# H-REAP 動作モードの設定例

# 内容

概要 前提条件 要件 使用するコンポーネント 表記法 背景説明 H-REAP により REAP の欠点を解消 設定 <u>ネットワ</u>ーク図 コンフィギュレーション AP によるコントローラのプライミングと H-REAP の設定 H-REAP の動作理論 <u>H-REAP のスイッ</u>チング状態 <u>中央認証、中央スイッチング</u> <u>中央認証、中央スイッ</u>チングの確認 認証停止、スイッチング停止 中央認証、ローカル スイッチング 中央認証、ローカル スイッチングの確認 認証停止、ローカル スイッチング ローカル認証、ローカル スイッチング <u>ローカル認証、ローカル スイッチングの確認</u> トラブルシュート 関連情報

## <u>概要</u>

このドキュメントでは、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)の概念を紹介し、そのさまざまな動作モードを設定例とともに説明しま す。

# <u>前提条件</u>

### <u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

・ワイヤレス LAN コントローラ(WLC)および WLC の基本パラメータの設定方法に関する知

• REAP に関する知識

#### <u>使用するコンポーネント</u>

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いています。

- •ファームウェア リリース 7.0.116.0 が稼働する Cisco 4400 シリーズ WLC
- Cisco 1131AG Lightweight アクセス ポイント(LAP)
- ・バージョン 12.4(11)T が稼動する Cisco 2800 シリーズのルータ
- •ファームウェア リリース 4.0 が稼働する Cisco Aironet 802.11a/b/g クライアント アダプタ
- Cisco Aironet Desktop Utility バージョン 4.0
- バージョン 4.0 が稼働している Cisco Secure ACS

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ました。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 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実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 は、ブランチ オフィスとリモート オフィスに導入されるワイヤレス ソリューションで す。H-REAP によって、ブランチ オフィスやリモート オフィスにある Access Point (AP; アクセ ス ポイント)を、各オフィスにコントローラを導入することなく、本部から WAN リンク経由で 設定して制御できます。

H-REAP では、コントローラへの接続が失われたときに、クライアント データ トラフィックを ローカルでスイッチして、クライアント認証をローカルで実行することができます。コントロー ラに接続されたときには、H-REAP はトラフィックをコントローラにトンネリングして戻すこと もできます。接続モードでは、Hybrid REAP(H-REAP)AP はローカル認証も実行できます。

H-REAP は以下でのみサポートされます。

- ・1130AG、1140、1240、1250、1260、AP801、AP 802、1040、および AP3550 AP
- Cisco 5500、4400、2100、2500、および Flex 7500 シリーズ コントローラ
- Catalyst 3750G Integrated Controller Switch
- Catalyst 6500 シリーズ Wireless Services Module (WiSM)
- Integrated Services Router (ISR; サービス統合型ルータ)用 Wireless LAN Controller Module (WLCM; ワイヤレス LAN コントローラ モジュール)

H-REAP のクライアント トラフィックは、AP でローカルでスイッチすることも、コントローラ にトンネリングして戻すこともできます。これは、WLAN の設定によって異なります。また、H-REAP 上のローカルでスイッチされたクライアント トラフィックに 802.1Q タグを付けることで 、有線側での分離を提供することもできます。WAN がダウンしている場合でも、ローカルでス イッチされてローカルで認証される WLAN 上のサービスは継続されます。

注:APがH-REAPモードで、リモートサイトでローカルにスイッチされる場合、RADIUSサーバ

設定に基づいて特定のVLANにユーザを動的に割り当てることはできません。ただし、AP でロー カルで行われるスタティック VLAN から Service Set Identifier(SSID)へのマッピングをベース とする特定の VLAN へのユーザの割り当ては可能です。そのため、特定の SSID に属しているユ ーザを、AP においてローカルで SSID がマップされる特定の VLAN に割り当てることができま す。

**注**: WLAN での音声の展開が重要である場合、H-REAP モードではサポートされない CCKM と Connection Admission Control(CAC; 接続アドミッション制御)サポートを AP が 取得して、 AP をローカル モードで稼動させる必要があります。

