目次

概要

Hybrid Remote Edge Access Point (H-REAP; ハイブリッド リモート エッジ アクセス ポイント) は、ブランチ オフィスとリモート オフィスに導入されるソリューションです。 このソリューションを導入すると、Wide Area Network (WAN; ワイド エリア ネットワーク) リンクを介して、本部オフィスからブランチ オフィスまたはリモート オフィスにある 2 ~ 3 個の Access Point (AP; アクセス ポイント) を設定したり制御したりできます。各オフィスにコントローラを配置する必要はありません。 このドキュメントでは、H-REAP 環境に発生するいくつかの一般的な問題について説明します。 このドキュメントでは、これらの問題をトラブルシューティングする方法も説明します。 H-REAP を導入するときの H-REAP 設計の考慮事項については、『H-REAP の設計および導入ガイド』を参照してください。設定手順については、「Hybrid REAP の設定」を参照してください。

前提条件

要件

- H-REAP とその動作モードに関する実践的な知識
- Lightweight Access Point (LAP; Lightweight アクセス ポイント) をコントローラに登録するプロセスの知識
- 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。

- バージョン 5.1 を実行する Cisco 4400 と 2100 シリーズ Wireless LAN Controller (WLC; ワ

イヤレス LAN コントローラ）
- Cisco 1130AG AP、1240 AG AP、1250 AP
- バージョン 12.4 を実行する Cisco 2800 と 3800 シリーズ ルータ

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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

H-REAP の使用には、注意する必要がある制限があります。

- Hybrid REAP は 1130AG、1140、1240、1250、1260、AP801、AP 802、1040、AP3550 AP および Cisco WiSM、Cisco 5500、4400、2100、2500、Flex 7500 シリーズ コントローラ、Catalyst 3750G Integrated Wireless LAN Controller Switch、サービス統合型ルータ用のコントローラ ネットワーク モジュールでのみサポートされています。
- コントローラではアクセス ポイントからトンネリングされてこないデータは制御できないため、データ パスの制御を必要とするセキュリティ タイプ（VPN など）は、ローカル スイッチング WLAN 上のトラフィックに対しては機能しません。 その他のセキュリティ タイプは、H-REAP とコントローラの間のパスが稼働している限り、中央、ローカルのいずれでスイッチが行われるかに関係なく、すべての WLAN に対して機能します。 このコンジットがダウンした場合は、これらのセキュリティ オプションの一部のみが機能し、新しいクライアントはローカルでスイッチされる WLAN にだけ接続できます。
- H-REAP アクセス ポイントがスタンドアロン モードになると、オープン、共通、WPA-PSK、または WPA2-PSK の認証用に設定された WLAN は、「ローカル認証、ローカル スイッチング」状態になり、新しいクライアント認証を続行します。コントローラ ソフトウェア リリース 4.2 以降では、802.1X、WPA-802.1X、WPA2-802.1X、または Cisco Centralized Key Management（CCKM）用に設定された WLAN でもこのように動作します。 ただし、これらの認証タイプでは外部の RADIUS サーバが設定されている必要があります。 その他の WLAN は、「認証停止、スイッチング停止」状態（WLAN が中央スイッチング用に設定されている場合）または「認証停止、ローカル スイッチング」状態（WLAN がローカル スイッチング用に設定されている場合）のいずれかになります。
- 接続モードの H-REAP では、コントローラは、クライアントがその AP に関連付けることを防止するために、クライアントの除外やブラックリストへの掲載を自由に行うことができます。 この機能は、自動方式でも手動方式でも発生することがあります。 グローバル設定および WLAN ごとの設定に従い、複数回の認証試行失敗や IP 盗用など、さまざまな理由によりクライアントを任意の期間除外することができます。 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。 この機能は、AP が接続モードである間にのみ使用可能できます。 この除外リストに掲載されているクライアントは、スタンドアロン モードになっている間でもアクセス ポイントに接続できません。
- AP がスタンドアロン モードのとき、MAC 認証を使用する WLAN（ローカルまたはアップストリーム）では、追加のクライアント認証を許可しません。これは、同様に設定された 802.1X または WebAuth の WLAN が同じスタンドアロン モードで動作する仕組みと同じで

