# 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

## 内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 背景説明 設定 ネットワーク図 WLC の基本動作用の設定と WLAN の設定 リモート サイトにインストールするための AP のプライミング WAN リンクを確立するための 2800 ルータの設定 リモート サイトでの REAP AP の配備 確認 トラブルシュート トラブルシューティングのためのコマンド 関連情報

## <u>概要</u>

Cisco Unified Wireless Network に導入された Remote-edge Access Point(REAP; リモートエッ ジアクセス ポイント)機能を使用すれば、ワイヤレス LAN(WLAN)コントローラ(WLC)か ら Cisco Lightweight アクセス ポイント(LAP)をリモート配備できます。 この機能は、ブラン チオフィスや小規模な小売サイトに最適です。このドキュメントでは、REAP ベースの WLAN ネ ットワークを Cisco 1030 シリーズの LAP や 4400 WLC を使用して配備する方法について説明し 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。

- •WLCに関する知識とWLCの基本的なパラメータの設定方法に関する知識
- Cisco 1030 LAP での REAP モードの動作に関する知識
- 外部 DHCP サーバおよび Domain Name System (DNS; ドメイン ネーム システム) サーバ

のどちらかまたは両方の設定に関する知識

• Wi-Fi Protected Access (WPA)の概念に関する知識

#### <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 4.2 が稼動する Cisco 4400 シリーズ WLC
- Cisco 1030 LAP
- Cisco IOS®ソフトウェアリリース12.2T13が稼働する2台のCisco 2800シリーズルータ
- ・ファームウェアリリース3.0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 3.0

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。

#### <u>表記法</u>

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。

### <u>背景説明</u>

REAP モードでは、WAN リンクを経由して LAP を配置し、WLC との通信を維持しながら、通常 の LAP 機能を利用できます。REAP モードは、現時点では 1030 LAP でしかサポートされていま せん。

この機能を実現するために、1030 REAP では、Lightweight Access Point Protocol(LWAPP)の コントロール プレーンが、ワイヤレス データ プレーンと分離されています。通常の LWAPP ベ ースのアクセス ポイント(AP)で使用されるのと同じ方法で中央集中型の制御と管理を行うた めに Cisco WLC が引き続き使用されていますが、すべてのユーザ データは AP でローカルにブ リッジされています。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。

REAP AP では、次の2つの動作モードがサポートされています。

• 通常の REAP モード

• スタンドアロン モード

REAP AP と WLC の間の WAN リンクがアップすると、LAP は通常の REAP モードに設定され ます。LAP が通常の REAP モードで動作している場合は、最大 16 個までの WLAN をサポートで きます。

WLC と LAP の間の WAN リンクがダウンすると、REAP が有効になっている LAP はスタンドア ロン モードに切り替わります。Wired Equivalent Privacy (WEP)または任意のローカル認証方 式を使用して WLAN が設定されている場合は、スタンドアロン モードでは、REAP LAP は WLC なしで WLAN を 1 つだけ単独でサポートできます。この場合、REAP AP がサポートする WLAN は、AP に設定されている最初の WLAN である WLAN 1 になります。このようになるのは、他の ほとんどの認証方法では、コントローラと情報をやりとりする必要があるので、WAN リンクが ダウンすると処理ができなくなるためです。スタンドアロン モードでは、最低限の機能セットが LAP でサポートされます。REAP LAP がスタンドアロン モードのときにサポートする機能セッ トを、通常モードで(WAN リンクがアップしていて WLC への通信もアップしているときに) REAP LAP がサポートする機能と比較して、次の表に示します。

通常の R	REAP モー	ドとスタ	ンドアロン	モードで	<b>REAP LAP</b>	がサポー	トす	る機能
-------	---------	------	-------	------	-----------------	------	----	-----