#### <u>H-REAP により REAP の欠点を解消</u>

REAP の詳細は、『<u>Lightweight AP とワイヤレス LAN コントローラ(WLC)での Remote-Edge</u> <u>AP(REAP)の設定例』を参照してください。</u>

H-REAP は、REAP に次の欠点があるために導入されました。

- REAP は有線側の分離を行いません。これは 802.1Q サポートがないためです。WLAN から のデータは同一の有線サブネット上で受信します。
- •WAN に障害が発生しているとき、REAP AP は、コントローラで指定された最初の WLAN 以 外のすべての WLAN 上で提供されるサービスを停止します。

H-REAP は、これらの2つの欠点に次の方法を使って対処します。

- dot1Q サポートと VLAN から SSID へのマッピングを提供します。この VLAN から SSID へのマッピング は、H-REAP で実行する必要があります。これを実行しているときには、設定された VLAN が中間のスイッチとルータのポートを正しく経由することを許可されている必要があります。
- ローカル スイッチング用に設定されたすべての WLAN に継続的なサービスを提供します。

### 設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

#### <u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



# <u>コンフィギュレーション</u>

この例では、コントローラが基本構成ですでに設定されていることを前提としています。コント ローラは次の構成を使用しています。

- 管理インターフェイス IP アドレス: 172.16.1.10/16
- AP マネージャ インターフェイス IP アドレス: 172.16.1.11/16
- デフォルト ゲートウェイ ルータ IP アドレス: 172.16.1.25/16
- バーチャル ゲートウェイ IP アドレス: 1.1.1.1

注:このドキュメントでは、H-REAPとコントローラの間で使用可能なルータとスイッチの WAN設定と設定については説明しません。これは、読者が WAN のカプセル化と使用されている ルーティング プロトコルを理解していることを前提としているためです。また、WAN リンクを 経由する H-REAP とコントローラの間の接続を維持するための、これらの設定方法を読者が理解 していることを前提としています。この例では、HDLC カプセル化が WAN リンクで使用されて います。

#### <u>AP によるコントローラのプライミングと H-REAP の設定</u>

CAPWAP 検出メカニズムが利用できないリモート ネットワークからコントローラを AP で検出 する場合、プライミングを利用できます。この方式で、AP を接続するコントローラを指定でき ます。

H-REAP 対応の AP のプライミングを行うには、AP を本社の有線ネットワークに接続します。 H-REAP 対応の AP は、ブートアップ時にそれ自体の IP アドレスを最初に検索します。DHCP サ ーバ経由で IP アドレスを取得すると、ブートアップして、登録プロセスを実行するコントローラ を検索します。

H-REAP AP は、『<u>ワイヤレス LAN コントローラ(WLC)への Lightweight AP(LAP)の登録</u>』 で説明されている方法のいずれかでコントローラの IP アドレスを学習できます。

**注**:APでCLIコマンドを使用してコントローラを検出するようにLAPを設定することもできます 。詳細は、「<u>CLI コマンドを使用した H-REAP コントローラの検出」を参照してください。</u>

このドキュメントの例では、H-REAP にコントローラの IP アドレスを学習させるために DHCP オプション 43 の手順を使用しています。そして、コントローラに加入し、最新のソフトウェア イメージと設定をコントローラからダウンロードして、無線リンクを初期化します。ダウンロー ドした設定は不揮発性メモリに保存されて、スタンドアロン モードで使用されます。

LAP がコントローラに登録されてから、次の手順を実行します。

- 1. コントローラの GUI で、[Wireless] > [Access Points] を選択します。このコントローラに登録された LAP が表示されます。
- 2. 設定する AP をクリックします。

CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS H	ÆLP .	EEEDBACK	Sale Cu
Wireless	All APs	ana 1997 ya 19		Ki (- 1666) (- 1666)	panel Party - Trea	າວີ ກ່ວວກວ່ຽກວ່າ.	5.566	1996 - 1993 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 - 1996 -	
Access Points     All APs     Padias	Current Filter		None		[Change Filter]	[Clear Filter]			
802.11a/n 802.11b/g/n Global Configuration	Number of APs		i						
► Advanced	AP Name	AP M	odel		P MAC	AP Up Time		Admin Status	Operationa Status
Mesh	AP001a.a219.ad44	AIR-L	AP1131AG-A-K9	·	0:1a:a2:19:ad:44	0 d, 00 h 06 m	n 12 s	Enabled	REG
▶ 802.11a/n ▶ 802.11b/g/n							6162.63		

