ハイブリッド リモート エッジ アクセス ポイント（H-REAP）の基本的なトラブルシューティング

目次

はじめに

ハイブリッド リモート エッジ アクセス ポイント（H-REAP）はブランチ オフィスおよびリモートオフィス配備のためのソリューションです。 それは各オフィスのコントローラを配置する必要なしでオフィスからの Wide Area Network（WAN）リンクによってブランチまたはリモートオフィスの 2 つか 3 つのアクセス ポイント（AP）を設定し、制御することを顧客が可能にします。 この資料は H-REAP 環境に発生する場合があるいくつかのよくある 問題を説明します。 この資料はまた方法で情報をこれらの問題を解決する提供したものです。 H-REAP をおよびコンフィギュレーションのステップのための設定 Hybrid REAP 展開するとき H-REAP 設計上の考慮事項に関して H-REAP 設計および配置ガイドを参照して下さい。

前提条件

要件

- H-REAP および動作モードの機能ナレッジ
- コントローラへの Lightweight アクセスポイント（LAP）登録 手続のナレッジ
- Lightweight アクセス ポイント プロトコル（LWAPP）に関する知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 4400 および 2100 シリーズ ワイヤレス LAN コントローラ（WLCs）その実行バージョン 5.1
- Cisco 1130AG AP、1240 AG AP、および 1250 AP
- バージョン 12.4 を実行する Cisco 2800 および 3800 シリーズ ルータ

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

これらは H-REAP を使用する間、覚えるべき制限です。

- Hybrid REAP は 1130AG、1140、1240、1250、1260、AP801、AP 802、1040、および AP3550 AP だけと Cisco WiSM、Cisco 5500、4400、2100、2500、統合サービス ルータのための屈曲 7500 シリーズでコントローラ、Catalyst 3750G Integrated Wireless LAN Controller スイッチおよびコントローラ ネットワークモジュール サポートされます。
- コントローラがそれに戻ってトンネル伝送されないデータをコントロールできないのでデータパスの制御を、VPN のような必要とするどのセキュリティ型でもローカルでスイッチド WLAN のトラフィックを、使用しません。 H-REAP とコントローラ間のパスが稼働していれば、他のどのセキュリティ型も中央にでまたはローカルでスイッチド WLAN 動作します。 このコンジットがダウンしている時、これらのセキュリティオプションのサブセットだけが新しいクライアントがローカルでスイッチド WLAN に接続することを可能にします。
- H-REAP アクセス ポイントが入るとき独立方式、開いたのために、共有されて設定される WLAN、WPA-PSK、または WPA2-PSK 認証は「ローカル認証、ローカル スイッチング」状態を入力し、新しいクライアント認証を続けます。コントローラ ソフトウェア リリース 4.2 または それ 以降では、これは 802.1X、WPA-802.1X、WPA2-802.1X、または Cisco Centralized Key Management （CCKM）のために設定される WLAN にまたあてはまます。 ただし、これらの認証種別は外部のRADIUSサーバが設定されることを必要とします。 他の WLAN は「認証入力しま」、状態の下で切り替えます（WLAN が中央切り替えのために設定されたら）または（WLAN がローカル スイッチングのために設定されたら）「認証、ローカル スイッチング」状態を。
- 接続されたモードの H-REAP を使うと、コントローラはクライアント 除外/何人かのクライアントが AP を使うと関連付けることを防ぐためにブラックリストに載せることを課して自由です。 この機能は自動化されるか、または手動方式で発生する場合があります。 グローバルおよび毎 WLAN コンフィギュレーションに関して、クライアントは繰り返された失敗した認証試みから IP 盗難まで及ぶ、またあらゆる所定の時間のためにことができます原因の多くのために除く。 また、クライアントをこの除外リストに手動で入れることもできます。 この機能の使用は AP が接続されたモードにある間、だけ可能性のあるです。 この除外リストに置かれたクライアントは独立方式にある間、AP に接続してなく残ります
- MAC 認証を使用する WLAN は（ローカルかアップストリーム）もはや 802.1X の同様に設定された WLAN 方法と同一であるか、または WebAuth が同じモードで操作する AP が独立方

