP	Cisco Radio は稼働状態です。
LRADIF_DOWN	Cisco Radio に問題があるか、管理上無効にされています。
LRADIF_LOAD_PROFILE_FAILED	クライアント密度がシステムのキャパシティを超えている可能性があります。
LRADIF_NOISE_PROFILE_FAILED	802.11 以外のノイズが設定しきい値を超えました。
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 干渉がチャネル上のしきい値を超えました。チャネルの割り当てを確認してください。

表 D-1　システム メッセージとその説明（続き）

エラー メッセージ	説明
LRADIF_COVERAGE_PROFILE_FAILED	カバレッジ ホールの可能性が検出されました。Lightweight アクセス ポイント履歴を調べて、一般的な問題がないかどうかを確認し、必要に応じて Lightweight アクセス ポイントを追加してください。
LRADIF_LOAD_PROFILE_PASSED	負荷がしきい値の制限内に戻りました。
LRADIF_NOISE_PROFILE_PASSED	検出されたノイズがしきい値より小さくなりました。
LRADIF_INTERFERENCE_PROFILE_PASSED	検出された干渉がしきい値より小さくなりました。
LRADIF_COVERAGE_PROFILE_PASSED	不良電波を受信しているクライアント数はしきい値内です。
LRADIF_CURRENT_TXPOWER_CHANGED	情報メッセージです。
LRADIF_CURRENT_CHANNEL_CHANGED	情報メッセージです。
LRADIF_RTS_THRESHOLD_CHANGED	情報メッセージです。
LRADIF_ED_THRESHOLD_CHANGED	情報メッセージです。
LRADIF_FRAGMENTATION_THRESHOLD_ CHANGED	情報メッセージです。
RRM_DOT11_A_GROUPING_DONE	情報メッセージです。
RRM_DOT11_B_GROUPING_DONE	情報メッセージです。
ROGUE_AP_DETECTED	セキュリティ上の問題がある可能性があります。マップと傾向を使用して調べてください。
ROGUE_AP_REMOVED	不正なアクセス ポイントのタイムアウトが検出されました。ユニットがシャットダウンしたか、カバレッジ領域外に移動しました。
AP_MAX_ROGUE_COUNT_EXCEEDED	現在のアクティブな不正なアクセス ポイント数がシステムのしきい値を超えました。
LINK_UP	肯定的な確認メッセージです。
LINK_DOWN	ポートに問題があるか、管理上無効にされています。
LINK_FAILURE	ポートに問題があるか、管理上無効にされています。
AUTHENTICATION_FAILURE	セキュリティ違反の試行が検出されました。調査してください。
STP_NEWROOT	情報メッセージです。
STP_TOPOLOGY_CHANGE	情報メッセージです。
IPSEC_ESP_AUTH_FAILURE	WLAN IPSec の設定を確認してください。
IPSEC_ESP_REPLAY_FAILURE	IP アドレスのスプーフィング試行がないかどうか確認してください。
IPSEC_ESP_POLICY_FAILURE	WLAN とクライアントの間で IPSec 設定が矛盾していないかどうか確認してください。
IPSEC_ESP_INVALID_SPI	情報メッセージです。
IPSEC_OTHER_POLICY_FAILURE	WLAN とクライアントの間で IPSec 設定が矛盾していないかどうか確認してください。
IPSEC_IKE_NEG_FAILURE	WLAN とクライアントの間で IPSec IKE 設定が矛盾していないかどうか確認してください。
IPSEC_SUITE_NEG_FAILURE	WLAN とクライアントの間で IPSec IKE 設定が矛盾していないかどうか確認してください。
IPSEC_INVALID_COOKIE	情報メッセージです。

表 D-1　システム メッセージとその説明（続き）

エラー メッセージ	説明
RADIOS_EXCEEDED	サポートされている Cisco Radio の最大数を超えました。同じレイヤ 2ネットワークでコントローラの障害を調べるか、別のコントローラを追加してください。
SENSED_TEMPERATURE_HIGH	ファン、空調、その他の冷却装置を確認してください。
SENSED_TEMPERATURE_LOW	室温が低くないか、低温の原因が他にないかどうかを調べてください。
TEMPERATURE_SENSOR_FAILURE	温度センサーを至急交換してください。
TEMPERATURE_SENSOR_CLEAR	温度センサーは正常に動作しています。
POE_CONTROLLER_FAILURE	ポートを確認してください。深刻な障害が検出されました。
MAX_ROGUE_COUNT_EXCEEDED	現在のアクティブな不正なアクセス ポイント数がシステムのしきい値を超えました。
SWITCH_UP	コントローラは SNMP のポーリングに応答しています。
SWITCH_DOWN	コントローラは SNMP のポーリングに応答していません。コントローラと SNMP の設定を確認してください。
RADIUS_SERVERS_FAILED	RADIUS とコントローラの間のネットワーク接続を確認してください。
CONFIG_SAVED	実行中の設定はフラッシュに保存されました。設定はリブート後にアクティブになります。
MULTIPLE_USERS	同じユーザ名の別のユーザがログインしています。
FAN_FAILURE	コントローラの温度を監視して、オーバーヒートしないようにしてください。
POWER_SUPPLY_CHANGE	電源が故障していないか確認してください。
COLD_START	コントローラはリブートされた可能性があります。
WARM_START	コントローラはリブートされた可能性があります。

CLI を使用したトラブルシューティング

お使いのコントローラで問題が発生した場合には、この項のコマンドを使用して情報を収集し、問題をデバッグすることができます。

1. **show process cpu**：システム内で各タスクが使用している CPU の現状を表示します。このコマンドは、タスクの中に CPU を独占して別のタスクの実行を妨げているものがないかどうか調べる際に役立ちます。

   次のような情報が表示されます。

```
Name                Priority      CPU Use     Reaper
 reaperWatcher       ( 3/124)     0 %       (  0/  0)%   I
 osapiReaper          (10/121)    0 %       (  0/  0)%   I
 TempStatus          (255/  1)    0 %      (  0/  0)%   I
 emWeb               (255/  1)    0 %     (  0/  0)%   T 300
 cliWebTask          (255/  1)    0 %     (  0/  0)%   I
 UtilTask            (255/  1)    0 %      (  0/  0)%   T 300
```

   上の例のフィールドの説明は、次のとおりです。

   - Name フィールドは、CPU が実行対象としているタスクです。
   - Priority フィールドは、次の 2 種類の値を示しています。1）実際のファンクション コールから生成されたタスクの最初の優先順位。2）システムの各優先順位で割ったタスクの優先順位。
   - CPU Use フィールドは、それぞれのタスクの CPU 利用率です。
   - Reaper フィールドは、次の 3 種類の値を示しています。1）ユーザ モードの操作でそのタスクが予定されている所要時間。2）システム モードの操作でそのタスクが予定されている所要時間。3）そのタスクが Reaper タスク モニタで監視されているかどうか（監視されている場合は「T」で表示）。タスクが Reaper タスク モニタで監視されている場合は、タスク モニタに警告するまでのタイムアウト値も秒単位で示されます。

   （注）　CPU 総利用率を % で表示するには、**show cpu** コマンドを入力してください。

2. **show process memory** : システム内で各プロセスが割り当てているメモリと、割り当て解除されているメモリの現状を表示します。

   次のような情報が表示されます。

```
Name                Priority     BytesInUse  BlocksInUse  Reaper
 reaperWatcher       ( 3/124)     0           0         (  0/  0)%   I
 osapiReaper          (10/121)    0        0 (  0/  0)%   I
 TempStatus          (255/  1)    308         1         (  0/  0)%   I
 emWeb               (255/  1)    294440       4910   (  0/  0)%  T 300
 cliWebTask          (255/  1)    738         2 (  0/  0)%   I
 UtilTask            (255/  1)    308         1 (  0/  0)%  T 300
```

   上の例のフィールドの説明は、次のとおりです。

   - Name フィールドは、CPU が実行対象としているタスクです。
   - Priority フィールドは、次の 2 種類の値を示しています。1）実際のファンクション コールから生成されたタスクの最初の優先順位。2）システムの各優先順位で割ったタスクの優先順位。
   - BytesInUse フィールドは、ダイナミック メモリの割り当てでそのタスクに使用される実際のバイト数です。
   - BlocksInUse フィールドは、そのタスクを実行する際に割り当てられる連続メモリです。

- Reaper フィールドは、次の 3 種類の値を示しています。1）ユーザ モードの操作でそのタスクが予定されている所要時間。2）システム モードの操作でそのタスクが予定されている所要時間。3）そのタスクが Reaper タスク モニタで監視されているかどうか（監視されている場合は「T」で表示）。タスクが Reaper タスク モニタで監視されている場合は、タスク モニタに警告するまでのタイムアウト値も秒単位で示されます。

3. **show tech-support**：現在の設定内容、最新のクラッシュ ファイル、CPU 利用率、メモリ利用率など、システムの状態についての一連の情報を表示します。

4. **show running-config**：コントローラの現在の設定内容がすべて表示されます。アクセス ポイントの設定は表示されません。このコマンドで表示されるのは、ユーザが設定した値だけです。システムから設定されたデフォルト値は表示されません。このコマンドは **show run-config** コマンドとは違い、現在の設定内容の一部と多数のダイナミック情報を出力しません。その代わり **show running-config** コマンドでは、コントローラの設定内容をコマンド形式の平文で出力します。