3. [APs > Details] ウィンドウで [High Availability] タブをクリックし、AP が登録に使用するコントローラ名を定義してから [Apply] をクリックします。

iliilii cisco	MONITOR WLANS CONTROLLER WIREL	ESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK
Wireless * Access Points	All APs > Details for AP001a.a219.ad44	High Availability Inventory	Advanced
All APs Radios 802.11a/n 802.11b/g/n Global Configuration	Name Primary Controller WLC-4400	Nanagement IP Addr	255
<ul> <li>Advanced</li> <li>Mesh</li> <li>HREAP Groups</li> </ul>	Secondary Controller Tertiary Controller		
<ul> <li>B02.11a/n</li> <li>B02.11b/g/n</li> <li>Media Stream Country Timers</li> </ul>	AP Failover Priority Low		
▶ Qo5			
最大3台(プラ~	イマリ、セカンダリ、三次)の	コントローラ名を定義	iできます。 AP は、こ

取べる日(フライマラ、ビガラスラ、二次)のコラトローラ名を定義できます。 AF は、こ のウィンドウに指定した順序でコントローラを検索します。この例では、コントローラを1 台だけ使用しているので、そのコントローラをプライマリ コントローラとして定義してい ます。

 H-REAP 用に LAP を設定します。H-REAP モードで動作するように LAP を設定するには、 同じ [APs > Details] ウィンドウの [General] タブで、[AP mode] ドロップダウン メニューか ら [H-REAP] を選択します。これによって LAP が H-REAP モードで動作するように設定さ れます。

cisco	MONITOR WLANS CO	NTROLLER WIRELESS SECURITY	MANAGEMENT COMMAN	DS HELP EEEDBACK
Vireless Access Points All APs * Radios 902.11a/n 802.11a/n 802.11b/g/n Global Configuration Advanced Mesh HREAP Groups 802.11a/n 802.11b/g/n Media Stream Country Timers QQS	MONITOR WLANS CO General Credential AP Name Location AP MAC Address Base Radio MAC Admin Status AP Node AP Sub Mode Operational Status Port Number	APOOLER WIRELESS SECURITY	MANAGEMENT COMMAN Y Inventory Advan Versions Primary Software Versi Backup Software Versi Predownload Status Predownload Status Predownload Retry Con Boot Version IOS Version IOS Version Mini IOS Version IP Config IP Address Static IP Static IP	DS HELP EEEDBACK ced ion 7.0.116.0 on 0.0.0.0 None h None y Time NA 12.3.8.0 12.4(23c)JA2 3.0.51.0 10.78.177.28 [7] 172.10.110
			Netmask Gateway J DNS IP Address Domain Name	255.255.0.0 17.18.1.25 0.0.0.0

注:この例では、APのIPアドレスがスタティックモードに変更され、スタティックIPアドレス172.18.1.10が割り当てられていることがわかります。このように割り当てられているのは、これがリモートオフィスで使用するサブネットであるためです。そのため、DHCPサーバからの IP アドレスを使用するのは、登録段階の最初だけです。AP がコントローラに登録された後に、アドレスをスタティック IP アドレスに変更します。

これで LAP がコントローラをプライミングし、H-REAP モード用に設定されました。次の手順として、コントローラ側で H-REAP を設定し、H-REAP のスイッチング状態を検討します。

#### <u>H-REAP の動作理論</u>

きません。

H-REAP 対応の LAP は、次の 2 つのモードで動作します。

- 接続モード:H-REAP の WLC への CAPWAP コントロール プレーン リンクが動作中である 場合を、H-REAP が接続モードであるといいます。つまり、LAP と WLC の間の WAN リン クがダウンしていないことを意味します。
- スタンドアロン モード:H-REAP の WLC への WAN リンクがダウンしている場合を、H-REAP がスタンドアロン モードであるといいます。たとえば、H-REAP が WAN リンク経由 で接続された WLC への接続を失っている場合です。