す。
- WLC バージョン 4.2.61.0 以降は、CCKM を使用して高速セキュア ローミングがサポートされています。 H-REAP モードは、CCKM を使用して、レイヤ 2 の高速セキュア ローミングをサポートしています。 この機能によって、クライアントが 1 つの AP からもう 1 つの AP にローミングするときに、完全な RADIUS EAP 認証を行う必要がなくなります。 H-REAP アクセス ポイントで CCKM 高速ローミングを使用するには、H-REAP グループを設定する必要があります。

H-REAP のトラブルシューティング

H-REAP の円滑な設定やクライアント接続を妨げる可能性がある一般的な状況がいくつかあります。 ここでは、そのような状況の一部と、推奨されるトラブルシューティングの手順について説明します。

H-REAP が WLC に加入しない

H-REAP が WLC に加入しない場合には、次のような基本的な理由があります。

- H-REAP が IP アドレスを取得できない、または間違った IP アドレスが割り当てられている。
- H-REAP と WLC 間にレイヤ 3 接続がない。
- H-REAP と WLC 間に Lightweight Access Point Protocol (LWAPP; Lightweight アクセス ポイント プロトコル) 接続がない。
- 他の理由として、H-REAP が異なるコントローラに加入しようとしている、証明書が一致しない、WLC または H-REAP 自体の問題などがある。

次の手順を実行して、これらの問題をトラブルシューティングします。

1. H-REAP AP に IP アドレスが割り当てられていることを確認します。AP のコンソールから DHCP を使用している場合は、次のコマンドを使用して AP がアドレスを受け取っていることを確認します。を探します。`AP_CLI#`**`show dhcp lease`**このコマンドの出力がない場合は、この AP には DHCP アドレスが指定されていません。次に、スタティック IP アドレスが AP に正しく割り当てられていることを確認します。 次のコマンドを使用して確認できます。`AP_CLI#`**`show lwapp ip config`**`LWAPP Static IP Configuration`**`IP Address 10.77.244.222`**`IP netmask 255.255.0.0Default Gateway 10.77.244.220`AP に割り当てられている 10.77.244.222 というスタティック IP アドレスが出力に表示されます。 この IP アドレスが、割り当てられている目的のアドレスと異なる場合は、IP アドレスを修正します。
2. AP とコントローラの管理インターフェイス間の IP 接続を確認します。IP アドレスが確認されたら、コントローラの管理 IP アドレスに ping を送信し、AP がコントローラと通信できることを確認します。 AP のコンソールから次の構文を使用して ping コマンドを使用します。`AP_CLI#`**`ping`** `10.77.244.210`*`!--- 10.77.244.210/27 is the example management interface IP address of the controller.`*ping に成功しない場合は、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。 アップストリームのネットワークが正しく設定されていることを確認し、企業ネットワークへの WAN アクセスが稼働していることを確認します。 コントローラが稼働していて、**NAT/PAT** 境界の背後に**配置されていない**ことを確認します。 コントローラから AP に同じ構文で ping を送信します。 コントローラと H-REAP 間のパスの **MTU** が、少なくとも **1500** に設定されていることを確認します。 これは、WAN の H-REAP 側にあるコンピュータから **ping -l 1500 <WLC 管理 IP>** コマンドを使用して確認できます。成功した **ping** コマンドの出力例を次に示します。**`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=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Reply from 10.77.244.210: bytes=1500 time=6ms TTL=252Ping 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 接続を確認します。H-REAP とコントローラの間の IP 接続を確認した後は、コントローラ上で LWAPP デバッグを実行し、WAN 経由で LWAPP メッセージが送受信されていることを確認し、関連する問題を特定します。 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。 後続のコマンドの出力を 1 つの AP に限定するには、次のコマンドを使用します。AP_CLI#**debug mac addr** <AP?s wired MAC address>.デバッグ出力を制限するように設定したら、次のコマンドを使用して LWAPP のデバッグを有効にします。Controller_CLI#**debug lwapp events enable**次のようなデバッグ 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 ---------- ---------- ----------このデバッグ出力では、コントローラと AP 間の LWAPP メッセージの送信が成功したことが示されています。それに続いて、AP からの加入要求の成功が示され、それと並行してコントローラからの加入応答が示されています。この後、AP はコントローラに登録されます。このような LWAPP デバッグ メッセージが表示されない場合は、コントローラを検出するための方式が少なくとも 1 つ H-REAP で設定されていることを確認します。 これらの方式 (ローカル サブネットのブロードキャスト、DHCP オプション 43、DNS など) が設定されている場合は、設定が適切であることを確認します。 検出方式が何も設定されていない場合は、コンソール CLI から、コントローラの IP アドレスが AP に手動で入力されていることを確認します。AP_CLI#**lwapp ap controller ip address** <management interface Ip address of controller>
4. H-REAP を手動で設定した場合、ネットワークの別の場所に AP を移動するときに、以前に関連付けられていたコントローラ情報を必ず消去します。 消去すると、新しい場所で AP とコントローラを関連付けることができます。 以前の設定を消去するには、AP CLI**#clear lwapp private-config** コマンドを発行します。 次に、AP が正しいコントローラに加入するかどうかを確認します。AP が通信するコントローラを確認するには、**debug ip udp** コマンドを AP CLI に発行します。 このコマンドの出力から、AP の IP スタックを通過する各パケットの送信元アドレスと宛先アドレスを確認します。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 から送信されていることと、それらのパケットが管理インターフェイス (10.77.244.210) とコントローラの AP Manager インターフェイス (10.77.244.211) に到達することが分かります。

