ブランチオフィスでの REAP 導入ガイド

内容

概要

このドキュメントでは、リモート エッジ アクセス ポイント（REAP）を展開する場合に考慮する必要のある情報について説明します。 基本的な REAP 設定情報については、『Remote-Edge AP (REAP) with Lightweight APs and Wireless LAN Controllers (WLCs) Configuration Example』を参照してください。

注：REAP機能はWLCリリース3.2.215までサポートされています。WLCリリース4.0.155.5から、この機能は7.0.x.xまでわずかな機能拡張を含むHybrid REAP(H-REAP)と呼ばれます。7.2.103リリースから、この機能は FlexConnect と呼ばれます。

Cisco IOS® ソフトウェア リリース 12.3(7)JX 以降を実行する 1010、1020、1100 および 1200 シリーズ AP などの従来の Cisco Lightweight アクセス ポイント プロトコル（LWAPP）ベースのアクセス ポイント（AP）（別名 LAP）は、シスコのワイヤレス LAN コントローラ（WLC）を介

して中央管理および制御できます。 また、これらの LAP はワイヤレス データ集約の単一ポイントとしてコントローラを管理者が使用できるようにします。

これらの LAP はコントローラが QoS やアクセス コントロール リスト（ACL）の適用などの拡張機能を実行することを可能にしますが、すべてのワイヤレス クライアント トラフィックの入出力の単一ポイントとなるコントローラの要件は、ユーザのニーズを満たすのではなく、むしろ妨げる可能性があります。リモート オフィスなどの環境によっては、コントローラですべてのユーザ データを終端することは、特に WAN リンク経由で使用できるスループットが限られている場合に帯域幅の負荷がかかり過ぎる可能性があります。また、LAP と WLC 間のリンクが停止する傾向がある場合は、リモート オフィスへの WAN リンクと同じように、ユーザ データの終端のために WLC に依存する LAP を使用することによって、WAN の停止時にワイヤレス接続が切断される可能性があります。

代わりに、動的な構成管理、AP ソフトウェア アップグレード、およびワイヤレス侵入検知などのタスクを実行するために従来の LWAPP のコントロール プレーンを利用する AP アーキテクチャを使用できます。これによって、ワイヤレス データをローカルのまま保持する、ワイヤレス インフラストラクチャを集中的に管理する、WAN の停止時に回復できるようにすることが可能になります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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。

1030 REAP アーキテクチャの概要

Cisco 1030 REAP はリモート機能を提供するために、LWAPP のコントロール プレーンとワイヤレス データ プレーンを切り離しています。通常の LAP と同様に中央集中型の制御と管理のために、Cisco WLC を引き続き使用しています。違いは、すべてのユーザ データが AP でローカルにブリッジされていることです。ローカル ネットワーク リソースへのアクセスは、WAN が停止していても維持されます。図 1 は、基本的な REAP アーキテクチャを示します。

図 1：基本的な REAP アーキテクチャ図

注：従来のLAPとのREAP機能の基本的な相違点のリストについては、付録Aを参照してください。

どのような場合に REAP AP を使用するか

Cisco 1030 REAP AP は、主に次の 2 つの条件の下で使用する必要があります。

- LAP と WLC 間のリンクが停止する傾向がある場合は、リンクの障害発生時にワイヤレス ユーザが中断なくデータにアクセスできるように、1030 REAP を使用できます。
- AP の有線ポートで（他のすべての LAP のデータと同じように、コントローラで終端するのではなく）すべてのユーザ データをローカルに終端する必要がある場合は、コントローラ インターフェイスまたは Wireless Control System（WCS）によって中央制御を可能にするため、1030 REAP を使用できます。 これにより、データはローカルのままになります。

カバレッジまたはユーザの密度のため、1 つのサイトで 2 個または 3 個以上の 1030 REAP AP が必要な場合は、2006 または 2106 WLC の展開を検討します。これらのコントローラは、あらゆるタイプの最大 6 個の LAP をサポートできます。これは、より経済的で REAP のみの展開と比較して豊富な機能が提供される可能性があります。