   以下は、その出力例です。

```
radius auth add 1 10.50.3.104 1812 ascii ****

radius backward compatibility enable

radius admin-authentication disable

radius cred-cache enable

radius callStationIdType macAddr

radius acct retransmit-timeout 1 4

radius acct network 1 disable

radius auth rfc3576 enable 1

radius auth retransmit-timeout 1 6

radius auth network 1 disable

radius auth management 1 disable

radius auth ipsec enable
```

（注）　平文でパスワードを表示するには、**config passwd-cleartext enable** と入力してください。このコマンドを実行するには、管理者のパスワードを入力する必要があります。このコマンドは、このセッションに限り有効です。リブート後は、保存されません。

（注）　このコマンドの出力をアップロードする際に、TFTP　は使用できません。この出力は、必要に応じてカット & ペーストしてください。

システム ロギングとメッセージ ロギングの設定

システム ロギングを使用すると、コントローラのシステム イベントを最大 3 台のリモート syslog サーバにログできるようになります。syslog メッセージはコントローラに設定されている syslog サーバごとにログされるため、コントローラは各 syslog メッセージのコピーを送信します。複数のサーバに syslog メッセージを送信できるため、1 台の syslog サーバが一時的に使用できなくなってもメッセージが失われることがありません。メッセージ ロギングを使用すると、システム メッセージをコントローラのバッファまたはコンソールにログできるようになります。

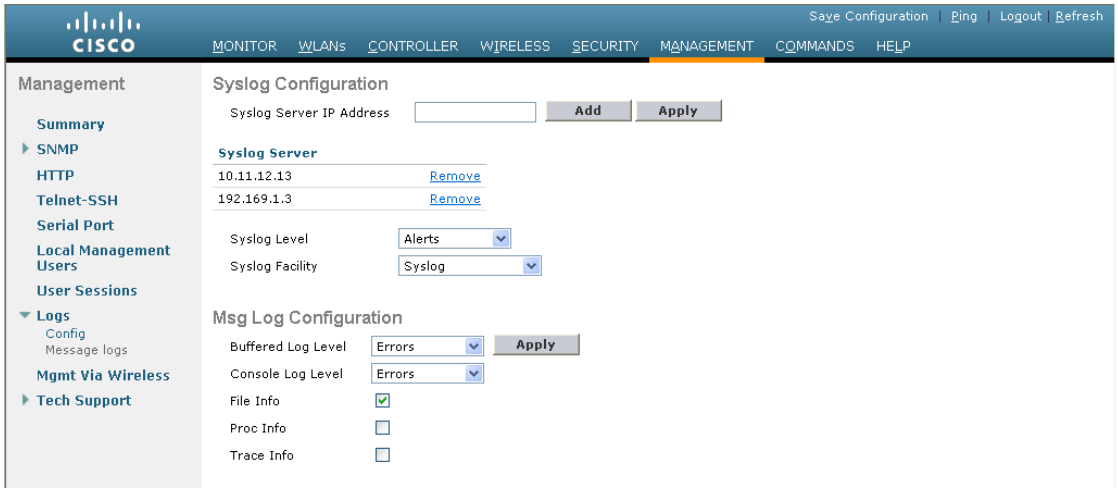
システム ロギングとメッセージ ロギングを設定するには、コントローラ GUI または CLI を使用します。

GUI を使用したシステム ロギングとメッセージ ロギングの設定

GUI を使用してシステム ロギングとメッセージ ロギングを設定する手順は、次のとおりです。

ステップ 1　**Management** > **Logs** > **Config** の順にクリックします。Syslog Configuration ページが表示されます（図 D-1 を参照）。

図 D-1　Syslog Configuration ページ



ステップ 2　Syslog Server IP Address フィールドに、syslog メッセージの送信先となるサーバの IP アドレスを入力し、**Add** をクリックします。コントローラには最大 3 台の syslog サーバを追加できます。このフィールドの下には、すでにコントローラに追加されている syslog サーバのリストが表示されます。

（注）　コントローラから syslog サーバを削除するには、目的のサーバの右側の **Remove** をクリックします。

ステップ 3　syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、Syslog Level ドロップダウン ボックスから次のいずれかのオプションを選択します。

- **Emergencies** = 重大度レベル 0
- **Alerts** = 重大度レベル 1 （デフォルト値）
- **Critical** = 重大度レベル 2
- **Errors** = 重大度レベル 3
- **Warnings** = 重大度レベル 4
- **Notifications** = 重大度レベル 5
- **Informational** = 重大度レベル 6
- **Debugging** = 重大度レベル 7

syslog レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、syslog サーバに送信されます。たとえば、syslog レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしか syslog サーバに送信されません。

ステップ 4　syslog サーバに送信する syslog メッセージのファシリティを設定するには、Syslog Facility ドロップダウン ボックスから次のいずれかのオプションを選択します。

- **Kernel** = ファシリティ レベル 0
- **User Process** = ファシリティ レベル 1
- **Mail** = ファシリティ レベル 2
- **System Daemons** = ファシリティ レベル 3
- **Authorization** = ファシリティ レベル 4
- **Syslog** = ファシリティ レベル 5（デフォルト値）
- **Line Printer** = ファシリティ レベル 6
- **USENET** = ファシリティ レベル 7
- **Unix-to-Unix Copy** = ファシリティ レベル 8
- **Cron** = ファシリティ レベル 9
- **FTP Daemon** = ファシリティ レベル 11
- **System Use 1** = ファシリティ レベル 12
- **System Use 2** = ファシリティ レベル 13
- **System Use 3** = ファシリティ レベル 14
- **System Use 4** = ファシリティ レベル 15
- **Local Use 0** = ファシリティ レベル 16
- **Local Use 1** = ファシリティ レベル 17
- **Local Use 2** = ファシリティ レベル 18
- **Local Use 3** = ファシリティ レベル 19
- **Local Use 4** = ファシリティ レベル 20
- **Local Use 5** = ファシリティ レベル 21
- **Local Use 6** = ファシリティ レベル 22
- **Local Use 7** = ファシリティ レベル 23

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　コントローラのバッファとコンソールに対するロギング　メッセージの重大度レベルを設定するには、Buffered Log Level および Console Log Level ドロップダウン リストから次のいずれかのオプションを選択します。

- **Emergencies** = 重大度レベル 0

- **Alerts** = 重大度レベル 1
- **Critical** = 重大度レベル 2
- **Errors** = 重大度レベル 3（デフォルト値）
- **Warnings** = 重大度レベル 4
- **Notifications** = 重大度レベル 5
- **Informational** = 重大度レベル 6
- **Debugging** = 重大度レベル 7

ロギング レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ロギング レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしかログされません。

ステップ 7　ソース ファイルの情報をメッセージ ログに含める場合は、**File Info** チェック ボックスをオンにします。デフォルト値は有効（enable）です。

ステップ 8　プロセス情報をメッセージ ログに含める場合は、**Proc Info** チェック ボックスをオンにします。デフォルト値は無効（disable）です。

ステップ 9　トレースバック情報をメッセージ ログに含める場合は、**Trace Info** チェック ボックスをオンにします。デフォルト値は無効（disable）です。

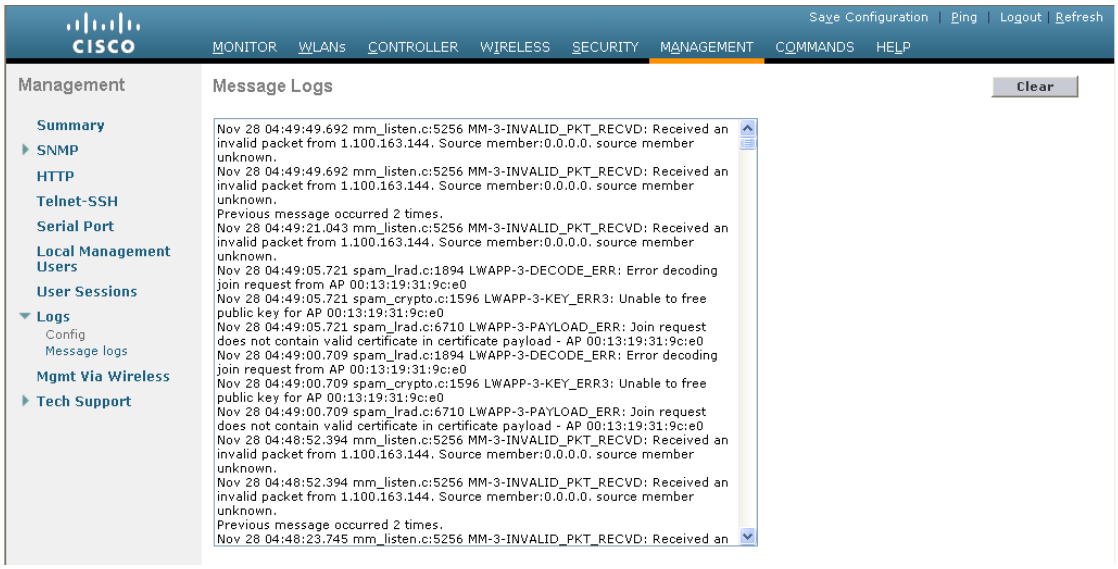
ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更を保存します。

GUI を使用したメッセージ ログの表示

コントローラの GUI を使用してメッセージ ログを表示するには、**Management** > **Logs** > **Message Logs** の順にクリックします。Message Logs ページが表示されます（図 D-2 を参照）。