式にあるとき追加クライアント認証を可能にしません。
- WLC バージョン 4.2.61.0 および それ 以降は CCKM を使用して高速セキュアローミングをサポートします。 CCKM を使用する H-REAP モード サポート レイヤ2 高速セキュアローミング。 この機能は 1 AP から別のものにクライアント 移動として完全な RADIUS EAP 認証のための必要を防ぎます。 CCKM ファースト ローミングを H-REAP アクセス ポイントによって使用するために、H-REAP グループを設定する必要があります。

H-REAP トラブルシューティング

起こり、スムーズな H-REAP 設定およびクライアント 接続を防ぐ状況および少数の一般的なシナリオがあります。 これらは推奨される トラブルシューティングの手順とのちょうど少数のそのような状況です。

H-REAP は WLC に加入しません

これらは WLC に加入しない H-REAP のための基本的な原因です:

- H-REAP はそれ自身に IP アドレスを得ることができませんかまたは不正確な IP アドレスと割り当てられました。
- H-REAP と WLC 間にレイヤ3 接続がありません。
- H-REAP と WLC 間に Lightweight Access Point Protocol（LWAPP）接続がありません。
- 他の理由は WLC または H-REAP 自体における別のコントローラ、証明書 ミスマッチ、問題、等に加入する H-REAP です。

これらの問題を解決するためにこれらのステップを実行して下さい:

1. H-REAP AP IP アドレスが割り当てられることを確認して下さい。DHCP が AP のコンソールによって使用される場合、AP がこのコマンドでアドレスを取得することを確認して下さい:を探します。
   ```
   AP_CLI#show dhcp lease
   ```
   このコマンドの出力がどれもではない場合、DHCP アドレッシングがこの AP のために使用されないことを意味します。静的IP アドレスが適切な方法ある意味では AP に割り当てられるようにこの場合、して下さい。 これはこのコマンドで確認することができます:
   ```
   AP_CLI#show lwapp ip config


   LWAPP Static IP Configuration
   IP Address          10.77.244.222
   IP netmask          255.255.0.0
   Default Gateway     10.77.244.220
   ```
   出力は AP に 10.77.244.222 の静的IP アドレスを割り当てました表示するものです。 これが割り当てられるべき意図されていた IP アドレスではない場合 IP アドレスを訂正して下さい。
2. コントローラの AP とマネージメントインターフェイス間の IP接続を確認して下さい。IP アドレスが確認されたら、AP がコントローラと通信できることを確かめるためにコントローラの管理IPアドレスを ping して下さい。 この構文と AP のコンソールによって ping コマンドを使用して下さい:
   ```
   AP_CLI#ping 10.77.244.210
   !--- 10.77.244.210/27 is the example management interface IP address of the controller.
   ```

PING が正常ではない場合、AP とコントローラ間の IP接続に問題があることを示します。アップストリーム ネットワークが正しく設定されること、そして社内ネットワークに戻るWANアクセスが稼働しているようにして下さい。 コントローラが正常に動作して、あらゆる NAT/PAT 境界の後ろにないことを確認して下さい。 コントローラから同じ構文の AP に ping して下さい。 コントローラと H-REAP 間のパスのための MTU が 1500 の少くともあることを確かめて下さい。 これは PING と- WAN の H-REAP 側のコンピュータからの I 1500 *<WLC 管理 IP >*コマンド チェックすることができます。成功したping コマンドの出力例はここにあります:

```
ping -l 1500 10.77.244.210

Pinging 10.77.244.204 with 1500 bytes of data:

Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252
Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252

Ping statistics for 10.77.244.204:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum =  6ms, Average =  6ms
```

3. AP とコントローラ間の LWAPP 接続を確認して下さい。H-REAP とコントローラ間の IP接続が確認されたら、LWAPP メッセージが WAN を渡って確認し伝えられる、関連問題を行って下さいことを明らかにするためにコントローラの LWAPP デバッグを。 最初に、コントローラ上で、デバッグ出力の範囲を制限するための MAC フィルタを作成します。 単一 AP にそれに続くコマンドの出力を制限するのにこのコマンドを使用して下さい:
   AP_CLI#**debug mac addr** *<AP's wired MAC address>* .
   デバッグ 出力を制限するためにこれが設定 されたらこのコマンドで LWAPP デバッグをつけて下さい:
   Controller_CLI#**debug lwapp events enable**