		REAP	REAP
		(nomial mode)	(standalone mode)
	IPv4	Yes	Yes
	IPv6	Yes	Yes
Protocols	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
	Number of SSIDs	16	l (the first one)
WLAN	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
MLANI	Multiple interfaces	No	No
VLAN	802.1Q Support	No	No
	Rogue AP detection	Yes	No
WLAN Security	Exclusion list	Yes	Yes (existing members only)
	Peer-to-Peer blocking	No	No
	Intrusion Detection System	Yes	No
	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
Layer 2 Security	WPA-PSK	Yes	Yes
	WPA2-PSK	No	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No
	Web Authentication	No	No
	IPsec	No	No
Layer 3 Security	L2TP	No	No
	VPN Pass-through	No	No
	Access Control Lists	No	No
	QoS Profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
QoS	Per-user bandwidth contracts	No	No
_	WMM	No	No
	802.11e (future)	No	No
	AAA QoS Profile override	Yes	No
Mahalita	Intra-subnet	Yes	Yes
Mobility	Inter-subnet	No	No
DHCP	Internal DHCP Server	No	No
	External DHCP Server	Yes	Yes
Topology	Direct connect (2006)	No	No

この表には、複数の VLAN ぱ両方のモードの REAP LAP でサポートされないことが示されてい ます。複数の VLAN がサポートされないのは、REAP LAP が IEEE 802.1Q VLAN タギングを実 行できないので、REAP LAP が存在できるのは 1 つのサブネット上だけになるためです。そのた め、各 Service Set Identifier (SSID)のトラフィックは、有線ネットワークと同じサブネットで 終端します。その結果、SSID 間にまたがる無線伝送中に無線トラフィックがセグメント化され ることがあったとしても、有線側のデータ トラフィックは分割されません。 <u>REAP の配備、REAP の管理および制限についての詳細は、『</u>ブランチオフィスでの REAP 導入 ガイド』を参照してください。

## <u>設定</u>

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。

デバイスを設定してネットワーク構成を実装するには、次の手順を実行します。

- 1. WLC の基本動作用の設定と WLAN の設定
- 2. <u>リモート サイトにインストールするための AP のプライミング</u>
- 3. WAN リンクを確立するための 2800 ルータの設定
- 4. <u>リモート サイトでの REAP LAP の配備</u>

#### <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。



本社とブランチオフィスは専用回線を使用して接続されています。この専用回線は両端の 2800 シリーズ ルータで終端しています。この例では、Open Shortest Path First(OSPF)プロトコル を使用し、WAN リンク上で PPP カプセル化を使用してデータをルーティングしています。本社 には 4400 WLC があり、リモート オフィスには 1030 LAP を配備する必要があります。1030 LAP では、2 つの WLAN をサポートする必要があります。WLAN のパラメータは次のとおりで

- す。
  - ・WLAN 1SSID:SSID1認証:オープン暗号化:Temporal Key Integrity Protocol(TKIP)(WPA Pre-Shared Key [WPA-PSK])
  - WLAN 2SSID: SSID2認証: Extensible Authentication Protocol (EAP)暗号化: TKIP注 : WLAN 2の場合、このドキュメントの設定ではWPA(802.1x認証とTKIP(暗号化)を使用し ます。

この設定に合せて、デバイスを設定する必要があります。

#### WLC の基本動作用の設定と WLAN の設定

基本動作用に WLC を設定するには、command-line interface(CLI; コマンドライン インターフェ イス)上でスタートアップ コンフィギュレーション ウィザードを使用できます。この他、GUI を使用して WLC を設定することもできます。このドキュメントでは、CLI 上でスタートアップ コンフィギュレーション ウィザードを使用した、WLC 上の設定について説明しています。

WLC が初めて起動すると、スタートアップ コンフィギュレーション ウィザードに直接入ります 。基本設定を設定するには、コンフィギュレーション ウィザードを使用します。このウィザード は、CLI または GUI で実行できます。スタートアップ コンフィギュレーション ウィザードの例 を次に示します。