図 D-2　Message Logs ページ



（注）　コントローラから現在のメッセージ ログをクリアするには、**Clear** をクリックします。

CLI を使用したシステム ロギングとメッセージ ロギングの設定

CLI を使用してシステム ロギングとメッセージ ロギングを設定する手順は、次のとおりです。

ステップ 1　システム ロギングを有効化し、syslog メッセージの宛先 syslog サーバの IP アドレスを設定するには、次のコマンドを入力します。

config logging syslog host *server_IP_address*

コントローラには最大 3 台の syslog サーバを追加できます。

（注）　コントローラから syslog サーバを削除するには、次のコマンドを入力します。
config logging syslog host *server_IP_address* **delete**

ステップ 2　syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、次のコマンドを入力します。

config logging syslog level *severity_level*

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注）　代わりに、*severity_level* パラメータに 0 ～ 7 の数を入力することもできます。

（注）　syslog レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、syslog サーバに送信されます。たとえば、syslog レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしか syslog サーバに送信されません。

ステップ 3　syslog サーバへ発信する syslog メッセージのファシリティを設定するには、次のコマンドを入力します。

config logging syslog facility *facility_code*

facility_code は、次のいずれかです。

- authorization = 認可システム。ファシリティ レベル = 4。
- auth-private = 認可システム（プライベート）。ファシリティ レベル = 10。
- cron = cron/at ファシリティ。ファシリティ レベル = 9。
- daemon = システム デーモン。ファシリティ レベル = 3。
- ftp = FTP デーモン。ファシリティ レベル = 11。
- kern = カーネル。ファシリティ レベル = 0。
- local0 = ローカル使用。ファシリティ レベル = 16。
- local1 = ローカル使用。ファシリティ レベル = 17。
- local2 = ローカル使用。ファシリティ レベル = 18。
- local3 = ローカル使用。ファシリティ レベル = 19。
- local4 = ローカル使用。ファシリティ レベル = 20。
- local5 = ローカル使用。ファシリティ レベル = 21。
- local6 = ローカル使用。ファシリティ レベル = 22。
- local7 = ローカル使用。ファシリティ レベル = 23。
- lpr = ライン プリンタ システム。ファシリティ レベル = 6。
- mail = メール システム。ファシリティ レベル = 2。
- news = USENET ニュース。ファシリティ レベル = 7。
- sys12 = システム使用。ファシリティ レベル = 12。
- sys13 = システム使用。ファシリティ レベル = 13。
- sys14 = システム使用。ファシリティ レベル = 14。
- sys15 = システム使用。ファシリティ レベル = 15。
- syslog = syslog 自体。ファシリティ レベル = 5。
- user = ユーザ プロセス。ファシリティ レベル = 1。
- uucp = UNIX 間コピー システム。ファシリティ レベル = 8。

ステップ 4　コントローラのバッファとコンソールに対するロギング　メッセージの重大度レベルを設定するには、次のコマンドを入力します。

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

（注）　代わりに、*severity_level* パラメータに 0 ～ 7 の数を入力することもできます。

（注）　ロギング　レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ロギング レベルを Warnings（重大度レベル 4）に設定した場合は、重大度が 0 ～ 4 のメッセージしかログされません。

ステップ 5　コントローラがメッセージ ログ内にソース ファイルの情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging fileinfo {**enable** | **disable**}

デフォルト値は有効（enable）です。

ステップ 6　コントローラがメッセージ ログ内にプロセス情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging procinfo {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 7　コントローラがメッセージ ログ内にトレースバック情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging traceinfo {**enable** | **disable**}

デフォルト値は無効（disable）です。

ステップ 8　メッセージ ログのタイムスタンプを有効または無効にするには、次のコマンドを入力します。

config service timestamps log {**datetime** | **uptime** | **disable**}

このとき、次のようになります。

- **datetime** = メッセージ ログは、標準の日付と時刻でタイムスタンプされます。
- **uptime** = メッセージ ログは、コントローラが最後にリセットされてからの時間でタイムスタンプされます。
- **disable** = メッセージ ログはタイムスタンプされません。

ステップ 9　変更を保存するには、次のコマンドを入力します。

save config

CLI を使用したシステム ログとメッセージ ログの表示

ロギング パラメータとバッファの内容を表示するには、次のコマンドを入力します。

show logging

次のような情報が表示されます。

```
Logging to buffer :
- Logging filter level..................................... errors
- Number of lines logged..................................... 1000
- Number of lines dropped.................................... 2752
Logging to console :
- Logging filter level..................................... errors
- Number of lines logged..................................... 0
- Number of lines dropped.................................... 3752
Logging to syslog :
- Logging filter level..................................... alerts
- Syslog facility.......................................... syslog
- Number of lines logged..................................... 0
- Number of lines dropped.................................... 3752
- Number of remote syslog hosts.............................. 2
  - Host 0.................................... 10.11.12.1
  - Host 1.................................... 192.169.1.3
  - Host 2.................................... Not Configured
Logging of traceback....................................... Enabled
- Traceback logging level.................................. debugging
Logging of process information.............................. Enabled
Logging of source file informational........................ Enabled
Timestamping of messages................................... Enabled
- Timestamp format......................................... Date and Time

Logging buffer (1000 logged, 2752 dropped)

Nov 14 13:27:32.308 mm_listen.c:5246 MM-3-INVALID_PKT_RECVD: Received an invalid
packet from 1.100.163.51. Source member:0.0.0.0. source member unknown.
Nov 14 13:27:21.204 spam_lrad.c:1894 LWAPP-3-DECODE_ERR: Error decoding join request
from AP 00:13:19:31:9c:e0
Nov 14 13:27:21.203 spam_crypto.c:1596 LWAPP-3-KEY_ERR3: Unable to free public key for
AP 00:13:19:31:9c:e0
Nov 14 13:27:21.203 spam_lrad.c:6710 LWAPP-3-PAYLOAD_ERR: Join request does not
contain valid certificate in certificate payload - AP 00:13:19:31:9c:e0
Nov 14 13:27:16.189 spam_lrad.c:1894 LWAPP-3-DECODE_ERR: Error decoding join request
from AP 00:13:19:31:9c:e0
Nov 14 13:27:16.189 spam_crypto.c:1596 LWAPP-3-KEY_ERR3: Unable to free public key for
AP 00:13:19:31:9c:e0
Nov 14 13:27:16.188 spam_lrad.c:6710 LWAPP-3-PAYLOAD_ERR: Join request does not
contain valid certificate in certificate payload - AP 00:13:19:31:9c:e0
Previous message occurred 2 times.
Nov 14 13:27:03.659 mm_listen.c:5246 MM-3-INVALID_PKT_RECVD: Received an invalid
packet from 1.100.163.51. Source member:0.0.0.0. source member unknown.
...
```

CCXv5 クライアント デバイスのトラブルシューティング

コントローラでは、CCXv5 クライアントとの通信に関する問題のトラブルシューティングのために設計された 3 つの機能がサポートされています。診断チャネル、クライアント レポート、およびローミング診断とリアルタイム診断です。CCX の詳細は、「Cisco Client Extensions の設定」の項（P. 6-37）を参照してください。

（注）　これらの機能は、CCXv5 クライアントでのみサポートされています。CCX 以外のクライアントでの使用や、以前のバージョンの CCX を実行するクライアントでの使用はサポートされていません。

診断チャネル

診断チャネル機能により、WLAN とのクライアント通信に関する問題のトラブルシューティングが可能になります。クライアントに発生している通信の問題の原因を特定するために、定義済みのテストのセットを使用してクライアントとアクセス ポイントをテストし、その後、ネットワーク上でクライアントを動作させるための修正措置を行うことができます。診断チャネルを有効にするには、コントローラの GUI や CLI を使用します。また、診断テストを実行するには、コントローラの CLI や WCS を使用します。

クライアント レポート

クライアント レポート プロトコルは、クライアント情報を交換するためにクライアントとアクセス ポイントによって使用されます。クライアント レポートは、クライアントがアソシエートするときに自動で収集されます。クライアント のアソシエート後は、いつでもコントローラの GUI や CLI を使用してクライアント レポート要求を任意の CCXv5 クライアントに送信できます。クライアント レポートには次の 4 種類があります。

- Client profile：クライアントの設定に関する情報を示します。
- Operating parameters：クライアントの現在の動作モードの詳細を示します。
- Manufacturers information：使用している無線 LAN クライアント アダプタに関するデータを示します。
- Client capabilities：クライアントの機能に関する情報を示します。

ローミング診断とリアルタイム診断

ローミング ログとリアルタイム ログ、および統計を使用して、システムの問題を解決できます。イベント ログにより、クライアント デバイスの動作を識別および追跡できるようになります。これは、WLAN 上に存在する可能性がある問題を診断する際に特に役立ちます。イベント ログはイベントのログを示し、アクセス ポイントへそれらをレポートします。イベント ログには次の 3 つのカテゴリがあります。

- Roaming ログ：このログは、指定されたクライアントのローミング イベントの履歴を示します。クライアントは、ローミングの失敗や成功などの直近のローミング イベントを最低 5 つ以上保持します。
- Robust Security Network Association（RSNA; ロバスト セキュリティ ネットワーク アソシエーション）ログ：このログは、指定されたクライアントの認証イベントの履歴を示します。クライアントは、失敗や成功などの直近の認証イベントを最低 5 つ以上保持します。
- Syslog：このログは、クライアントの内部システム情報を示します。たとえば、802.11 の動作、システムの動作などに関する問題を示します。