すべての 1000 シリーズ AP と同様、単一の 1030 AP は約 5,000 平方フィートをカバーします。これは、各サイトの無線周波（RF）の伝播特性、およびワイヤレス ユーザとそのスループットのニーズのために必要な数によって異なります。最も一般的な展開では、単一の 1000 シリーズ AP は、802.11b では 512 kBps で 12 人のユーザ、802.11a では 2 MbPS で 12 人のユーザを同時にサポートできます。すべての 802.11 ベースのテクノロジーと同様に、メディア アクセスは共有されます。したがって、より多くのユーザがワイヤレス AP に接続すると、スループットがそれに応じて共有されます。繰り返しになりますが、ユーザの密度の増加やスループット要件の上昇に従って、ユーザあたりのコストを節約して機能を拡張するためにローカル WLC の追加を検討してください。

注：1030 REAPは、他のLAPと同様に動作するように設定できます。したがって、リモート サイトの WLAN インフラストラクチャのサイズを拡張するために WLC を追加しても、既存の REAP への投資を引き続き活用できます。

REAP の導入

1030 REAP は WLC インフラストラクチャから離れたリモート サイトに配置されるように設計されているため、コントローラを検出して接続するために LAP が使用する従来のゼロタッチ方式（DHCP オプション 43 のような）は通常採用されません。代わりに、1030 が中央サイトの WLC に接続できるように、LAP を最初にプライミングする必要があります。

プライミングとは、自分が接続できる WLC のリストを LAP に提供する処理のことです。単一の WLC に接続すると、LAP にはモビリティ グループのすべてのコントローラが通知され、グループ内のコントローラに接続するために必要なすべての情報が提供されます。モビリティ グループ、ロード バランシング、コントローラの冗長性の詳細については、『Cisco 440X シリーズ ワイヤレス LAN コントローラの配備』を参照してください。

ネットワーク オペレーション センター（NOC）またはデータセンターのような中央サイトでこれを実行するには、REAP が有線ネットワークに接続されている必要があります。これにより、REAP は単一の WLC を検出できます。コントローラに一度接続すると、LAP は WLAN インフラストラクチャに対応する LAP OS バージョンをダウンロードします。その後、モビリティ グループ内のすべての WLC の IP アドレスが AP に転送されます。これにより、リモート サイトで電源が投入されると、IP 接続が使用可能であれば、AP はリストから最も使用率の低いコントローラ

を検出して接続できるようになります。

注：DHCPオプション43とドメインネームシステム(DNS)ルックアップは、REAPでも動作します。AP がセントラル コントローラを見つけられるようにリモート サイトで DHCP または DNS を設定する方法の詳細は、『Cisco 440X シリーズ ワイヤレス LAN コントローラの配備』を参照してください。

この時点で、必要に応じて 1030 にスタティック アドレスを指定できます。これは、IP アドレッシング方式が宛先のリモート サイトと一致することを確実にします。また、各 LAP が接続を試みる 3 台のコントローラについて説明するため WLC の名前を入力することができます。この 3 台への接続に失敗すると、LWAPP の自動ロード バランシング機能によって LAP はクラスタ内の残りのコントローラのリストから最も負荷が少ない AP を選択します。LAP 設定の編集は、WLC のコマンドライン インターフェイス（CLI）または GUI、あるいはより簡単な WCS を介して行います。

注：1030 REAPは、接続するWLCがレイヤ3 LWAPPモードで動作する必要があります。これは、コントローラに IP アドレスを割り当てる必要があることを意味します。また、WLC は各リモート サイトで DHCP サーバが使用可能であるか、またはプライミング プロセス中にスタティック アドレスが割り当てられていることを必要とします。コントローラに組み込まれている DHCP 機能は、1030 LAP またはユーザにアドレスを提供するために使用できません。

リモート サイトに出荷するために 1030 LAP の電源をオフにする前に、各 1030 が REAP モードに設定されていることを確認します。すべての LAP のデフォルトは通常のローカル機能を実行することですが、1030 は REAP 機能を実行するために設定する必要があるため、これは非常に重要です。これは、コントローラの CLI または GUI を使用して LAP レベルで実行するか、より簡単に WCS テンプレートを使用して実行できます。