クライアントを認証するために使用する認証メカニズムは、**中央**または**ローカル**として定義でき ます。

• 中央認証:リモート サイトからの WLC の処理を含む認証タイプのことです。

 ・ローカル認証:WLC からの認証の処理をまったく含まない認証タイプのことです。
 注:LAPがどのモードであっても、H-REAPですべての802.11認証およびアソシエーション処理 が行われます。接続モードの場合、H-REAP は WLC にこれらのアソシエーションと認証のプロ キシを設定します。スタンドアロン モードの場合、LAP はそのようなイベントを WLC に通知で

クライアントが H-REAP AP に接続すると、AP はすべての認証メッセージをコントローラに転送 します。正常な認証の後、そのデータ パケットはローカルでスイッチされるかコントローラにト ンネリングして戻されます。これは、接続されている WLAN の設定に従って変わります。

H-REAP では、コントローラに設定された WLAN は次の 2 つのモードで動作できます。

- ・中央スイッチング: H-REAP の WLAN は、その WLAN のデータ トラフィックを WLC にトンネリングされるように設定した場合、中央スイッチング モードで動作するといいます。
- ・ローカル スイッチング: H-REAP の WLAN は、その WLAN のデータ トラフィックが、 WLC にトンネリングされることなく、LAP 自体の有線インターフェイスにおいてローカルで 終端する場合、ローカル スイッチング モードで動作するといいます。注: H-REAPローカル スイッチングに設定できるのはWLAN 1 ~ 8だけです。これは、H-REAP機能をサポートする 1130、1240、および1250シリーズのAPに適用できるのは、これらのWLANだけです。

# H-REAP のスイッチング状態

前述のセクションで説明した認証とスイッチング モードを組み合わせると、H-REAP は次のいず れかの状態で動作します。

- <u>中央認証、中央スイッチング</u>
- <u>認証停止、スイッチング停止</u>
- <u>中央認証、ローカル スイッチング</u>
- •認証停止、ローカルスイッチング
- <u>ローカル認証、ローカル スイッチング</u>

#### <u>中央認証、中央スイッチング</u>

この状態では、WLAN に対して、AP がすべてのクライアント認証要求をコントローラに転送し

、すべてのクライアント データを WLC にトンネリングします。この状態は、H-REAP が接続モ ードであるときにのみ有効です。このモードで動作するように設定されている WLAN は、認証方 式が何であろうと、WAN 停止時には失われます。

この例では、次の設定を使用します。

- WLAN/SSID 名: Central
- [Layer 2 Security] : WPA2
- H-REAP ローカル スイッチング:無効

GUIを使って中央認証、中央スイッチング用に WLC を設定するには、次の手順を実行します。

1. [WLANs] をクリックして、**central** という名前の新しい WLAN を作成してから、[Apply] を クリックします。

cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
WLANs	WLANs > New								
<ul> <li>WLANs WLANs</li> <li>Advanced</li> </ul>	Type Profile Name SSID ID	Centr Centr	। र al र						

2. この WLAN は中央認証を使用しているので、[Layer 2 Security] フィールドで [WPA2] 認証 を使用します。WPA2 は WLAN のデフォルトのレイヤ 2 セキュリティです。

WLANS	General Security QoS Advanced
Advanced	Profile Name Central
	SSID Central
	Status Finabled
	Radio Policy All  Interface/Interface Group(G) management
	Multicast Vlan Feature  Enabled
	Broadcast SSID 🛛 🕅 Enabled

3. [AAA Servers] タブを選択し、認証用に設定された適切なサーバを選択します。

cisco	MONITOR WLANS CONTROLLER WIRELESS	SECURITY MANAGEMENT COM	MANDS HELP FEEDBACK
WLANS WLANS WLANS Advanced	WLANS > Edit 'Central'  General Security QoS Advanced Layer 2 Layer 3 AAA Servers Select AAA servers below to override use of de Radius Servers Radius Server Overwrite interface Enabled Authenticate Server 1 Server 2 Server 3 Local EAP Authentication Local EAP Authentication Local EAP Authentication Enabled Authentication Enabled Authentication priority order for web-auth user	efault servers on this WLAN tion Servers Accounting Servers Enabled None = 1. Port1012 = None =	LDAP Servers Server 1 None • Server 2 None • Server 3 None •