統計レポートは、クライアントの 802.1X とセキュリティの情報を示します。クライアント のアソシエート後は、いつでもコントローラの CLI を使用してイベント ログおよび統計の要求を任意の CCXv5 クライアントに送信できます。

GUI を使用した診断チャネルの設定

コントローラの GUI を使用して診断チャネルを設定する手順は、次のとおりです。

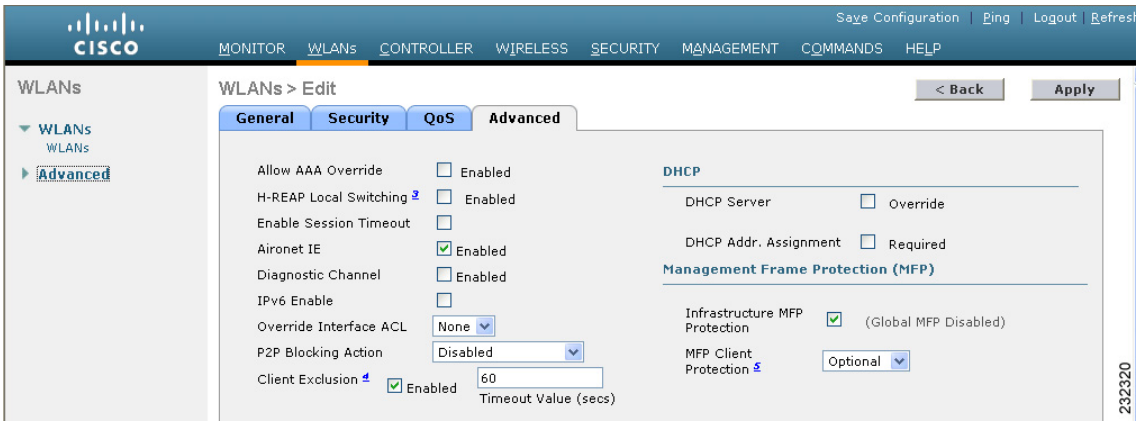
ステップ 1　**WLANs** をクリックして、WLANs ページを開きます。

ステップ 2　新しい WLAN を作成するか、既存の WLAN のプロファイル名をクリックします。

（注）　診断テストを実行するための新しい WLAN を作成することをお勧めします。

ステップ 3　WLANs > Edit ページが表示されたら、**Advanced** タブをクリックして WLANs > Edit（Advanced）ページを開きます（図 D-3 を参照）。

図 D-3　　WLANs > Edit（Advanced）ページ



ステップ 4　この WLAN 上で診断チャネルでのトラブルシューティングを有効にする場合は、**Diagnostic Channel** チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします（デフォルト値）。

（注）　クライアント上で診断テストを開始するには、CLI を使用します。詳細は、「CLI を使用した診断チャネルの設定」の項（P. D-16）を参照してください。

ステップ 5　**Apply** をクリックして、変更を適用します。

ステップ 6　**Save Configuration** をクリックして、変更を保存します。

CLI を使用した診断チャネルの設定

コントローラの CLI を使用して診断チャネルを設定する手順は、次のとおりです。

ステップ 1　特定の WLAN 上で診断チャネルでのトラブルシューティングを有効にするには、次のコマンドを入力します。

config wlan diag-channel {**enable** | **disable**} *wlan_id*

ステップ 2　変更されたかどうかを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

次のような情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... employee1
Network Name (SSID).............................. employee
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. Infinity
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Enabled
...
```

ステップ 3　DHCP テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx dhcp-test *client_mac_address*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 4　デフォルト ゲートウェイの ping テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx default-gw-ping *client_mac_address*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 5　DNS サーバの IP アドレスの ping テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx dns-ping *client_mac_address*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 6　DNS 名前解決テストを特定のホスト名に対して実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx dns-resolve *client_mac_address host_name*

（注）　このテストでは、クライアントで診断チャネルを使用する必要はありません。

ステップ 7　アソシエーション テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx test-association *client_mac_address ssid bssid* {**802.11a** | **802.11b** | **802.11g**} *channel*

ステップ 8　802.1X テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx test-dot1x *client_mac_address profile_id bssid* {**802.11a** | **802.11b** | **802.11g**} *channel*

ステップ 9　プロファイルのリダイレクト テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx test-profile *client_mac_address profile_id*

profile_id は、クライアント レポートが有効になっているクライアント プロファイルのものでなければなりません。

（注）　ユーザは親の WLAN へリダイレクトされます。他のプロファイルへはリダイレクトされません。表示されるプロファイルは、ユーザの親のプロファイルのみとなります。ただし、親 WLAN のプロファイルには、診断する子 WLAN を 1 つ持つことができます。

ステップ 10　テストを中断またはクリアする必要がある場合は、次のコマンドを使用します。

- 現在のテストを中断する要求をクライアントに送信するには、次のコマンドを入力します。
  config client ccx test-abort *client_mac_address*
  保留にできるテストは一度に 1 つだけのため、このコマンドは現在保留中のテストを中断します。
- コントローラ上のテスト結果をクリアするには、次のコマンドを入力します。
  config client ccx clear-results *client_mac_address*

ステップ 11 クライアントにメッセージを送信するには、次のコマンドを入力します。

config client ccx send-message *client_mac_address message_id*

message_id は、次のいずれかです。

- 1 = SSID が無効です。
- 2 = ネットワーク設定が無効です。
- 3 = WLAN の信頼性に矛盾があります。
- 4 = ユーザの資格情報が正しくありません。
- 5 = サポートに問い合わせてください。
- 6 = 問題は解決されました。
- 7 = 問題は解決されていません。
- 8 = 後でもう一度試してください。
- 9 = 示された問題を修正してください。
- 10 = ネットワークによってトラブルシューティングが拒否されました。
- 11 = クライアント レポートを取得しています。
- 12 = クライアント ログを取得しています。
- 13 = 取得が完了しました。
- 14 = アソシエーション テストを開始しています。
- 15 = DHCP テストを開始しています。
- 16 = ネットワーク接続テストを開始しています。
- 17 = DNS ping テストを開始しています。
- 18 = 名前解決テストを開始しています。
- 19 = 802.1X 認証テストを開始しています。
- 20 = クライアントを特定のプロファイルへリダイレクトしています。
- 21 = テストが完了しました。
- 22 = テストに合格しました。
- 23 = テストに合格しませんでした。
- 24 = 診断チャネル動作をキャンセルするか WLAN プロファイルを選択して通常の動作を再開します。
- 25 = クライアントによってログの取得が拒否されました。
- 26 = クライアントによってクライアント レポートの取得が拒否されました。
- 27 = クライアントによってテスト要求が拒否されました。
- 28 = ネットワーク（IP）設定が無効です。
- 29 = ネットワークに関する既知の機能停止または問題があります。
- 30 = 定期的なメンテナンスの時期です。
- 31 = WLAN のセキュリティ方式が正しくありません。
- 32 = WLAN の暗号化方式が正しくありません。
- 33 = WLAN の認証方式が正しくありません。

ステップ 12 最新のテストのステータスを確認するには、次のコマンドを入力します。

show client ccx last-test-status *client_mac_address*

デフォルト ゲートウェイの ping テストに対しては、次のような情報が表示されます。

```
Test Type..................................... Gateway Ping Test
Test Status................................... Pending/Success/Timeout

Dialog Token.................................. 15
Timeout....................................... 15000 ms
Request Time.................................. 1329 seconds since system boot
```

ステップ 13 最新のテスト応答のステータスを確認するには、次のコマンドを入力します。

show client ccx last-response-status *client_mac_address*

802.1X 認証 テストに対しては、次のような情報が表示されます。

```
Test Status................................... Success

Response Dialog Token......................... 87
Response Status............................... Successful
Response Test Type............................ 802.1x Authentication Test
Response Time................................. 3476 seconds since system boot
```

ステップ 14 最新の合格診断テストの結果を確認するには、次のコマンドを入力します。

show client ccx results *client_mac_address*

802.1X 認証 テストに対しては、次のような情報が表示されます。

```
dot1x Complete................................ Success
EAP Method.................................... *1,Host OS Login Credentials
dot1x Status.................................. 255
```

ステップ 15 前回のテストでクライアントが取得した関連データ フレームを確認するには、次のコマンドを入力します。

show client ccx frame-data *client_mac_address*

次のような情報が表示されます。

```
LOG Frames:

Frame Number:..................................... 1
Last Frame Number:................................ 1120
Direction:........................................ 1
Timestamp:........................................ 0d 00h 50m 39s 863954us
Frame Length:..................................... 197
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd bd b0  ............D...
00000010: 00 12 44 bd bd b0 f0 af  43 70 00 f2 82 01 00 00  ..D.....Cp......
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 32 33 2d  31 30 00 00 00 00 00 00  ...AP23-10......
00000050: 00 00 00 00 00 00 26 96  06 00 40 96 00 ff ff dd  ......&...@.....
00000060: 18 00 50 f2 01 01 00 00  50 f2 05 01 00 00 50 f2  ..P.....P.....P.
00000070: 05 01 00 00 40 96 00 28  00 dd 06 00 40 96 01 01  ....@..(....@...