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC_MainOffice
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 172.16.1.50
Management Interface Netmask: 255.255.0.0
Management Interface Default Router: 172.16.1.60
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 172.16.1.1
AP Manager Interface IP Address: 172.16.1.51
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (172.16.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Main
Network Name (SSID): SSID1
Allow Static IP Addresses [YES][no]: Yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: Yes
Enable 802.11a Network [YES][no]: Yes
Enable 802.11g Network [YES][no]: Yes
Enable Auto-RF [YES][no]: Yes
```

Configuration saved! Resetting system with new configuration... この例では、WLC で次のパラメータを設定します。

・システム名
・管理インターフェイスの IP アドレス
・AP マネージャ インターフェイスの IP アドレス

- 管理インターフェイスのポート番号
- 管理インターフェイスの VLAN ID
- モビリティ グループの名前
- SSID
- 他の多数のパラメータ

これらのパラメータは、WLC を基本動作用に設定するために使用します。このセクションの WLC 出力に示されているように、WLC では管理インターフェイス IP アドレスとして 172.16.1.50 が使用され、AP マネージャ インターフェイス IP アドレスとして 172.16.1.51 が使 用されています。ネットワークに 2 つの WLAN を設定するためには、WLC で次の手順を実行し ます。

- 1. WLC の GUI で、ウィンドウの上部のメニューにある WLANs をクリックします。WLANs ウィンドウが表示されます。このウィンドウには、WLC に設定されている WLAN の一覧が 表示されます。スタートアップ コンフィギュレーション ウィザードを使用して 1 つの WLAN を設定したので、この WLAN の他のパラメータを設定する必要があります。
- 2. WLAN SSID1 の Edit をクリックします。以下が一例です。

4 • • • • 🔘 🗊 🖽	0 1 2 3 3	1 in the second							10 - C - C
Croce Sectors							Save C	onfiguration	Ping Logout Refresh
HE AND	MONITOR	WLANS	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	COMMANDS	HEUP	
WLANS	WLANS								New
WLANS WLANS	WLAN ID	WLAN SSI	D		Admin Status	Security Polic	ies		
AP GIOUPS YEAR	1	SSID1			Enabled	802.1×			Barneve Anchors
	* WLAN IS	Ds 9-16 will i	not be pushed to 1	130,1200 and	1240 AP mode	s.			

WLANs > Edit ウィンドウが表示されます。このウィンドウでは、General Policies、 Security Policies、RADIUS server など、その WLAN に固有のパラメータを設定できます。

 WLANs > Edit ウィンドウで次のように選択します。この WLAN を有効にするために、 General Policies 領域にある Admin Status の横の Enabled チェックボックスにチェックマ ークを付けます。WLAN 1 で WPA を使用するために、Layer 2 Security ドロップダウン メ ニューから WPA を選択します。ウィンドウの最下部で WPA パラメータを定義します。 WLAN 1 で WPA-PSK を使用するために、WPA Parameters 領域にある Pre-Shared Key の 横の Enabled チェックボックスにチェックマークを付けて、WPA-PSK のパスフレーズを入 力します。WPA-PSK では、暗号化に TKIP が使用されます。注: WPA-PSKパスフレーズ

#### は、クライアントアダプタに設定されているパスフレーズと一致している必要があります。 [Apply] をクリックします。以下が一例です。

÷ • ⇒ • 🔘 🕃 🖽	Q. E. @ Ø S- D						100	- 6 >