基本的な REAP プライミング機能

リモート サイトに配置された REAP が接続する、モビリティ グループ内の WLC に 1030 REAP が接続すると、次の情報が提供されます。

必要な REAP 設定

- モビリティ グループ内の WLC の IP アドレスのリスト（controller/AP の接続時に自動的に提供されます）
- REAP AP モード（REAP 機能を実行するには、AP を REAP モードで動作するように設定する必要があります）

オプションの REAP 設定

- スタティック IP アドレス（AP ごとに入力するオプション設定）
- プライマリ、セカンダリ、ターシャリ WLC の名前（AP ごとに、または WCS テンプレートを使用して入力するオプション設定）
- AP の名前（AP ごとに入力するオプションの情報設定）
- AP の ロケーション情報（AP ごとに、または WCS テンプレートを使用して入力するオプションの情報設定）

REAP-to-Controller リンク要件

REAP の展開を計画する際には、いくつかの基本要件を覚えておく必要があります。これらの要件は、REAP LWAPP 制御トラフィックが通過する WAN リンクの速度と遅延にかかわります。1030 LAP は、IP セキュリティ トンネル、フレーム リレー、DSL（非 PPPoE）および専用回線などの WAN リンク上で使用されることを意図しています。

注：1030 REAP LWAPPの実装では、APとWLC間の1500バイトのMTUパスが想定されています。1500 バイト以下の MTU によって移行中に発生するフラグメンテーションは、予期しない結果をもたらします。したがって、1030 LAP はルータが予防的に 1500 バイト以下にパケットをフラグメント化する PPPoE などの環境に適していません。

すべての 1030 LAP はデフォルトで、ハートビート メッセージを 30 秒ごとにコントローラに返信するため、WAN リンクの遅延は特に重要です。ハートビート メッセージが失われると、LAP は 1 秒ごとに 5 回の連続的なハートビートを送信します。すべて失敗すると、LAP はコントローラの接続が切断されたと判断し、1030 はスタンドアロン REAP モードに戻ります。1030 LAP は WLC との間の大きな遅延を許容できますが、LAP とコントローラ間の遅延が 100 ミリ秒を超えないようにする必要があります。これは、認証に失敗したと判断する前に待機する時間を制限するクライアント側のタイマーによるものです。

REAP の制約

1030 AP は集中的に管理され、WAN リンクの停止時に WLAN サービスを提供するように設計されていますが、REAP が WLC 接続時に提供できるサービスと接続の切断時に提供できるサービスには違いがあります。

WLAN

1030 REAP では、それぞれ独自の Multiple Basic Service Set Identifier（MBSSID）がある、最大 16 の WLAN（すべてのセキュリティ、QoS、および他のポリシーとともに、それぞれ Service Set Identifier（SSID）を含むワイヤレス プロファイル）をサポートできます。ただし、コントローラとの接続が中断された場合、1030 REAP は最初の WLAN のみををサポートできます。WAN リンクが停止している間は、最初の WLAN 以外のすべての WLAN は使用できません。そのため、WLAN 1 はプライマリ WLAN を意味し、これに合わせたセキュリティ ポリシーを計画する必要があります。この最初の WLAN のセキュリティは WAN リンクで障害が発生すると、バックエンドの RADIUS 認証でも障害が発生するため、特に重要です。これは、このようなトラフィックが LWAPP コントローラのプレーンを通過するためです。したがって、すべてのユーザにワイヤレス アクセスが許可されません。

この最初の WLAN では、Wi-Fi Protected Access（WPA-PSK）の事前共有キー部分などのローカル認証/暗号化方式を使用することが推奨されます。WPA-PSK（またはWEP）を使用すると、WANリンクがダウンしても、適切に設定されたユーザがローカルネットワークリソースにアクセスできます。

注：**すべての**RADIUSベースのセキュリティ方式では、認証メッセージをLWAPPコントロールプレーン経由で中央サイトに送信する必要があります。したがって、すべての RADIUS ベースのサービスは WAN の停止中は利用できません。これには、RADIUS ベースの MAC 認証、802.1X、WPA、WPA2、および 802.11i が含まれますが、これらに限定されません。