4. この WLAN は中央スイッチングを使用しているため、[H-REAP Local Switching] チェック ボックスがオフになっている([Local Switching] チェック ボックスが選択されていない)こ とを確認してください。 次に、[Apply] をクリックします。

/LANS	WLANs > Edit 'Central'	
<ul> <li>WLANS WLANS</li> <li>Advanced</li> </ul>	General       Security       QoS       Advanced         Diagnostic Channel       Enabled       Enabled         IPv6 Enable 2       Image: Channel interface ACL       None Image: Channel interface ACL       None Image: Channel interface ACL         P2P Blocking Action       Disabled       Image: Channel interface ACL       None Image: Channel interface ACL       None Image: Channel interface ACL         Cliant Exclusion 2       Image: Channel interface ACL       None Image: Channel interface ACL       Image: Channel interface ACL         Cliant Exclusion 2       Image: Channel interface ACL       None Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL         Maximum Allowed Clients 1       Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL         Static IP Tunneling Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL         Static IP Tunneling Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL         Static IP Tunneling Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL         Static IP Tunneling Image: Channel interface ACL       Image: Channel interface ACL       Image: Channel interface ACL         Static IP	MFP Client Protection # Optionel • DTIM Period (in beacon intervals) 802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 NAC NAC State None • Load Balancing • Client Load Balancing •
	Scan Defer Time 100 (msecs) HREAP H-REAP Local Switching T Enabled H-REAP Local Auth T Enabled Learn Client IP Address T Enabled	Voice Media Session Snooping 🔲 Enabled Re-anchor Roamed Voice Clients 🗖 Enabled

### <u>中央認証、中央スイッチングの確認</u>

次のステップを実行します。

- 1. ワイヤレス クライアントを同じ SSID およびセキュリティ設定で設定します。この例で、 SSID は *Central であり、セキュリティ方式は WPA2* です。
- 2. [RADIUS server] > [User Setup] で設定されているユーザ名とパスワードを入力して、クラ イアントの central SSID をアクティブにします。この例では、ユーザ名とパスワードに *User1 を使用しています。*

Enter Wireless N	etwork Password	×
Please enter your E network	AP-FAST username and password to log on to the wireless	
User Name :	User1	
Password :	•••••	
Log on to :		
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter	
Profile Name :	WPA-Enterprise	
	OK Cancel	000200000000000000000000000000000000000

は、RADIUS サーバによって中央で認証され、H-REAP AP に関連付けられます。これで、 H-REAP は、**中央認証、中央スイッチング**になります。

Cisco Airor	et Desktop Utility	y - Current Profile:	WPA2-Enterprise	? 🔀
Action Options	<u>H</u> elp			
Current Status CISCO SYSTE	Profile Management	Diagnostics		
Iltut	III. Profile Name:	central		
	Link Status:	Authenticated	Network Type: Infrastructur	e
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server I	Based Authentication:	EAP-FAST	Data Encryption: AES	
	IP Address:	fe80::240:96ff:feac		
	Signal Strength:		Good	
			Advanced	

## <u>認証停止、スイッチング停止</u>

「<u>中央認証、中央スイッチング」セクションで説明したのと同じ設定で、コントローラに接続する WAN リンクをディセーブルにします。</u>これで、コントローラは AP からのハートビートの応答を待ちます。ハートビートの応答は、キープアライブ メッセージと同様のものです。コントローラは 1 秒に 1 回、連続したハートビートを 5 回試行します。

WLC は、H-REAP からのハートビート応答を受信しないので、LAP の登録を解除します。

WLC の CLI から debug capwap events enable コマンドを発行して、登録解除処理を確認します 。次に示すのは、この debug コマンドの出力例です。

Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Did not receive heartbeat reply from AP 00:15:c7:ab:55:90 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 0! Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 0 Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00: 15:c7:ab:55:90 slot 1! Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15: c7:ab:55:90 slot 1