inco Serres						onfiguration Ping	Logout	Refres
A A	MONITOR WLANS CO	NTROLLER WIREL	ESS SECURITY	MANAGEMENT	COMMANDS	HELP		
WLANS	WLAN ID	1						
WI ANS	WLAN SSID	SSID1						
WLANS AP Groups VLAN	General Policies			Securit	y Policies			
	Radio Policy	All				From the	-	
	Admin Status	Enabled		Layer	2 Security	WPA	-	$\sim$
	Session Timeout (secs)	1800				MAC Filtering	)	
	Quality of Service (QoS)	Silver (best effort)		Layer	3 Security	None		
	WMM Policy	Disabled .				Web Policy *	_	
	7920 Phone Support	Client CAC Limit	AP CAC Limit					
	Broadcast SSID	Enabled						
	Allow AAA Override	Enabled		* Web and L2	Policy cannot be TP.	e used in combination	n with IPse	¢
	Client Exclusion	Enabled ** 60 Tim	eout Value (secs)	** Wh	en client exclusio leans infinity(will	an is enabled, a time I require administrati	out value o ive overrid	ef le to
	DHCP Server	C Override		reset e	excluded clients)			
	DHCP Addr. Assignment	Required						
	Interface Name	management ·						
	Radius Servers							
		Authentication Server	Accounting Se	ervers				
	Server 1	none 💌	none 💌					
	Server 2	none 💌	none 💌					
	Server 3	none 💌	none 💌					
	WPA Parameters							
	802.11 Data Encryption	TKIP-MIC						
	Pre-Shared Key	Enabled						
		E Set Passphrase	******					
								1

これで、WLAN1にWPA-PSKの暗号化を設定できました。

- 4. WLAN 2 を定義するために、WLANs ウィンドウにある **New** をクリックします。WLAN > New ウィンドウが表示されます。
- 5. WLAN > New ウィンドウで、WLAN ID と WLAN SSID を定義して、**Apply** をクリックしま す。以下が一例です。

★ • * * Ø 2 4 Ø	E @ 3 E-3							199 - 6 ×
Cinco Sentene								Logout Refresh
A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS WLANS	WLAN ID	2						
AP Groups VLAN	WLAN SSID	SSID2						
	L							

2 番目の WLAN の WLAN > Edit ウィンドウが表示されます。

6. WLANs > Edit ウィンドウで次のように選択します。この WLAN を有効にするために、 General Policies 領域にある Admin Status の横の Enabled チェックボックスにチェックマ ークを付けます。この WLAN に WPA を設定するために、Layer 2 Security ドロップダウン メニューから WPA を選択します。Radius Servers 領域で、このクライアントの認証に使用 する適切な RADIUS サーバを選択します。[Apply] をクリックします。以下が一例です。

ו⇒•© 2 ∆	0, 11 6 3 14 . 3			111-1
Cinco Serren			Save	Configuration   Ping   Logout   Refr
	MONITOR WEAKS CO	NIROLLER WIRELESS SECORITY	MANAGEMENT COMMAND	S HEDP
WLANS	WLANs > Edit			< Back Apply
WLANS WLANS	WLAN ID	2 SSID2		
ar croups room	General Policies		Security Policies	
	Radio Policy	All	Laver 2 Security	WPA •
	Admin Status	Enabled		MAC Fittering
	Quality of Service (QoS)	Silver (best effort)	Layer 3 Security	None