1030 REAP は、802.1q VLAN タギングを実行できないため、単一のサブネットにしか存在できません。したがって、各 SSID のトラフィックは、有線ネットワークの同じサブネットで終端します。つまり、ワイヤレス トラフィックは SSID 間にまたがる伝送中にセグメント化されることがありますが、有線側でユーザ トラフィックが分割されることはありません。

セキュリティ

1030 REAP は、シスコのコントローラ ベースの WAN アーキテクチャでサポートされているすべてのレイヤ 2 のセキュリティ ポリシーを提供できます。これには、WEP、802.1X、WPA、WPA2、および 802.11i などすべてのレイヤ 2 認証と暗号化タイプが含まれます。前述したように、これらのセキュリティ ポリシーのほとんどは、バックエンドの認証のために WLC 接続を必要とします。WEP と WPA-PSK は、AP レベルで完全に実装されているため、バックエンドの RADIUS 認証を必要としません。このため、WAN リンクがダウンしても、ユーザは引き続き接続できます。Cisco WLC の提供するクライアント除外のリストの機能は、1030 LAP でサポートされています。コントローラへの接続が使用可能な場合は、MAC フィルタリングは 1030 で機能します。

注：APがスタンドアロンモードの場合、REAPはWPA2-PSKをサポートしません。

すべてのレイヤ 3 セキュリティ ポリシーは、1030 LAP で使用できません。これらのセキュリティ ポリシーには、コントローラで実行される Web 認証、コントローラ ベースの VPN の終端、ACL、およびピアツーピア ブロッキングが含まれます。VPN パススルーは、外部 VPN コンセントレータに接続するクライアントでは動作します。ただし、指定した VPN コンセントレータに宛てられたトラフィックだけを許可するコントローラの機能（VPN パススルーのみ）は動作しません。

ネットワーク アドレス変換（NAT）

REAP が接続する WLC は、NAT 境界の背後には存在できません。ただし、LWAPP（UDP ポート 12222 と 12223）に使用するポートが 1030 に転送されることを前提として、リモート サイトの REAP は NAT ボックスの背後に置くことができます。つまり、ポート フォワーディングが確実に動作するには各 REAP にスタティック アドレスが必要で、それぞれの NAT インスタンスの背後には 1 つの AP のみが存在できます。この理由は、NAT IP アドレスあたり 1 つのポート フォワーディング インスタンスのみが存在できることです。これは、リモート サイトの NAT サービスの背後で動作できるのは 1 つの LAP のみであることを意味します。1 対 1 の NAT は、それぞれの外部 IP アドレスの LWAPP ポートをそれぞれの内部 IP アドレス（スタティック REAP IP アドレス）に転送できるため、複数の REAP で動作可能です。

Quality of Service（QoS）

802.1p precedence ビットに基づいたパケットのプライオリティは、REAP が 802.1q タギングを実行できないため使用できません。これは Wi-Fi マルチメディア（WMM）と 802.11e はサポートされていないことを意味します。SSID に基づいたパケットのプライオリティと Identity Bases Networking はサポートされています。ただし、Identity-Based Networking 経由の VLAN 割り当ては、802.1q タギングを実行できないため REAP では動作しません。

ローミングとクライアントのロード バランシング

複数の REAP が存在し、AP 間のモビリティが必要な環境では、各 LAP が同じサブネット上にある必要があります。レイヤ 3 モビリティは、1030 LAP ではサポートされていません。通常、リモート オフィスはこのような柔軟性を必要とするほどの数の LAP を導入しないため、これは制限とはなりません。

アップストリーム コントローラ接続が使用できる場合は、アグレッシブ クライアント ロード バランシングはサイト内のすべての REAP にまたがって提供されます（ロード バランシングはホスト コントローラ上でのみ有効にすることができます）。

Radio Resource Management (RRM)

コントローラに接続できる場合、1030 LAP は WLC の RRM メカニズムからダイナミック チャネルと出力電力を受け取ります。WAN リンクがダウンすると、RRM は機能せず、チャネルと電力の設定は変更されません。

不正検出と IDS 機能

REAP アーキテクチャは通常の LAP と同様、すべての不正検出と侵入検知シグニチャ (IDS) をサポートします。ただし、セントラル コントローラとの接続が失われると、収集されたすべての情報が共有されなくなります。そのため、リモート サイトの RF ドメインが表示されなくなります。