   これらと同じようなデバッグ メッセージが表示されます:

```
-----------------------------------------------
       -------------------------------------------------
       -------------------------------------------------------
       Thu Mar 15 15:07:56 2007: 00:12:44:b2:ae:d0
Received LWAPP DISCOVERY REQUEST from AP 00:12:44:b2:ae:d0
to ff:ff:ff:ff:ff:ff on port '1'
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Received LWAPP JOIN REQUEST from AP 00:12:44:b2:ae:d0
to 00:0b:85:33:84:a0 on port '1'
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
 AP AP0012.d92b.3a5e: txNonce  00:0B:85:33:84:A0 rxNonce  00:12:44:B2:AE:D0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
LWAPP Join-Request MTU path from AP 00:12:44:b2:ae:d0
is 1500, remote debug mode is 0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0 Successfully added NPU Entry
for AP 00:12:44:b2:ae:d0 (index 50)Switch IP: 10.77.244.211,
Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 172.16.1.10, AP Port: 45989,
        next hop MAC: 0 0:12:d9:2b:3a:5e
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Successfully transmission of LWAPP Join-Reply to AP 00:12:44:b2:ae:d0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
 Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 0
       Thu Mar 15 15:08:06 2007: 00:12:44:b2:ae:d0
Register LWAPP event for AP 00:12:44:b2:ae:d0 slot 1
       Thu Mar 15 15:08:08 2007: 00:12:44:b2:ae:d0
```

```
Received LWAPP CONFIGURE REQUEST from AP 00:12:44:b2:ae:d0 to  00:0b:85:33:84:a0
       ----------------------------------------------------
       ----------------------------------------------------
       ----------------------------------------------------
```

このデバッグ 出力は AP からの正常な加入 要求およびコントローラからの平行加入応答に先行しているコントローラと AP 間の LWAPP メッセージの正常な伝達を示します。 AP がコントローラによって登録される以降。そのような LWAPP デバッグ メッセージが見られない場合、H-REAP にコントローラが検出することができる少なくとも 1 方式があることを確認して下さい。 そのようなメソッドが (ローカルサブネット ブロードキャスト、DHCP オプション 43、または DNS のように) きちんと整っていたら、正しく設定されることを確認して下さい。 他の発見 方法がきちんと整っていない場合、コントローラの IP アドレスがコンソール CLI による AP に手動で入力されるようにして下さい。

```
AP_CLI#lwapp ap controller ip address
  <management interface Ip address of controller>
```

4. H-REAP を手動で設定する場合、AP がネットワークの別の位置にによって変わるときクリア以前に関連するコントローラ 情報確かめて下さい。 これは AP が新しい場所のコントローラによって関連付けるようにします。 以前のコンフィギュレーションを削除するために、AP CLI#clear **lwapp private 構成**コマンドを発行して下さい。 それから AP が正しいコントローラに加入するかどうか、確認して下さい。どのとコントローラを AP が伝えるか確認するために、AP CLI に **debug ip udp コマンドを**発行して下さい。 AP の IPスタックを横断するこのコマンドの出力から、各パケットの送信元 および 宛先アドレスを表示して下さい。次に例を示します。AP_CLI#debug **IP UDP**

```
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=60
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223)
, length=75
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989)
, length=49
*Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=76
*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
```

この出力から、UDP パケットが AP から送信されること、そしてマネージメントインターフェイスに達することがわかります (10.77.244.210) およびコントローラの AP マネージャ インターフェイス (10.77.244.211) 。

5. コントローラに加入する AP 試みが失敗する場合証明書問題を解決して下さい。LWAPP メッセージがコントローラで見られるが、AP が加入しない場合これは本当らしいです証明書問題。 トラブルシューティング 証明書問題が含まれているその他の LWAPP トラブルシューティングに役立つ ヒントに関しては LWAPP アップグレード ツールを解決します助言を参照して下さい。
6. H-REAP AP が WLCs に加入しないという 1 つの他の原因はプロキシARP が H-REAP AP のためのゲートウェイで無効に なる場合です。 AP コンソールから、このメッセージは記録されます:

```
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=60
*Mar 15 16:41:47.999: UDP: sent src=10.77.244.222(45989), dst=10.77.244.210(12223)
, length=75
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
*Mar 15 16:41:48.000: UDP: rcvd src=10.77.244.210(12223), dst=10.77.244.222(45989)
, length=49
```

```
*Mar 15 16:41:57.778: UDP: sent src=10.77.244.222(45989), dst=10.77.244.211(12223)
, length=76
*Mar 15 16:41:57.779: UDP: rcvd src=10.77.244.211(12223), dst=10.77.244.222(45989)
, length=22
```