00000080: 00 dd 05 00 40 96 03 04  dd 16 00 40 96 04 00 02  ....@......@....
00000090: 07 a4 00 00 23 a4 00 00  42 43 00 00 62 32 00 00  ....#...BC..b2..
000000a0: dd 05 00 40 96 0b 01 dd  18 00 50 f2 02 01 01 82  ...@......P.....
000000b0: 00 03 a4 00 00 27 a4 00  00 42 43 5e 00 62 32 2f  .....'...BC^.b2/

LOG Frames:

Frame Number:..................................... 2
Last Frame Number:................................ 1120
Direction:........................................ 1
Timestamp:........................................ 0d 00h 50m 39s 878289us
Frame Length:..................................... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 0d ed c3 a0 22  ..............."
00000010: 00 0d ed c3 a0 22 00 bd  4d 50 a5 f7 78 08 00 00  ....."..MP..x...
00000020: 64 00 01 00 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 84 00 0f 00 ff  l...............
00000040: 03 19 00 72 6f 67 75 65  2d 74 65 73 74 31 00 00  ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96  06 00 40 96 00 10 00 dd  ......#...@.....
00000060: 06 00 40 96 01 01 00 dd  05 00 40 96 03 04 dd 05  ..@.......@.....
00000070: 00 40 96 0b 01 dd 18 00  50 f2 02 01 01 81 00 03  .@......P.......

00000080: a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 d2  ...'...BC^.b2/..
00000090: b4 ab 84                                          ...

LOG Frames:

Frame Number:..................................... 3
Last Frame Number:................................ 1120
Direction:........................................ 1
Timestamp:........................................ 0d 00h 50m 39s 881513us
Frame Length:..................................... 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd 80 30  ............D..0
00000010: 00 12 44 bd 80 30 60 f7  46 c0 8b 4b d1 05 00 00  ..D..0`.F..K....
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 00 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 34 30 2d  31 37 00 00 00 00 00 00  ...AP40-17......
00000050: 00 00 00 00 00 00 26 dd  18 00 50 f2 01 01 00 00  ......&...P.....
00000060: 50 f2 05 01 00 00 50 f2  05 01 00 00 40 96 00 28  P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01  00 dd 05 00 40 96 03 04  ....@.......@...

00000080: dd 16 00 40 96 04 00 05  07 a4 00 00 23 a4 00 00  ...@........#...
00000090: 42 43 00 00 62 32 00 00  dd 05 00 40 96 0b 01 dd  BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85  00 03 a4 00 00 27 a4 00  ..P..........'..
000000b0: 00 42 43 5e 00 62 32 2f  00 0b 9a 1d 6f           .BC^.b2/....o
...
```

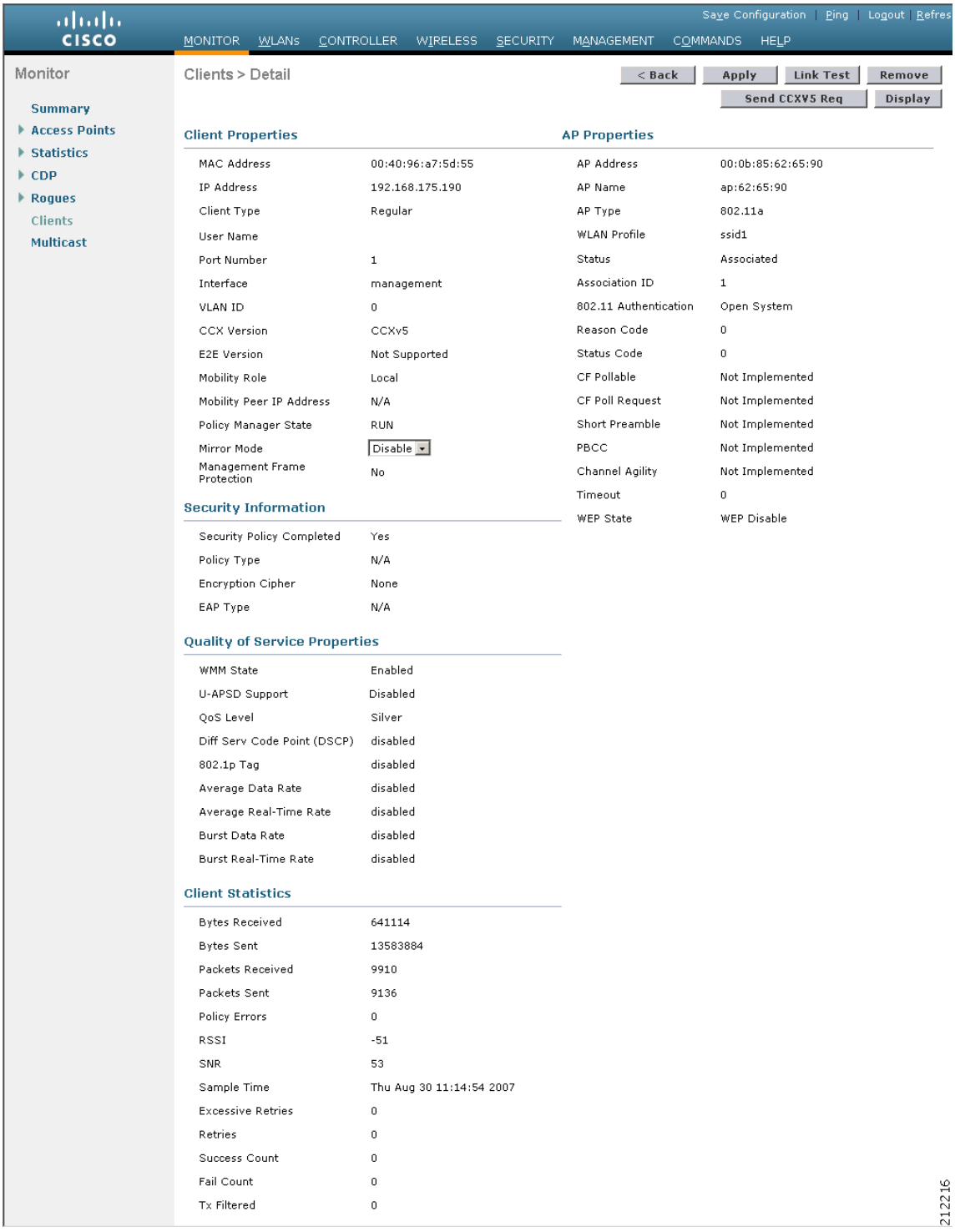
GUI を使用したクライアント レポートの設定

コントローラの GUI を使用してクライアント レポートを設定する手順は、次のとおりです。

ステップ 1　**Monitor** > **Clients** をクリックして、Clients ページを開きます。

ステップ 2　目的のクライアントの MAC アドレスをクリックします。Clients > Detail ページが表示されます（図 D-4 を参照）。

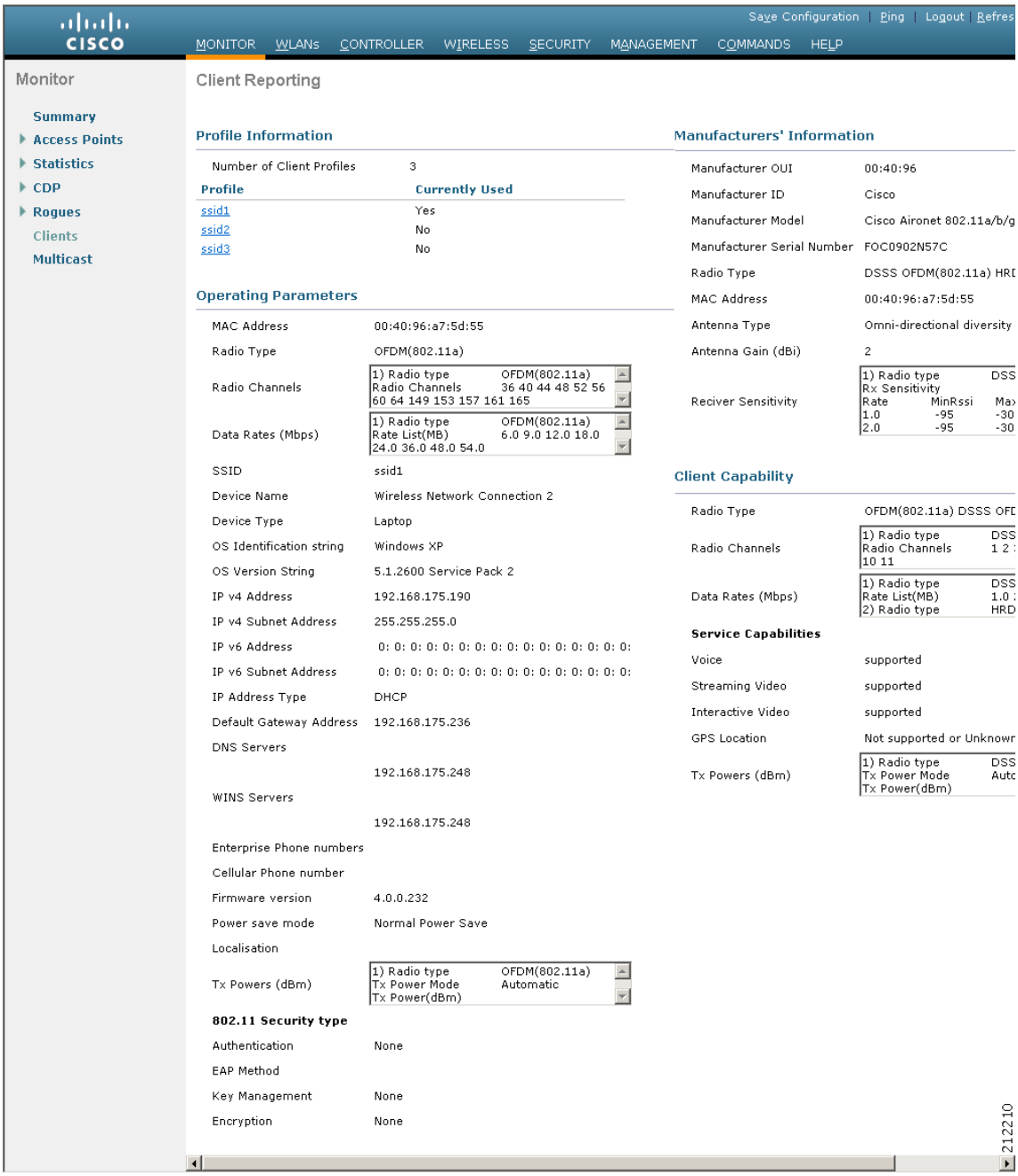
図 D-4　Clients > Detail ページ



ステップ 3　レポート要求をクライアントに送信するには、**CCXv5 Req** ボタンをクリックします。

ステップ 4　クライアントのパラメータを表示するには、**Display** をクリックします。Client Reporting ページが表示されます（図 D-5 を参照）。

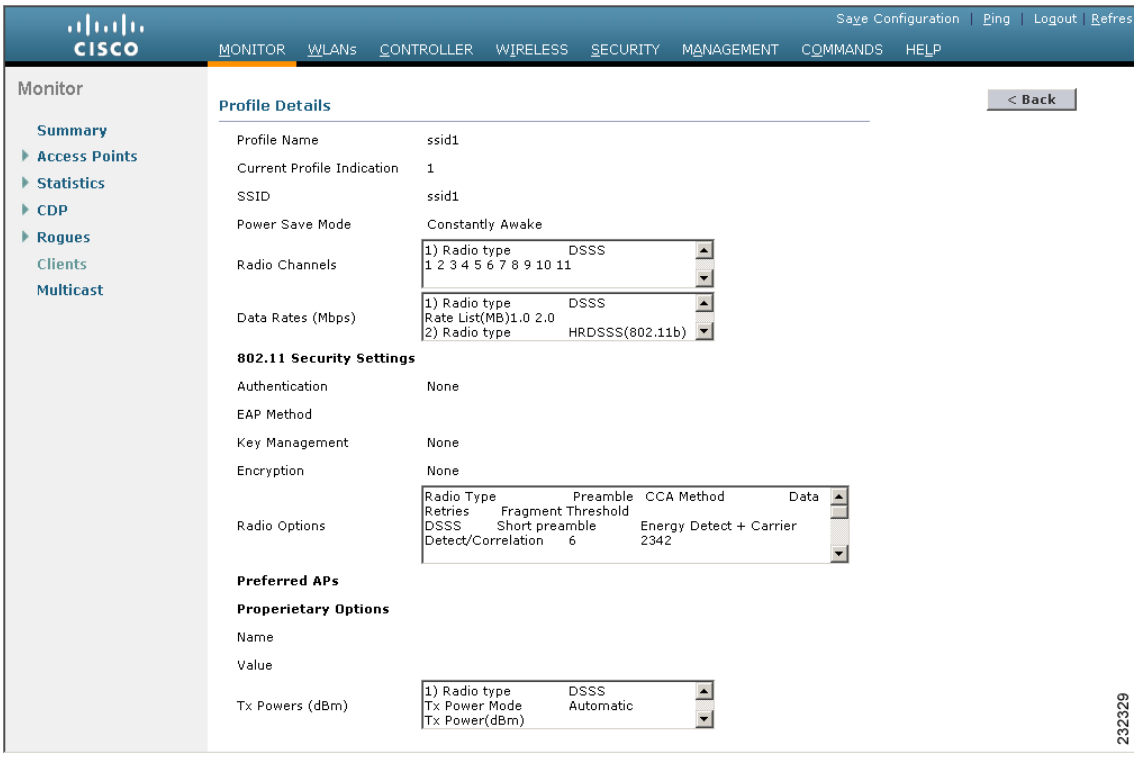
図 D-5　Client Reporting ページ



このページには、クライアント プロファイルおよび現在それらが使用されているかどうかが表示されます。クライアントの動作パラメータ、製造元、および機能に関する情報も表示されます。

ステップ 5　目的のクライアント プロファイルのリンクをクリックします。Profile Details ページが表示されます（図 D-6 を参照）。

図 D-6　Profile Details ページ



このページには、SSID、省電力モード、無線チャネル、データ レート、802.11 セキュリティ設定などのクライアント プロファイルの詳細が表示されます。

CLI を使用したクライアント レポートの設定

コントローラの CLI を使用してクライアント レポートを設定する手順は、次のとおりです。

ステップ 1　クライアント プロファイルを送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-profiles *client_mac_address*

ステップ 2　現在の動作パラメータを送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-operating-parameters *client_mac_address*

ステップ 3　製造元の情報を送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-manufacturer-info *client_mac_address*

ステップ 4　機能情報を送信する要求をクライアントに送信するには、次のコマンドを入力します。

config client ccx get-client-capability *client_mac_address*

ステップ 5　クライアント レポートの情報をクリアするには、次のコマンドを入力します。

config client ccx clear-reports *client_mac_address*

ステップ 6　クライアント プロファイルを表示するには、次のコマンドを入力します。

show client ccx profiles *client_mac_address*

次のような情報が表示されます。