REAP の制約の概要

「付録 B」の表は、通常の動作中の REAP の機能と WAN リンク全体における WLC への接続が使用できない場合の REAP の機能をまとめたものです。

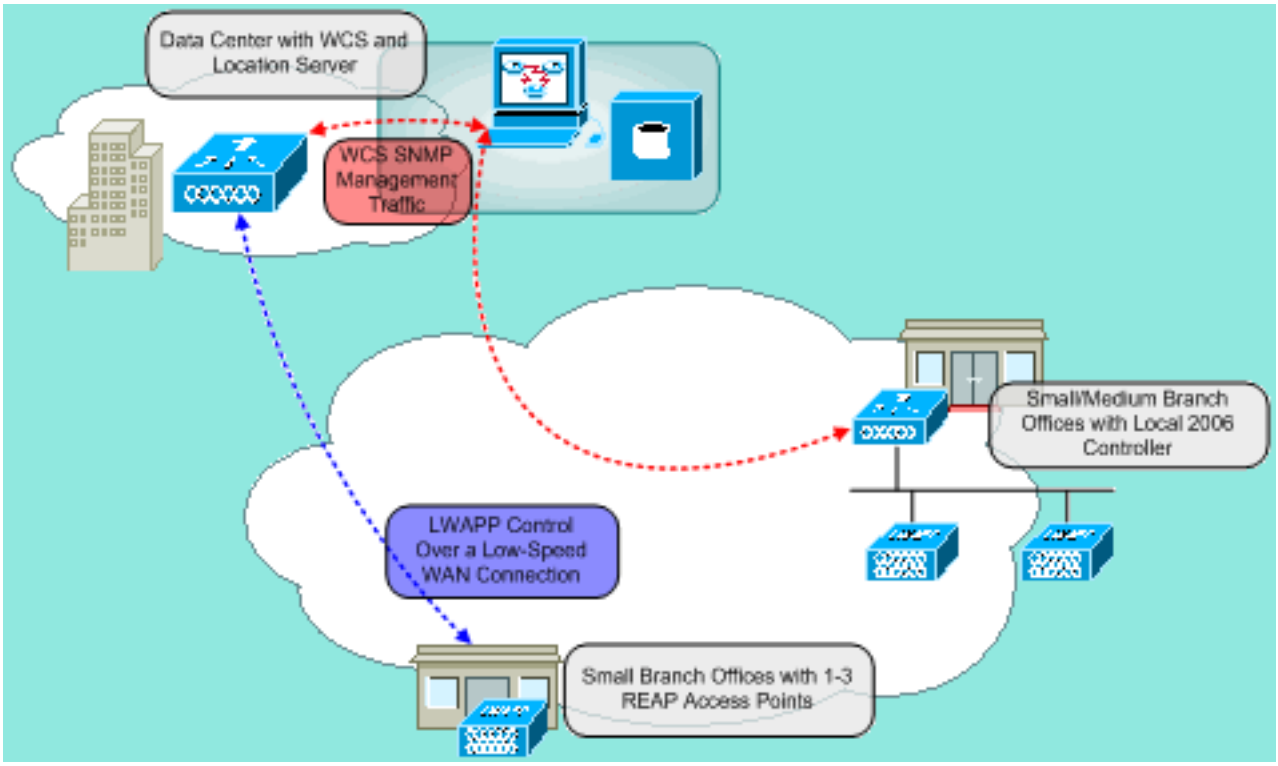
REAP と中央集中型 WLAN アーキテクチャの管理

1030 REAP の管理は、通常の LAP や WLC の管理と同じです。管理と設定はすべて、各コントローラの CLI または Web GUI を使用してコントローラ レベルで実行されます。システム全体の設定およびネットワーク可視性は、すべてのコントローラと AP (REAP またはその他) を単一のシステムとして管理できる WCS を介して提供されます。REAP とコントローラの接続が切断された場合、管理機能も中断されます。