	WMM Policy	Disabled •		Web Policy *
	7920 Phone Support	Client CAC Limit CAP CAC Limit		
	Broadcast SSID	Enabled	* Web Policy cann	ot be used in combination with IPsec
	Allow AAA Override Client Exclusion	Enabled ** 60	and L2TP.	clusion is enabled, a timeout value of
	DHCP Server	Timeout Value (secs)	reset excluded clie	y(will require administrative override to ints)
	DHCP Addr. Assignment	Required		
	Interface Name	management .		
	Radius Servers			
		Authentication Servers Accounting	Servers	
	Server 1	IP:172.16.1.1, Port:1812 • none •	>	
	Server 2	none · none ·		
	Server 3	none none .		
	WPA Parameters			
	802.11 Data Encryption	TKIP-MIC		
	Pre-Shared Key	Enabled		

**注:この**ドキュメントでは、RADIUSサーバとEAP認証を設定する方法については説明していま せん。<u>WLC で EAP 認証を設定する方法については、『</u>WLAN コントローラ(WLC)での EAP 認証の設定例』を参照してください。

### <u>リモート サイトにインストールするための AP のプライミング</u>

プライミングとは、自分が接続できるコントローラのリストを LAP が取得する処理のことです。 1 つのコントローラに LAP が接続するとすぐに、そのモビリティ グループ内のすべてのコントロ ーラが LAP に通知されます。そのようにして、LAP はグループ内の任意のコントローラに加入 するために必要な情報をすべて学習します。

REAP 対応の AP のプライミングを行うためには、AP を本社の有線ネットワークに接続します。 このように接続すると、AP が 1 つのコントローラを見つけることができます。本社のコントロ ーラに LAP が加入した後、WLAN のインフラストラクチャと設定に対応するバージョンの AP オ ペレーティング システム (OS) のバージョンを AP がダウンロードします。モビリティ グルー プ内のすべてのコントローラの IP アドレスが AP に転送されます。AP が必要な情報をすべて入 手したら、AP をリモート サイトで接続できるようになります。IP 接続が使用できる場合は、リ ストから最も使用率が低いコントローラを AP が見つけて参加できます。

**注:リモートサ**イトにAPを出荷するためにAPをオフにする前に、APを「REAP」モードに設定 してください。コントローラの CLI か GUI を使用するか、Wireless Control System(WCS)の テンプレートを使用して、AP レベルでモードを設定できます。デフォルトでは、AP は通常の「 local」機能を実行するように設定されています。

コントローラを見つけるために、LAP は次の方法のいずれかを使用できます。

・レイヤ2のディスカバリ

・レイヤ3のディスカバリローカルサブネットのブロードキャストの使用DHCPオプション43の使用DNSサーバの使用Over-the-Air Provisioning(OTAP)の使用内部DHCPサーバの使用注:内部DHCPサーバを使用するには、LAPがWLCに直接接続されている必要があります。

このドキュメントでは、DHCP オプション 43 ディスカバリ メカニズムを使用して LAP が WLC に登録されていることを前提としています。DHCP オプション 43 を使用して LAP をコントロー <u>ラに登録する方法および他のディスカバリ メカニズムについての詳細は、『</u>ワイヤレス LAN コ ントローラ(WLC)への Lightweight AP(LAP)の登録』を参照してください。

LAP がコントローラを見つけたら、AP がコントローラに登録されていることが WLC の Wireless ウィンドウに表示されます。以下が一例です。

÷•*** ◎ 🖸 🖄 !	Q B 6 9 6 6 9				11 - 8 ×
Cinca Statem				Save Configuration	ring Logout Refresh
A. A.	MONITOR WLANS CONT	TROLLER WIRELESS SECURITY MA	NAGEMENT COM	MANDS HELP	
Wireless	All APs				
Access Points All APs	Search by Ethernet MAC	Search			
802.11a Radios 802.11b/g Radios				Operational	
Bridging	AP Name	AP 10 Ethernet MAL	Admin Status	Status	