```
Number of Profiles.............................. 1
Current Profile................................. 1

Profile ID...................................... 1
Profile Name.................................... wifiEAP
SSID............................................ wifiEAP
Security Parameters[EAP Method,Credential]..... EAP-TLS,Host OS Login Credentials
Auth Method..................................... EAP
Key Management................................. WPA2+CCKM
Encryption...................................... AES-CCMP
Power Save Mode................................. Constantly Awake
Radio Configuration:
Radio Type...................................... DSSS
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 1.0 2.0

Radio Type...................................... HRDSSS(802.11b)
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 5.5 11.0

Radio Type...................................... ERP(802.11g)
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

Radio Type...................................... OFDM(802.11a)
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier
Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
Radio Channels................................ 36 40 44 48 52 56 60 64 149 153 157
161 165
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0
```

ステップ 7　クライアントの動作パラメータを表示するには、次のコマンドを入力します。

show client ccx operating-parameters *client_mac_address*

次のような情報が表示されます。

```
Client Mac..................................... 00:40:96:b2:8d:5e
Radio Type..................................... OFDM(802.11a)

Radio Type..................................... OFDM(802.11a)
  Radio Channels............................... 36 40 44 48 52 56 60 64 100 104 108
112 116 120 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode................................ Automatic
  Rate List(MB)................................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

Power Save Mode................................ Normal Power Save
SSID........................................... wifi
Security Parameters[EAP Method,Credential]..... None
Auth Method.................................... None
Key Management................................. None
Encryption..................................... None
Device Name.................................... Wireless Network Connection 15
Device Type.................................... 0
OS Id.......................................... Windows XP
OS Version..................................... 5.1.2600 Service Pack 2
IP Type........................................ DHCP address
IPv4 Address................................... Available
IP Address..................................... 70.0.4.66
Subnet Mask.................................... 255.0.0.0
Default Gateway................................ 70.1.0.1
IPv6 Address................................... Not Available
IPv6 Address.................................  0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
0: 0: 0: 0:
IPv6 Subnet Mask............................  0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
0: 0: 0: 0:
DNS Servers.................................... 103.0.48.0
WINS Servers...................................
System Name.................................... URAVAL3777
Firmware Version............................... 4.0.0.187
Driver Version................................. 4.0.0.187
```

ステップ 8　クライアントの製造元情報を表示するには、次のコマンドを入力します。

show client ccx manufacturer-info *client_mac_address*

次のような情報が表示されます。

```
Manufacturer OUI.............................. 00:40:96
Manufacturer ID............................... Cisco
Manufacturer Model............................ Cisco Aironet 802.11a/b/g Wireless
Adapter
Manufacturer Serial........................... FOC1046N3SX
Mac Address................................... 00:40:96:b2:8d:5e
Radio Type.................................... DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)
Antenna Type.................................. Omni-directional diversity
Antenna Gain.................................. 2 dBi

Rx Sensitivity:
Radio Type.................................... DSSS
Rx Sensitivity ............................... Rate:1.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:2.0 Mbps, MinRssi:-95,
MaxRssi:-30
Radio Type.................................... HRDSSS(802.11b)
Rx Sensitivity ............................... Rate:5.5 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:11.0 Mbps, MinRssi:-95,
MaxRssi:-30
Radio Type.................................... ERP(802.11g)
Rx Sensitivity ............................... Rate:6.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:9.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:12.0 Mbps, MinRssi:-95,
MaxRssi:-30
Rx Sensitivity ............................... Rate:18.0 Mbps, MinRssi:-95,
MaxRssi:-30
```

ステップ 9　クライアントの機能情報を表示するには、次のコマンドを入力します。

show client ccx client-capability *client_mac_address*

（注）　このコマンドは、機能の現在の設定ではなく、クライアントで使用可能な機能を表示します。

次のような情報が表示されます。

```
Service Capability..............................  Voice, Streaming(uni-directional)
Video, Interactive(bi-directional) Video
Radio Type.....................................  DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)

Radio Type.....................................  DSSS
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  1.0 2.0

Radio Type.....................................  HRDSSS(802.11b)
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  5.5 11.0

Radio Type.....................................  ERP(802.11g)
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0