REAP での中央集中型 WLAN アーキテクチャ

図 2 は、さまざまなワイヤレス ネットワーキングのニーズを満たすために、中央集中型の LWAPP アーキテクチャの各部分がどのように連携するかを示します。管理および口ケーション サービスは、WCS および 2700 Location Appliance によって中央で提供されます。

図 2 : REAP での中央集中型 WLAN アーキテクチャ



付録 A

REAP アーキテクチャと通常の LAP の主な相違点は何ですか

- DHCP オプション 43 または DNS 解決がリモート サイトで使用できない場合は、まずセントラル オフィスで 1030 をプライミングする必要があります。その後、宛先サイトに出荷します。
- WAN リンクの障害が発生すると、最初の WLAN のみがアクティブなままになります。RADIUS を必要とするセキュリティ ポリシーは失敗します。WPA-PSK を使用する認証/暗号化は、WLAN 1 に対して推奨されます。WEP は動作しますが、推奨されません。
- レイヤ 3 暗号化なし（レイヤ 2 暗号化のみ）
- REAP が接続する WLC は、NAT 境界の背後には存在できません。ただし、REAP はそれぞれの内部スタティック REAP IP アドレスに両方の LWAPP ポートを（12222 と 12223）が転送されている場合は可能です。**注**：LAPから発信されるLWAPPトラフィックの送信元ポートは時間の経過とともに変化する可能性があるため、オーバーロード付きポートアドレス変換(PAT)/NATはサポートされていません。これは、LWAPP アソシエーションを切断します。同じ問題は、PIX/ASA のように設定に応じてポート アドレスが変更される REAP の NAT の実装でも発生する可能性があります。
- LWAPP 制御メッセージのみが WAN リンクを通過します。
- データ トラフィックは、1030 のイーサネット ポートでブリッジされます。
- 1030 LAP は、802.1Q タギング（VLAN）を実行しません。 したがって、すべての SSID からの無ワイヤレス トラフィックは同じ有線サブネットで終端します。

付録 B

REAP のノーマル モードとスタンドアロン モード間の機能の相違点は何ですか

	REAP（ノーマ	REAP（スタン

		ル モード）	ドアロン モード）
プロトコル	IPv4	Yes	Yes
	IPv6	Yes	Yes
	他のすべてのプロトコル	はい（クライアントでも IP が有効な場合のみ）	はい（クライアントでも IP が有効な場合のみ）
	IP プロキシ ARP	No	No
WLAN	SSID の数	16	1（最初の 1 つ）
	ダイナミック チャネル割り当て（DCA）	Yes	No
	ダイナミック電力制御	Yes	No
	ダイナミック ロード バランシング	Yes	No
VLAN	複数のインターフェイス	No	No
	802.1Q のサポート	No	No
WLAN セキュリティ	不正 AP 検出	Yes	No
	除外リスト	Yes	はい（既存のメンバのみ）
	ピアツーピア ブロッキング	No	No
	侵入検知システム	Yes	No
レイヤ 2 セキュリティ	MAC 認証	Yes	No
	802.1X	Yes	No
	WEP（64/128/152 ビット）	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	Yes	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
レイヤ 3 セキュリティ	Web 認証	No	No
	IPSec	No	No
	L2TP	No	No
	VPN パススルー	No	No
	アクセス コントロール リス	No	No

	ト		
QoS	QoS プロファイル	Yes	Yes
	ダウンリンク QoS（重み付けラウンドロビン キュー）	Yes	Yes
	802.1p のサポート	No	No
	ユーザあたりの帯域幅コントラクト	No	No
	WMM	No	No
	802.11e（予定）	No	No
	AAA QoS プロファイルの上書き	Yes	No
モビリティ	サブネット内	Yes	Yes
	サブネット間	No	No
DHCP	内部 DHCP サーバ	No	No
	外部 DHCP サーバ	Yes	Yes
トポロジ	直接接続（2006）	No	No

関連情報

- Lightweight AP とワイヤレス LAN コントローラ（WLC）での Remote-Edge AP（REAP）の設定例
- Unified Wireless Network での AP ロード バランシングおよび AP フォールバック
- Cisco 440X シリーズ ワイヤレス LAN コントローラの配備
- 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
- テクニカル サポートとドキュメント – Cisco Systems