H-REAP はスタンドアロン モードになります。

この WLAN は以前に中央で認証され、中央でスイッチされたので、制御とデータ トラフィック はコントローラにトンネリングして戻されました。そのため、コントローラがないと、クライア ントは H-REAP とのアソシエーションを維持することができず、接続解除されます。クライアン ト アソシエーションと認証が両方ともダウンしているこの H-REAP の状態を、認証停止、スイ ッチング停止といいます。

#### 中央認証、ローカル スイッチング

この状態では、WLAN に対して、WLC がすべてのクライアント認証を処理し、H-REAP LAP が データ パケットをローカルでスイッチします。クライアントの認証が成功した後、コントローラ は capwap コントロール コマンドを H-REAP に送信して、その特定のクライアントのデータ パ ケットをローカルでスイッチするように LAP に指示します。このメッセージは、認証が成功する たびにそのクライアントに送信されます。この状態は接続モードの場合にのみ適用されます。

この例では、次の設定を使用します。

- WLAN/SSID 名: Central-Local
- [Layer 2 Security] : WPA2.
- H-REAP ローカル スイッチング:有効

コントローラの GUI から、次の手順を実行します。

- 1. [WLANs] をクリックして、central-local という名前の新しい WLAN を作成してから、 [Apply] をクリックします。
- 2. この WLAN は中央認証を使用しているので、[Layer 2 Security] フィールドで [WPA2] **認証** を選択します。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBAC	к
WLANs	WLANs > Edit 'Central-Local'	
WLANS WLANS	General Security Qo5 Advanced	_
Advanced	Profile Name Central-Local Type WLAN SSID Central-Local Status Free Enabled	
	Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy     All       Interface/Interface Group(G)     management       Multicast Vlan Feature     Enabled       Broadcast SSID     Imagement	

3. [Radius Servers] セクションの下で、認証用に設定された適切なサーバを選択します。

LANS	WLANS > E	dit Centra	al-Local'					
WLANS	General	Security	QoS /	Advanced				
Advanced	Layer 2	Layer 3	AAA Ser	vers				
	Authentication Servers Accounting Servers						ers Server	2 None •
	Server 1			None None -				5 Indie
	Server	2		None IP:172.16.1	1, Port: 1812	None 💌		
	Server 3 None None							
	Local EAP Authentication							
	Local E							
	Authenti	ication prior	rity order fo	DI <sup>r</sup>				

4. [H-REAP Local Switching] チェック ボックスにチェックマークを入れて、この WLAN に属 しているクライアント トラフィックが H-REAP においてローカルでスイッチするようにし ます。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMEN	IT COMMANDS HELP EEEDBACK
WLANS WLANS WLANS Advanced	WLANS > Edit "Central-Local"         General Security QoS Advanced         Diagnostic Channel       Enabled         IPv6 Enable Z       Imabled         Override Interface ACL       None         P2P Blocking Action       Disabled         Client Exclusion Z       Imabled         Client Exclusion Z       Enabled         Static IP Tunneling 42       Enabled         Diff Channel Scanning Defer       Imabled         Scan Defer Priority       0       1       2       4       5       7         Scan Defer Time (meses)       100       Imabled       Imabled       Imabled       Imabled         HREAP       Local Switching R       Enabled       Imabled       Imabled       Imabled	MFP Client Protection 4 Optional  DTIM Period (in beacon intervals)  802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1 NAC NAC State None Load Balancing and Band Select Client Load Balancing Client Band Select  Voice Media Session Snooping Enabled Re-anchor Roamed Voice Clients Enabled

### <u>中央認証、ローカル スイッチングの確認</u>

次のステップを実行します。

- 1. ワイヤレス クライアントを同じ SSID およびセキュリティ設定で設定します。この例で、 SSID は *Central-Local であり、セキュリティ方式は WPA2* です。
- 2. [RADIUS server] > [User Setup] で設定されているユーザ名とパスワードを入力して、クラ イアントの central-local SSID をアクティブにします。この例では、ユーザ名とパスワード に User1 を使用しています。

Enter Wireless N	etwork Password 🗙 🗙
Please enter your E. network	AP-FAST username and password to log on to the wireless
User Name :	User1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name :	WPA-Enterprise
	OK Cancel