Radio Type.....................................  OFDM(802.11a)
  Radio Channels...............................  36 40 44 48 52 56 60 64 100 104 108
112 116 120 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  6.0 9.0 12.0 18.0 24.0 36.0 48.0
54.0
```

CLI を使用したローミング診断とリアルタイム診断の設定

コントローラの CLI を使用してローミング診断とリアルタイム診断を設定する手順は、次のとおりです。

ステップ 1　ログ要求を送信するには、次のコマンドを入力します。

config client ccx log-request *log_type client_mac_address*

log_type は、roam、rsna、または syslog です。

ステップ 2　ログ応答を表示するには、次のコマンドを入力します。

show client ccx log-response *log_type client_mac_address*

log_type は、roam、rsna、または syslog です。

log_type が roam であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 13s 322396us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3125(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 16s 599006us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3235(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 19s 882921us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3234(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 08s 815477us
                          Source BSSID=00:0b:85:81:06:c2, Target
BSSID=00:0b:85:81:06:d2, Transition Time=3281(ms)
                          Transition Reason: First association to WLAN
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 26s 637084us
                          Source BSSID=00:0b:85:81:06:d2, Target
BSSID=00:0b:85:81:06:c2, Transition Time=3313(ms)
```

log_type が rsna であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246578us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246625us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 01s 624375us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                        RSNA Result: Success
```

log_type が syslog であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278987us
                          Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278990us
                          Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278993us
                          Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278996us
                          Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279000us
                          Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279003us
                          Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory
elements missing in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279009us
                          Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory
elements missing in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279012us
                          Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory
elements missing in the OID response'
```

ステップ 3　統計の要求を送信するには、次のコマンドを入力します。

config client ccx stats-request *measurement_duration stats_name client_mac_address*

stats_name は、dot11 または security です。

ステップ 4　統計応答を表示するには、次のコマンドを入力します。

show client ccx stats-report *client_mac_address*

次のような情報が表示されます。

```
Measurement duration = 1

     dot11TransmittedFragmentCount       = 1
     dot11MulticastTransmittedFrameCount = 2
     dot11FailedCount                    = 3
     dot11RetryCount                     = 4
     dot11MultipleRetryCount             = 5
     dot11FrameDuplicateCount            = 6
     dot11RTSSuccessCount                = 7
     dot11RTSFailureCount                = 8
     dot11ACKFailureCount                = 9
     dot11ReceivedFragmentCount          = 10
     dot11MulticastReceivedFrameCount    = 11
     dot11FCSErrorCount                  = 12
     dot11TransmittedFrameCount        = 13
```

デバッグ ファシリティの使用方法

デバッグ ファシリティにより、コントローラの CPU とやり取りするすべてのパケットを表示できるようになります。受信したパケット、送信したパケット、またはその両方に対して有効にできます。デフォルトでは、デバッグ ファシリティによって受信されたすべてのパケットが表示されます。それらを表示する前に、アクセス コントロール リスト（ACL）を定義してパケットをフィルタリングすることもできます。ACL に渡されないパケットは、表示されずに破棄されます。

各 ACL には、動作（許可、拒否、無効化）、およびパケットの適合に使用する 1 つまたは複数のフィールドが含まれます。デバッグ ファシリティでは、次のレベルおよび値で動作する ACL が提供されます。

- ドライバ ACL
  - NPU のカプセル化の種類
  - ポート
- Ethernet header ACL
  - 宛先アドレス
  - 送信元アドレス
  - イーサネットの種類
  - VLAN ID
- IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート（該当する場合）
  - 宛先ポート（該当する場合）
- EoIP payload Ethernet header ACL
  - 宛先アドレス
  - 送信元アドレス
  - イーサネットの種類
  - VLAN ID
- EoIP payload IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート（該当する場合）
  - 宛先ポート（該当する場合）
- LWAPP payload 802.11 header ACL
  - 宛先アドレス
  - 送信元アドレス
  - BSSID
  - SNAP ヘッダの種類
- LWAPP payload IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート（該当する場合）

　－ 宛先ポート（該当する場合）

各レベルにおいて、複数の ACL を定義できます。パケットと一致する最初の ACL が、選択された ACL となります。

デバッグ ファシリティを使用する手順は、次のとおりです。

ステップ 1　デバッグ ファシリティを有効にするには、次のコマンドを入力します。

debug packet logging enable {**rx** | **tx** | **all**} *packet_count display_size*

このとき、次のようになります。

- **rx** の場合は受信したすべてのパケット、**tx** の場合は送信したすべてのパケット、**all** の場合は受信と送信の両方のパケットが表示されます。
- *packet_count* は、ログするパケットの最大数です。1 ～ 65535 の値をパケット数として入力できます。また、デフォルト値は 25 パケットです。
- *display_size* は、パケットを印刷する際の表示バイト数です。デフォルトでは、全パケットが表示されます。

（注）　デバッグ ファシリティを無効にするには、次のコマンドを入力します。**debug packet logging disable**

ステップ 2　パケットをログする ACL を設定するには、次のコマンドを使用します。

- **debug packet logging acl driver** *rule_index action npu_encap port*

  このとき、次のようになります。
  - *rule_index* の値は、1 ～ 6（両端の値を含む）です。
  - *action* は、permit、deny、または disable です。
  - *npu_encap* では、パケットのフィルタリング方法を定める、NPU のカプセル化の種類を指定します。指定可能な値には、dhcp、dot11-mgmt、dot11-probe、dot1x、eoip-ping、iapp、ip、lwapp、multicast、orphan-from-sta、orphan-to-sta、rbcp、wired-guest などがあります。
  - *port* は、パケットの送受信のための物理ポートです。
- **debug packet logging acl eth** *rule_index action dst src type vlan*

  このとき、次のようになります。
  - *rule_index* の値は、1 ～ 6（両端の値を含む）です。
  - *action* は、permit、deny、または disable です。
  - *dst* は、宛先の MAC アドレスです。
  - *src* は、送信元の MAC アドレスです。
  - *type* は、2 バイト タイプのコード（IP の場合は 0x800、ARP の場合は 0x806 など）です。このパラメータには、「ip」（0x800 の代わり）や「arp」（0x806 の代わり）などのいくつかの一般的な文字列値も使用できます。
  - *vlan* は、2 バイトの VLAN ID です。
- **debug packet logging acl ip** *rule_index action src dst proto src_port dst_port*

  このとき、次のようになります。
  - *proto* は、数値または getprotobyname() で認識される任意の文字列です。コントローラでは、次の文字列がサポートされています。ip、icmp、igmp、ggp、ipencap、st、tcp、egp、pup、udp、hmp、xns-idp、rdp、iso-tp4、xtp、ddp、idpr-cmtp、rspf、vmtp、ospf、ipip、および encap。

- *src_port* は、2 バイトの UDP/TCP 送信元ポート（telnet、23 など）か「any」です。コントローラでは、数値または getservbyname() によって認識される任意の文字列を受け付けます。コントローラでは、次の文字列がサポートされています。tcpmux、echo、discard、systat、daytime、netstat、qotd、msp、chargen、ftp-data、ftp、fsp、ssh、telnet、smtp、time、rlp、nameserver、whois、re-mail-ck、domain、mtp、bootps、bootpc、tftp、gopher、rje、finger、www、link、kerberos、supdup、hostnames、iso-tsap、csnet-ns、3com-tsmux、rtelnet、pop-2、pop-3、sunrpc、auth、sftp、uucp-path、nntp、ntp、netbios-ns、netbios-dgm、netbios-ssn、imap2、snmp、snmp-trap、cmip-man、cmip-agent、xdmcp、nextstep、bgp、prospero、irc、smux、at-rtmp、at-nbp、at-echo、at-zis、qmtp、z3950、ipx、imap3、ulistserv、https、snpp、saft、npmp-local、npmp-gui、および hmmp-ind。
- *dst_port* は、2 バイトの UDP/TCP 宛先ポート（telnet、23 など）か「any」です。コントローラでは、数値または getservbyname() によって認識される任意の文字列を受け付けます。コントローラでは、*src_port.* の場合と同じ文字列がサポートされています。

- **debug packet logging acl eoip-eth** *rule_index action dst src type vlan*
- **debug packet logging acl eoip-ip** *rule_index action src dst proto src_port dst_port*
- **debug packet logging acl lwapp-dot11** *rule_index action dst src bssid snap_type*

  このとき、次のようになります。
  - *bssid* は、Basic Service Set Identifier（BSSID; 基本サービス セット ID）です。
  - *snap_type* は、イーサネットの種類です。
- **debug packet logging acl lwapp-ip** *rule_index action src dst proto src_port dst_port*

（注） 設定されているすべての ACL を削除するには、次のコマンドを入力します。**debug packet logging acl clear-all**

ステップ 3　デバッグ出力の形式を設定するには、次のコマンドを入力します。

debug packet logging format {**hex2pcap** | **text2pcap**}

デバッグ ファシリティでは、hex2pcap と text2pcap という 2 つの出力形式がサポートされています。IOS によって使用される標準の形式では hex2pcap の使用がサポートされており、HTML フロントエンドを使用してデコードできます。text2pcap オプションは、一連のパケットを同一のコンソール ログ ファイルからデコードできるように代案として提供されます。図 D-7 は hex2pcap の出力例を示し、図 D-8 は text2pcap の出力例を示します。

図 D-7　Hex2pcap の出力例

```
tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..1n.....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                       NOPQRS
```

212235

図 D-8　Text2pcap の出力例

```
tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..1n.....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@._>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
```