5. AP がコントローラへの加入を試みても失敗する場合は、証明書の問題のトラブルシューティングを行います。コントローラに LWAPP メッセージが表示されているにもかかわらず、AP が加入に失敗する場合は、証明書に問題がある可能性があります。 証明書の問題のトラブルシューティングなど、LWAPP のトラブルシューティングのヒントについては、『LWAPP アップグレード ツールのトラブルシューティングのヒント』を参照してください。
6. H-REAP AP が WLC に加入しないもう 1 つの理由は、H-REAP AP のゲートウェイでプロキシ ARP がディセーブルになっているためです。 このメッセージは AP コンソールからログに記録されます。`*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 bug ID CSCse92856 によって発生します。 この問題は AP1130 と AP1240 にのみ適用されます。 この問題は AP1000s、AP1100、AP1200 には適用されません。この問題は、次の条件が満たされた場合にのみ発生します。HREAP モードが WLAN で使用されています。 この問題によりローカル モードは影響を受けません。 ネイティブ VLAN マッピングが必要です。AP は WLC の AP Manager 以外の異なる IP サブネットに存在する必要があります。プロキシ ARP は、AP のデフォルト ゲートウェイではディセーブルです。H-REAP AP は DHCP サーバからデフォルト ゲートウェイを受け取ります。この問題を解決するには、AP のデフォルト ゲートウェイ ルータでプロキシ ARP をイネーブルにします。

H-REAP モードの動作の確認

H-REAP が正しいコントローラに加入したら、いつでも H-REAP AP からコントローラに接続するかどうかを確認できます。 つまり、H-REAP AP が機能するモードを確認できます。 これは、AP CLI から **show lwapp reap status** コマンドを使用して確認できます。

AP_CLI#**show lwapp reap status**

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

この出力では、H-REAP AP が H-REAP モードおよび接続モードであることが示されています。つまり、AP とコントローラ間の WAN リンクは UP (接続済み) であり、動作モードは H-REAP です。

AP_CLI#**show lwapp reap status**

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

この出力には、AP がスタンドアロン モードであることが示されています。つまり、AP とコントローラ間の WAN リンクはダウンしています。 AP の動作モードは REAP です。 つまり、ローカル認証を使用するローカル スイッチングのために設定されている WLAN は機能し、この WLAN に新しいクライアントを許可します。 H-REAP のさまざまな動作モードについては、『H-REAP 動作モードの設定例』を参照してください。