これは Cisco バグ ID CSCse92856 によって引き起こされる場合があります。 この問題は AP1130 および AP1240 にだけ適用します。 この問題は AP1000s、AP1100、または AP1200 に適用しません。この問題はこれらの条件が満たされるとき発生します:HREAP モードは WLAN で使用されます。 ローカル モードはこの問題から影響を受けません。 ネイティブ VLAN マッピングが必要となります。AP は WLCs の AP マネージャより別の IPサブネットであるなります。プロキシARP は AP のためのデフォルト ゲートウェイで無効に なります。H-REAP AP は DHCPサーバからデフォルト ゲートウェイを得ます。この問題を解決するため、AP のデフォルト ゲートウェイ ルータのイネーブル プロキシARP。

H-REAP 動作モードの確認

H-REAP が正しいコントローラに加入したら、H-REAP AP がコントローラにいつでも接続されるかどうか確認できます。 すなわち、確認どのモードがで H-REAP によって AP が機能するかできます。 これは**提示 lwapp と収獲します** AP CLI からの **status コマンドを**確認することができます。

AP_CLI#show **lwapp はステータスを収獲します**

```
 AP Mode:          REAP, Connected
                   Radar detected on:
```

この出力は H-REAP AP が H-REAP モードおよび接続されたモードにあると言います。 すなわち、AP とコントローラ間の WAN リンクは（接続される）稼働し、動作モードは H-REAP です。

AP_CLI#show **lwapp はステータスを収獲します**

```
AP Mode:          REAP, Standalone
                  Radar detected on:
```

この出力は AP とコントローラ間の WAN リンクがダウンしていることを AP が独立方式にある、つまり意味しますと言います。 AP 動作モードは REAP です。 これはローカル認証でローカルスイッチングのために設定される WLAN がこの WLAN へ機能および割り当て新しいクライアントであることを意味します。 H-REAP の異なる動作モードを理解するために H-REAP 動作モード 設定例を参照して下さい。

H-REAP の Console コマンドは正常に動作していないし、エラーを返します

H-REAP CLI 戻りによって **ERROR!!!を**実行された 設定コマンド（設定の設定か消去）Command is disabled」というメッセージが返されます。 これは 2 つの原因の 1 つのために発生する場合があります:

- 接続されたモードにある H-REAP AP は（コントローラに登録されている）コンフィギュレーションがコンソールによって設定 されるか、または削除されないようにしません。 AP がこの状態にあるとき、コンフィギュレーションはコントローラ インターフェイスを通してする必要があります。 AP の設定コマンドへのアクセスが必要となる場合、設定コマンドを入力するように試みる前に AP が独立方式にあるようにして下さい。
- AP がコントローラにいずれかの時点で接続するか、または登録したら、H-REAP のデフォル

ト イネーブルパスワードが、Cisco、変更されるようにして下さい。 このデフォルトパスワードが変更されない場合、独立方式に移動されます H-REAP のコンソール CLI にアクセスできません。 イネーブルパスワードは AP が接続されるコントローラの CLI によってしか設定することができません。 コントローラでこのコマンド構文がコントローラのすべての AP にユーザー AP のコンソールパスワードかパスワードを設定 するのに使用することができます: （ WLC_CLI ） >config **ap ユーザ名 *<user-id>* パスワード *<passwd>* {すべて | <AP name>}**。 次に例を示します。

```
WLC-1>config ap username hreap password hreap all
```

注: WLC バージョン 5.0 および それ 以降を実行する場合、このコマンドを使用して下さい: **構成 ap mgmtuser は username username password password 秘密シークレットを{すべて追加します | AP 名前}注:** 設定 される コンソールパスワードがなかった AP に関してはコマンドがコントローラで入力されるときだけこの設定が AP に送信 されることに注意して下さい。 続いて WLC に加入するどの AP でもコマンドが再度入力されるように要求します。**注:** これらのコマンドは**ボックスから**デフォルトパスワードが変更されない時でさえ H 収獲します動作します:**lwapp ap ホスト名 *<name>*lwapp ap IP アドレス *<AP IP アドレス > < サブネットマスク >*lwapp ap ip default-gateway *<Gateway の IP アドレス >*lwapp ap コントローラ IP アドレス *<WLC IP アドレス >*クリア lwapp private 構成**