3. [OK] をクリックします。クライアントは、RADIUS サーバによって中央で認証され、H-REAP AP に関連付けられます。これで、H-REAP は、**中央認証、ローカル スイッチング**に

on Options	Help		
urrent Status	Profile Management	Diagnostics	
CISCO SYSTE	M S In Profile Name:	central-local	
	Link Status:	Authenticated	Network Type: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server E	ased Authentication:	EAP-FAST	Data Encryption: AES
	IP Address:	fe80::240:96ff;feac	
	Signal Strength:		Good

### <u>認証停止、ローカル スイッチング</u>

ローカルでスイッチされる WLAN が、WLC で処理される必要がある認証タイプ(EAP 認証(ダ イナミック WEP/WPA/WPA2/802.11i)、WebAuth、NAC など)用に設定されている場合、 WAN で障害が発生すると、**認証停止、ローカル スイッチング状態になります。**この状態では、 WLAN に対して、H-REAP は、認証を試みる新しいクライアントを拒否します。ただし、H-REAP は、既存のクライアントが適切に接続を保つように、ビーコンとプローブ応答の送信は続 行します。この状態は、スタンドアロン モードの場合にのみ有効です。

この状態を確認するため、「<u>中央認証、ローカル スイッチング」セクションで説明されているも</u> のと同じ設定を使用します。

WLC に接続している WAN リンクがダウンしている場合、WLC は H-REAP の登録を解除する処理を実行します。

登録が解除されると、H-REAP はスタンドアロン モードになります。

この WLAN 経由で関連付けられるクライアントは、引き続き接続を維持します。ただし、オーセンティケータであるコントローラが利用可能ではないため、H-REAP はこの WLAN からの新しい 接続を許可しません。

これは、同じ WLAN にある別のワイヤレス クライアントのアクティベーションによって確認で きます。このクライアントの認証が失敗し、クライアントが関連付けを許可されないことを確認 できます。

**注:**WLANクライアントの数が0になると、H-REAPは関連するすべての802.11機能を停止し、指 定されたSSIDのビーコンを発行しなくなります。これによって、WLAN は、次の H-REAP 状態 である、**認証停止、スイッチング停止**に移行します。

#### <u>ローカル認証、ローカル スイッチング</u>

この状態で、H-REAP LAP はクライアント認証を処理して、データ パケットをローカルでスイッチします。この状態は、スタンドアロン モードの場合で、かつ AP においてローカルで処理できる認証タイプに対してのみ有効であり、コントローラの処理は含みません。

以前、中央認証、ローカル スイッチング状態であった H-REAP は、設定された認証タイプが AP においてローカルで処理できる場合は、この状態に移行します。802.1x 認証などのように、設定 された認証がローカルで処理できない場合、スタンドアロン モードのときには H-REAP は認証 停止、ローカル スイッチング モードになります。

次に示すのは、スタンドアロン モードの AP においてローカルで処理できる一般的な認証メカニ ズムです。

- •開く
- 共有
- WPA-PSK
- WPA2-PSK

注:APが接続モードの場合、すべての認証プロセスがWLCによって処理されます。H-REAP が スタンドアロン モードであるとき、オープン、共有、WPA/WPA2-PSK 認証は、すべてのクライ アント認証が発生する LAP に転送されます。

**注:WLAN上で**ローカルスイッチングが有効になっているHybrid-REAPを使用している場合、外 部Web認証はサポートされません。

この例では、次の設定を使用します。

- WLAN/SSID 名:Local
- [Layer 2 Security] : WPA-PSK
- H-REAP ローカル スイッチング: enabled

コントローラの GUI から、次の手順を実行します。

- 1. [WLANs] をクリックして、Local という名前の新しい WLAN を作成してから、[Apply] をク リックします。
- 2. この WLAN はローカル認証を使用するため、[Layer 2 Security] フィールドで [WPA-PSK] か またはローカルで処理可能な前述のいずれかのセキュリティ メカニズムを選択します。 の例では WPA-PSK を使用しています。

cisco	MONITOR WLANS CON	TROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	нецр
WLANs	WLANs > Edit 'Local'	and the second secon	Sugap Contractor	Manage 7 Star	KUNGRO - BEN	S. BARRAN, C.
WLANS	General Security	QoS Advanced				
Advanced	Layer 2 Layer 3	AAA Servers				
	Layer 2 Security 2 V WPA+WPA2 Parameter	MPA+WPA2  Add MAC Filtering s				٦
	WPA Policy					
	WPA2 Policy	V				
	WPA2 Encryption	R AES TKIP	н::			
	Auth Key Mgmt	PSK 🔹				
	PSK Format	ASCII .				
		•••••				