Rogues	ap:\$1:5a:e0	5 00:0b:85:51:5a:e0	Enable	REG 1	Detail
Known Rogue APs					
Rogue Clients Adhoc Rogues					
Clients					
Global RF					
802.11a Network					
802.11h					
Country					
Timers					

通常の REAP モードに LAP を設定するには、次の手順を実行します。

- 1. WLC の GUI で、**[Wireless]**をクリックします。All APs ウィンドウが表示されます。このウ ィンドウには、WLC に登録されている AP の一覧が表示されます。
- REAP モードに設定する必要がある AP を選択して、Detail をクリックします。その AP の All APs > Detail ウィンドウが表示されます。このウィンドウでは、次のような AP のさまざ まなパラメータを設定できます。AP 名IP アドレス(スタティックに変更できます)管理ス テータスセキュリティ パラメータAP モードAP が接続できる WLC のリストその他のパラ メータ
- 3. AP Mode ドロップダウン メニューから REAP を選択します。このモードを使用できるのは、REAP 対応の AP だけです。
- 4. AP が登録に使用するコントローラ名をを定義して、Apply をクリックします。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できます。 AP 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。以 下が一例です

Wireless	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY				
Wireless				DECORT	MANAGEMENT	COMMANDS	HELP	
	All APs > Details						< Back	Apply
All APs 802:11a Radios 802:11b/g Radios vridging togues Rogue APs Known Rogue APs Rogue Clients Adhoc Rogues Clients Clients Clients Clients Clients Clients Country Clients Country Clients Country Clients	General AP Name Ethernet MAC Address Bese Radio MAC Regulatory Domain AP IP Address AP Static IP AP ID Admin Status AP Mode Operational Status Port Number AP Group Name Location Primary Controller Name Secondary Controller Name Statistics Timer	ap:S1:Sa:e0 00:0b:05:S1: 00:0b:05:S1: 00211bg: -A ( 172.16.1.00 AP Static IP [ Netmask 2 Gateway 1 S Enable • REG 1  Remote Office WLC_MainOff 100	5a:e0 5a:e0 00211a: -A 192.168.1.5 155.255.255.0 192.168.1.1		Versions S/W Version Boot Version Inventory Info AP Model AP Serial Num AP Certificate REAP Mode sup	3.2.7 2.1.7 AP10 ber WCN Type Manu pported Yes	8.0 8.0 30 092201RT facture Installed	
	the share of the first state	d						
	number of Radio Inter	Taces	2					

これで AP を REAP モードに設定できたので、リモート サイトに AP を配備できます。

注:この例のウィンドウでは、APのIPアドレスがスタティックに変更され、スタティックIPアドレス192.168.1.5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 サーバから取得する 172.16.1.80 という IP アドレスを使用するのは、プライミング段階の間だけです。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。

#### WAN リンクを確立するための 2800 ルータの設定

この例では、WANリンクを確立するために、2台の2800シリーズルータをOSPFで使用して、ネットワーク間で情報をルーティングしています。次に、このドキュメントのシナリオ例で使用する両方のルータの設定を示します。

本社
MainOffice# <b>show run</b>
Building configuration
Current configuration : 728 bytes !
version 12.2 service timestamps debug uptime