- **注:** 完全に AP に工場出荷時状態へ AP を、戻すことはイーサネット ライトが橙色に変わるまで **Mode ボタンを**起動しましたり、押します。 1131 で、このライトは Mode ボタンの近くにあり、イーサネットで明確にマークされます。 1242 で、これは白いプラスチック正面の下にあり、Mode ボタンを E. Release と notated AP を起動します許可すれば。 AP は AP の IOS リカバリイメージによって利用可能であるインターフェイスに戻ります。 新しい設定コマンドが望まれたら、AP は Cisco IOS® ソフトウェア リリース 12.3(11)JX1 または それ 以降を実行する必要があることに注意して下さい。 これは AP のコンソールによって **show version コマンドの**入力によって確認することができます。**注:** すべての **show および debug コマンドは** AP が接続されたモードにある間、設定 される デフォルトパスワードなしで機能し続け。この時点でどの LWAPP コンフィギュレーションでも作成するただことができます。

クライアントは H-REAP に接続できません

無線クライアントが H-REAP に接続できない場合これらのステップを実行して下さい:

1. コントローラと H-REAP 間の WAN リンクが稼働しているようにして下さい。
2. AP がきちんとコントローラに加入したこと、そしてコントローラは少なくとも 1 つの正しく設定された（および有効に される） WLAN があることを確認して下さい。 **H-REAP が**ローカルでスイッチド WLAN のための使用可能状態にあるようにして下さい
3. コントローラで、SSID をこのプロセスの解決を助けるようにブロードキャストするように WLAN を設定して下さい。 クライアントエンドで、クライアントが SSID の AP を見つけられるかどうか確認して下さい。 クライアントの WLAN の SSID 名前およびセキュリティとコンフィギュレーションを映して下さい。 接続に関する問題の大半は、クライアント側のセキュリティ設定によって発生します。
4. ローカルでスイッチド WLAN のクライアントがきちんと当たる IP であることを確認して下さい。 DHCP が使用される場合、アップストリーム DHCPサーバが正しく設定され、それクライアントにアドレスを提供することを確かめて下さい。 静的なアドレッシングが使用される場合、クライアントが正しいサブネットのために正しく設定されるようにして下さい。

5. UDP ポート 12222 および 12223 があらゆる中間ファイアウォールで開いていることを確認して下さい。
6. 更に H-REAP のコンソールポートでクライアント 接続上の問題を解決するために、このコマンドを発行して下さい:
   ```
   AP_CLI#show lwapp reap association
   ```
7. クライアントの 802.11 接続上の問題をデバッグするために、このコマンドを発行して下さい:
   ```
   AP_CLI#debug dot11 state enable
   ```
8. クライアントの 802.1X 認証プロセスおよび失敗をデバッグするために、このコマンドを発行して下さい:
   ```
   AP_CLI#debug dot1x events enable
   ```

Wireless Control System （ WCS ）レポート H-REAP モードの AP への不正確なクライアント数

ワイヤレス環境が Wireless Control System （ WCS ）によって管理されれば、時々この WCS はコントローラが規定 する正しいクライアント数に対して H-REAP AP に不正確なクライアントを、報告できます。

この問題は Cisco Bug ID CSCsg48059 （ 登録ユーザ専用 ）が原因で発生します。 WCS は H-REAP がコントローラで有効に なるとき余りに高いクライアント数を報告します。 これは回避策です。

1. 何人クライアントが AP かある特定のコントローラに関連付けられるか調べるために、**WCS モニタ > クライアント** 機能を使用して下さい。
2. 重複を避けるために無線型によって制限されるコントローラか AP によって検索して下さい。
3. 本当人口として見つけられる項目の総数を使用して下さい。また、WLC を使用して、正しいクライアント数を確認することもできます。

この問題はワイヤレス LAN コントローラ リリース 4.0.206.0 で解決されます。

関連情報

- Wireless LAN Controller に接続しない Lightweight アクセス ポイントのトラブルシューティング
- H-Reap 設計および導入ガイド
- Hybrid REAP の設定
- H-REAP 動作モードの設定例
- WCS の Hybrid REAP の設定
- Lightweight アクセス ポイントに関する FAQ
- テクニカル サポートとドキュメント – Cisco Systems