- 3. 選択を行うと、使用する事前共有鍵/パス フレーズを設定する必要があります。これは、認 証を成功させるためにクライアント側と同じにする必要があります。
- 4. [H-REAP Local Switching] チェック ボックスにチェックマークを入れて、この WLAN に属 しているクライアント トラフィックが H-REAP においてローカルでスイッチするようにし ます。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMEN	IT COMMANDS HELP
WLANS WLANS Advanced	WLANS > Edit 'Local'         General Security QoS Advanced         Diagnostic Channel       Enabled         IPv6 Enable Z       Image: Channel	MFP Client Protect DTIM Period (in be 802.11a/n (1 - 25 802.11b/g/n (1 - 3 NAC NAC State None Load Balancing and Client Load Balanci
	Scan Defer Time (msecs) HREAP H-REAP Local Switching 2 IV Enabled H-REAP Local Auth 22 IV Enabled Learn Client IP Address 2 IV Enabled	Voice Media Session Sno Re-anchor Roame

## <u>ローカル認証、ローカル スイッチングの確認</u>

次のステップを実行します。

1. クライアントを同じ SSID とセキュリティ設定で設定します。ここで、SSID は Local であ

り、セキュリティ方式は WPA-PSK です。

- クライアントで Local SSID をアクティブにします。クライアントはコントローラにおいて 中央で認証され、H-REAP と関連付けられます。クライアント トラフィックはローカルで スイッチされるように設定されます。これで、H-REAP は、中央認証、ローカル スイッチ ングの状態になりました。
- コントローラに接続する WAN リンクをディセーブルにします。いつものように、コントロ ーラは登録除外処理を実行します。H-REAP はコントローラから登録を解除されます。登録 が解除されると、H-REAP はスタンドアロン モードになります。ただし、この WLAN に属 しているクライアントは、引き続き H-REAP とのアソシエーションを維持します。また、 ここでの認証タイプはコントローラなしで AP においてローカルで処理できるので、H-REAP はこの WLAN 経由で新しいワイヤレス クライアントからのアソシエーションを許可 します。
- 4. これを確認するには、同じ WLAN で他のワイヤレス クライアントをアクティブにします。
   クライアントが正常に認証され、関連付けられることを確認できます。

# <u>トラブルシュート</u>

- 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、次のコマンドを入力します。
   AP\_CLI#show capwap reap association
- コントローラ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い、さらに、デバッグの出力を制限するには、次のコマンドを入力します。
   AP\_CLI#debug mac addr
- クライアントの 802.11 接続の問題をデバッグするには、次のコマンドを使用します。
   AP\_CLI#debug dot11 state enable
- クライアントの 802.1X 認証処理およびその障害をデバッグするには、次のコマンドを使用します。
   AP\_CLI#debug dot1x events enable
- バックエンドコントローラ/RADIUSのメッセージをデバッグするには、次のコマンドを使用します。

AP\_CLI#debug aaa events enable

また、クライアント debug コマンドの完全なセットを有効にするには、次のコマンドを使用します。

AP\_CLI#debug client



- ・ ワイヤレス LAN コントローラと Lightweight アクセスポイントの基本設定例
- ・
   <u>無線 LAN コントローラでの VLAN の設定例</u>
- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0
- Hybrid REAP の設計および導入ガイド
- <u>Hybrid Remote Edge Access Point (H-REAP)の基本的なトラブルシューティング</u>

- ・Lightweight アクセス ポイントの WLAN コントローラ フェールオーバーの設定例
- ・<u>ワイヤレス製品に関するサポート</u>
- ・ テクニカル サポートとドキュメント – Cisco Systems