```
service timestamps log uptime
no service password-encryption
hostname MainOffice
1
!
ip subnet-zero
!
1
1
interface Ethernet0
ip address 172.16.1.60 255.255.0.0
!--- This is the interface which acts as the default
gateway to the WLC. ! interface Virtual-Template1 no ip
address ! interface SerialO no ip address ! interface
Seriall !--- This is the interface for the WAN link. ip
address 10.0.0.1 255.0.0.0 encapsulation ppp !--- This
example uses PPP. Use the appropriate !--- encapsulation
for the WAN connection. ! router ospf 50 !--- Use OSPF
to route data between the different networks. log-
adjacency-changes network 10.0.0.0 0.255.255.255 area 0
network 172.16.0.0 0.0.255.255 area 0 ! ! ip classless
ip http server ! ! ! line con 0 line aux 0 line vty 0 4
! end
ブランチオフィス
BranchOffice#show run
Building configuration ...
Current configuration : 596 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
1
hostname BranchOffice
!
1
ip subnet-zero
!
!
!
interface Ethernet0
ip address 192.168.1.1 255.255.255.0
!--- This is the interface which acts as the default
gateway to the LAP. ! interface SerialO no ip address !
interface Serial1 !--- This is the interface for the WAN
link. ip address 10.0.0.2 255.0.0.0 encapsulation ppp
clockrate 56000 ! router ospf 50 !--- Use OSPF to route
data between the different networks. log-adjacency-
changes network 10.0.0.0 0.255.255.255 area 0 network
192.168.1.0 0.0.0.255 area 0 ! ip classless ip http
server ! ! ! ! line con 0 line aux 0 line vty 0 4 login
autocommand access enable-timeout 2 ! end
```

### <u>リモート サイトでの REAP AP の配備</u>

WLC での WLAN の設定、LAP のプライミング、本社とリモート オフィスの WAN リンクの確立

が完了したので、リモート サイトに AP を配布する準備が整いました。

リモート サイトで AP の電源を投入すると、プライミング段階に設定した順序で AP がコントロ ーラを探します。AP がコントローラを見つけると、コントローラに AP が登録されます。次に例 を示します。ポート 1 にあるコントローラに AP が参加したことが WLC に次のように表示され ます。

÷••* © 2 ₫	0	B & 3 B - 3							19 - 8 ×
Cinco Statems								onfiguration Ping	Logout Refresh
A. A.		MONITOR WLANS	CONTROLLER	WIRELES	IS SECURITY	MANAGEMENT	COMMANDS	HELP	
Wireless		All APs							
Access Points All APs		Search by Etherne	E MAC		Search				
B02.11b/g Radios Bridging		AP Name		AP ID	Ethernet MAC	Admin 5	itatus Operat Status	tional Port	
Rogues	<	ap:51:5a:e0		5	00:0b:05:51:5a	e0 Enable	REG	1	Detail
Rogue APs Known Rogue APs Rogue Clients Adhoc Rogues									
Clients									
Global RF 802.11a Network 802.11b/g Network									
Country									
Timers									

SSID1 という SSID で WPA-PSK が有効になっているクライアントは WLAN 1 の AP に関連付け られています。SSID2 という SSID で 802.1x 認証が有効になっているクライアントは WLAN 2 の AP に関連付けられています。次に、2 つのクライアントの例を示します。1 つのクライアント は WLAN 1 に接続されており、もう一つのクライアントは WLAN 2 に接続されています。

÷· → · ③ 🕃 🖧 🔘	693 6-3								12	- 8 ×
Cinco Serren									Logout	Ref Close
A.A.	MONITOR WLAN	CONTROLLER	WIRELESS SEC	URITY MANAGE	MENT CO	MMANDS	HELP	_		
Monitor	Clients						Items 1	to 2	of 2	
Summary	Search by MAC ad	Idress	Searc	h						
Statistics										
Ports	Client MAC Addr	AP Name	AP MAC Addr	WLAN	Туре	Status	Auth	Port	Detail	
Wireless Rogue APs Known Bogue APs	00:40:96:ac:dd:05	ap:S1:Sa:e0	00:0b:85:51:5a:e0	SSID1	802. <b>11</b> a	Associated	Yes	1	LinkTest Disable Remove	
Rogue Clients Adhoc Rogues 802.11a Radios	00:40:96:ac:e6:57	ap:51:5a:e0	00:0b:85:51:5a:e0	SSID2	802.11a	Associated	Yes	1	Detail LinkTest Disable Remove	
Clients RADIUS Servers										

## <u>確認</u>

ここでは、REAP 設定が正常に動作していることを確認します。

注:debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

WAN リンクをダウン状態にします。WAN リンクがダウン状態になると、AP と WLC との接続 が失われます。その場合、WLC は AP をリストから登録解除します。以下が一例です。