H-REAP のコンソール コマンドが機能せずエラーが返される

H-REAP の CLI から設定コマンド (設定の適用またはクリア) を実行すると、「**ERROR!!!**

Command is disabled」というメッセージが返されます。 これは、次の 2 つのいずれかの理由により発生します。

- H-REAP AP が接続モード (コントローラに登録済み) の場合、設定をコンソールから実行したり、消去したりはできません。 AP がこの状態の場合、コントローラ インターフェイスから設定を行う必要があります。 AP で設定コマンドを利用する必要がある場合は、設定コマンドを入力する前に、AP がスタンドアロン モードであることを確認します。
- いずれかの時点で AP がコントローラに接続または加入したら、H-REAP のデフォルト イネーブル パスワード「Cisco」を必ず変更します。 このデフォルト パスワードを変更しないと、H-REAP がスタンドアロン モードに移行したときに、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 が接続しているコントローラの CLI からのみ設定できます。 このコマンド構文は、各 AP のコンソール パスワードまたはコントローラのすべての AP のパスワードを設定するために、コントローラで使用できます。 (WLC_CLI) **>config ap username <user-id> password <passwd> {all | <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**コンソール パスワードが設定されていない AP の場合は、コントローラでコマンドが入力された時点で初めて、この設定が AP に送信されます。 それ以降に WLC に加入した AP に対しては、コマンドを再度入力する必要があります。**注**次のコマンドは、デフォルト パスワードを変更していなくても、H-REAP で**すぐに**使用できます。**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 >***clear lwapp private-config**
- **注**アクセス ポイントを完全に工場出荷時のデフォルト状態に戻すには、AP のブート時に、イーサネット ライトがオレンジ色になるまで **Mode** ボタンを押し続けます。 1131 では、このライトは Mode ボタンの近くにあり、Ethernet と明記されています。 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 がインターフェイスに戻ります。これは、AP の IOS Recovery Image から利用可能です。 新しい設定コマンドを使用する場合は、AP で Cisco IOS® ソフトウェア リリース 12.3(11)JX1 以降が実行されている必要があることに注意してください。 この番号は、AP のコンソールに **show version** コマンドを出力すると確認できます。**注**すべての **show** コマンドと **debug** コマンドは、デフォルトのパスワードが設定されていなくても、また AP が接続モードになっていても、問題なく動作します。この時点で初めて LWAPP の設定が可能になります。

クライアントが H-REAP に接続できない

ワイヤレス クライアントが H-REAP に接続できない場合は、次の手順を実行します。

1. コントローラと H-REAP 間の WAN リンクが起動していることを確認します。
2. AP がコントローラに正しく加入していることと、コントローラに少なくとも 1 つの WLAN が正しく設定されてイネーブルになっていることを確認します。 ローカルでスイッチされる WLAN で、**H-REAP** がイネーブルになっていることを確認します。
3. WLAN が SSID をブロードキャストするようにコントローラで設定すると、このプロセスのトラブルシューティングに役立ちます。 クライアント側では、クライアントが SSID で AP を見つけることができるかどうかを確認します。 クライアントの WLAN の SSID 名とセキュリティ設定をミラーリングします。 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される WLAN のクライアントに IP アドレスが正しく設定されていることを確認します。 DHCP を使用している場合は、アップストリームの DHCP サーバが正しく設定されていて、クライアントにアドレスを提供することを確認します。 スタティック アドレスを使用している場合は、クライアントが正しいサブネットに適切に設定されていることを確認します。
5. すべての中間ファイアウォールで UDP ポート **12222** および **12223** が開放されていることを確認します。
6. H-REAP のコンソール ポートでさらにクライアント接続問題のトラブルシューティングを行うには、次のコマンドを発行します。`AP_CLI#show lwapp reap association`
7. クライアントの 802.11 接続の問題をデバッグするには、次のコマンドを発行します。`AP_CLI#debug dot11 state enable`
8. クライアントの 802.1X 認証プロセスとエラーをデバッグするには、次のコマンドを発行します。`AP_CLI#debug dot1x events enable`

H-REAP モードで、Wireless Control System（WCS）が AP に不正確なクライアント数をレポートする

ワイヤレス環境で Wireless Control System（WCS; ワイヤレス コントロール システム）を管理している場合、この WCS から H-REAP AP に、コントローラで指定されている正しいクライアント数ではなく、間違ったクライアント数がレポートされることがあります。

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。 H-REAP がコントローラでイネーブルになっている場合、WCS は多すぎるクライアント数をレポートします。 回避策は次のとおりです。

1. AP または任意のコントローラに関連付けられているクライアントの数を確認するには、**WCS Monitor > Clients** 機能を使用します。
2. 重複を防ぐため、AP またはコントローラで検索します（無線タイプによって制限されます）。
3. 検索された項目の合計数を正しいクライアント数として使用します。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 で解決されています。

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
- ハイブリッド REAP の設定
- H-REAP 動作モードの設定例
- WCS でのハイブリッド REAP の設定
- Lightweight アクセス ポイントに関する FAQ（英語）
- テクニカルサポートとドキュメント - Cisco Systems