232343

ステップ 4　パケットが表示されない理由を判断するには、次のコマンドを入力します。

debug packet error {**enable** | **disable**}

ステップ 5　パケットのデバッグのステータスを表示するには、次のコマンドを入力します。

show debug packet

次のような情報が表示されます。

```
Status..................................... disabled
Number of packets to display..................... 25
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-Dot11 ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   LWAPP-IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
```

無線スニファの設定

コントローラでは、アクセス ポイント をネットワーク「スニファ」として設定できます。スニファは、特定のチャネル上のすべてのパケットを取り出して、パケット アナライザ ソフトウェアを実行しているリモート マシンに転送します。これらのパケットには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。スニファを使用すると、ネットワーク アクティビティを監視して記録し、問題を検出できます。

サポートされている主なサードパーティ製のネットワーク アナライザ ソフトウェア アプリケーションは、次のとおりです。

- Wildpackets Omnipeek または Airopeek（http://www.wildpackets.com）
- AirMagnet Enterprise Analyzer（http://www.airmagnet.com）
- Wireshark（http://www.wireshark.org）

無線スニファの必須条件

無線スニファを実行するには、次のハードウェアとソフトウェアが必要です。

- **専用アクセス ポイント**：スニファとして設定された アクセス ポイント は、同時にネットワーク上の無線アクセス サービスとして機能することはできません。カバレッジの障害を防ぐために、既存の無線ネットワークの一部ではない アクセス ポイント を使用してください。
- **リモート監視デバイス**：アナライザ ソフトウェアを実行できるコンピュータ。
- **Windows XP** または **Linux オペレーティング システム**：コントローラは、Windows XP と Linux のいずれのマシンでもスニファをサポートしています。
- **ソフトウェア**および**関連ファイル、プラグイン、**または**アダプタ**：アナライザ ソフトウェアによっては、スニファを有効にするために特殊なファイルが必要となる場合があります。
  - **Omnipeek** または **Airopeek**：http://www.wildpackets.com にアクセスし、手順に従ってソフトウェアを購入、インストール、および設定してください。
  - **AirMagnet :** http://www.airmagnet.com/products/ea_cisco/#top にアクセスし、手順に従ってソフトウェアを購入、インストール、および設定してください。
  - **Wireshark** : http://tools.cisco.com/support/downloads にアクセスし、手順に従って使用しているオペレーティング システム用の Wireshark と適切なインストール ウィザードをダウンロードしてください。

GUI を使用した、アクセス ポイントのスニファの設定

コントローラの GUI を使用して、アクセス ポイント上でスニファを有効化して設定する手順は、次のとおりです。

ステップ 1　**Wireless > Access Points > All APs** の順にクリックして、All APs ページを開きます。

ステップ 2　スニファとして設定するアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます（図 D-9 を参照）。

図 D-9　All APs > Details ページ

ステップ 3　AP Mode ドロップダウン ボックスから **Sniffer** を選択します。

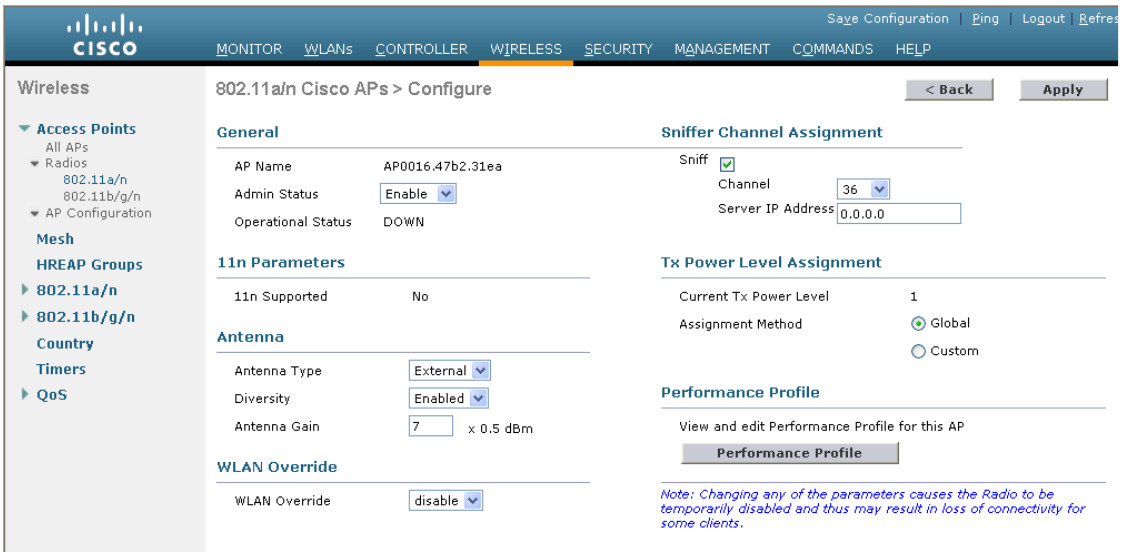
ステップ 4　**Apply** をクリックして、変更を適用します。

ステップ 5　アクセス ポイントをリブートするという警告が表示されたら、**OK** をクリックします。

ステップ 6　**Wireless > Access Points > Radios > 802.11a/n**（または **802.11b/g/n**）の順にクリックして、802.11a/n（または 802.11b/g/n）Radios ページを開きます。

ステップ 7　カーソルを目的のアクセス ポイントの青のドロップダウン矢印の上に置いて、**Configure** を選択します。802.11a/n（または 802.11b/g/n）Cisco APs > Configure ページが表示されます（図 D-10 を参照）。

図 D-10　802.11b/g/n Cisco APs > Configure ページ



ステップ 8　このアクセス ポイントでスニファを有効にする場合は、**Sniff** チェック ボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルトではオフになっています。

ステップ 9　ステップ 8 でスニファを有効にした場合は、次の手順に従ってください。

a. Channel ドロップダウン ボックスから、アクセス ポイントがパケットに対してスニファするチャネルを選択します。

b. Server IP Address フィールドに、Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスを入力します。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

CLI を使用した、アクセス ポイントのスニファの設定

コントローラの CLI を使用して、アクセス ポイント上でスニファを有効にする手順は、次のとおりです。

ステップ 1　アクセス ポイントをスニファとして設定するには、次のコマンドを入力します。

config ap mode sniffer *Cisco_AP*

Cisco_AP はスニファとして設定されるアクセス ポイントです。

ステップ 2　アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。アクセス ポイントはスニファ モードでリブートします。

ステップ 3　アクセス ポイントでスニファを有効にするには、次のコマンドを入力します。

config ap sniff {802.11a | 802.11b} enable *channel server_IP_address Cisco_AP*

このとき、次のようになります。

- *channel* はアクセス ポイントがパケットに対してスニファする無線チャンネルです。デフォルト値は 36（802.11a/n）と 1（802.11b/g/n）です。
- *server_IP_address* は Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスです。
- *Cisco_AP* はスニファとして設定されるアクセス ポイントです。

（注）　アクセス ポイントでスニファを無効にするには、次のコマンドを入力します。
config ap sniff {802.11a | 802.11b} disable *Cisco_AP*

ステップ 4　変更を保存するには、次のコマンドを入力します。

save config

ステップ 5　アクセス ポイントのスニファ設定を表示するには、次のコマンドを入力します。

show ap config {802.11a | 802.11b} *Cisco_AP*

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 17
Cisco AP Name.................................... AP1131:46f2.98ac
...
AP Mode ......................................... Sniffer
Public Safety ................................... Global: Disabled, Local: Disabled
Sniffing ........................................ No
...
```

Telnet または SSH を使用したアクセス ポイントのトラブルシューティング

コントローラは、Telnet プロトコルまたは Secure Shell（SSH）プロトコルを使用した Lightweight アクセス ポイントのトラブルシューティングをサポートしています。これらのプロトコルを使用すると、特にアクセス ポイントがコントローラに接続できない場合に、デバッグを簡単に行うことができます。

- 潜在的な競合やネットワーク セキュリティの脅威を避けるため、Telnet または SSH セッションを有効にしている間は次のコマンドを使用できません。**config terminal**、**telnet**、**ssh**、**rsh**、**ping**、**traceroute**、**clear**、**clock**、**crypto**、**delete**、**fsck**、**lwapp**、**mkdir**、**radius**、**release**、**reload**、**rename,renew**、**rmdir**、**save**、**set**、**test**、**upgrade**。
- Telnet または SSH セッション中に使用できる主なコマンドは次のとおりです。**debug**、**disable**、**enable**、**help**、**led**、**login**、**logout**、**more**、**no debug**、**show**、**systat**、**undebug**、**where**。

コントローラの CLI を使用して、Lightweight アクセス ポイント上で Telnet または SSH を有効にする手順は、次のとおりです。

ステップ 1　アクセス ポイントで Telnet または SSH の接続を有効にするには、次のコマンドを入力します。

config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

（注）　アクセス ポイントで Telnet または SSH の接続を無効にするには、次のコマンドを入力します。
config ap {**telnet** | **ssh**} **disable** *Cisco_AP*

ステップ 2　変更を保存するには、次のコマンドを入力します。

save config

ステップ 3　アクセス ポイントで Telnet または SSH が有効になっているかどうかを確認するには、次のコマンドを入力します。

show ap config general *Cisco_AP*

次のような情報が表示されます。

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.22.8.133
IP NetMask....................................... 255.255.248.0
Gateway IP Addr.................................. 10.22.8.1
Domain.......................................
Name Server...................................
Telnet State..................................... Enabled
Ssh State........................................ Enabled
...
```