(Cisco Controller) >debug lwapp events enable Wed May 17 15:04:22 2006: Did not receive heartbeat reply from AP 00:0B:85:51:5A:E0 Wed May 17 15:04:22 2006: Max retransmissions reached on AP 00:0B:85:51:5A:E0 (CONFIGURE\_COMMAND, 1) Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Down LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17 15:04:22 2006: apfSpamProcessStateChangeInSpamContext: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17 15:04:22 2006: spamDeleteLCB: stats timer not initialized for AP 00:0b:85:51:5a:e0 Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 0! Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May 17 15:04:22 2006: Received LWAPP Down event for AP 00:0b:85:51:5a:e0 slot 1!

Wed May 17 15:04:22 2006: Deregister LWAPP event for AP 00:0b:85:51:5a:e0 slot 1

debug Iwapp events enable コマンドの出力には、WLC が AP からハートビートの応答を受信し なかったので、WLC が AP の登録を解除したことが示されています。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 秒間の間隔を空けてハートビート を 5 回連続して試みます。WLC が応答を受信しなければ、WLC は AP を登録解除します。

AP がスタンドアロン モードの時には、AP の電源 LED が点滅します。最初の WLAN(WLAN 1)のクライアントは WPA-PSK の暗号化専用に設定されているので、最初の WLAN(WLAN 1)に関連付けられているクライアントはその AP に引き続き関連付けられています。スタンドア ロン モードでは、LAP が自分で暗号化も処理します。次の例は、SSID1 および WPA-PSK を使 用して WLAN 1 に接続されているクライアントの(WAN リンクがダウンしているときの)ステ ータスを示しています。

**注**:TKIPはWPA-PSKで使用される暗号化です。

🛜 Cisco Aironet Desktop Utility -	Current Profile: SSID1		? ×
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS Profile Name:	SSID1		
Link Status:	Authenticated		
Wireless Mode:	5 GHz 54 Mbps	IP Address: 192.168.1.24	
Network Type:	Infrastructure	Current Channel: 64	
Server Based Authentication:	None	Data Encryption: TKIP	
Signal Strength:			
		Advanced	

WLAN 2 では EAP 認証が使用されているので、WLAN 2 に接続されているクライアントは接続解除されます。このように接続解除されるのは、EAP 認証を使用するクライアントは WLC と通信 する必要があるためです。次のウィンドウの例には、WAN リンクがダウンしているときに EAP 認証が失敗する例が示されています。

LEAP Authenticatio	n Status						?
Card N Profile N	LEAP Aut	hentication				×	
Steps	⚠	Card Name: Profile Name:	Cisco Airo SSID2	net 802.11a/b/	/g Wireless Ac	lapter	
2. Checking 3. Renewing 4. Detecting 5. Finding D		Message:	Unable to user in the Network ir may also v value for t	LEAP authenti specified amo frastructure m vant to increas this profile.	cate the wirel ount of time, night be down se the LEAP tir	ess . You meout	
			( Ok				Cancel

WAN リンクがアップしたら、AP は通常の REAP モードに再び切り替わり、コントローラに登録 されます。EAP 認証を使用するクライアントもアップ状態になります。以下が一例です。

🛜 Cisco Aironet Desktop Utility - Currer	nt Profile: 55ID2	<u>?</u> ×
<u>Action</u> <u>Options</u> <u>H</u> elp		
LEAP Authentication Status		? <u>- </u> ×
Card Name: Cisco Aironet 802.11		
Profile Name: SSID2		
Steps	Status	
1. Starting LEAP Authentication	Success	
2. Checking Link Status	Success	
3. Renewing IP address	Success	
4. Detecting IPX Frame Type	Success	
5. Finding Domain Controller	Success	
🗖 Sh	Cancel	
Auto Select Profiles		Urder Pronies

この例では、コントローラの debug lwapp events enable コマンドの出力は、次のような結果に なります。

(Cisco Controller) >debug lwapp events enable Wed May 17 15:06:40 2006: Successful transmission of LWAPP Discovery-Response to AP 00:0b:85:51:5a:e0 on Port 1 Wed May 17 15:06:52 2006: Received LWAPP JOIN REQUEST from AP 00:0b:85:51:5a:e0to 00:0b:85:33:84:a0 on port '1' Wed May 17 15:06:52 2006: LWAPP Join-Request MTU path from AP 00:0b:85:51:5a:e0is 1500, remote debug mode is 0 Wed May 17 15:06:52 2006: Successfully added NPU Entry for AP 00:0b:85:51:5a:e0(index 51) Switch IP: 172.16.1.51, Switch Port: 12223, intIfNum 1, vlanId 0AP IP: 192.168.1.5, AP Port: 5550, next hop MAC: 00:d0:58:ad:ae:cb Wed May 17 15:06:52 2006: Successfully transmission of LWAPP Join-Reply to AP 00:0b:85:51:5a:e0 Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 0 Wed May 17 15:06:52 2006: Register LWAPP event for AP 00:0b:85:51:5a:e0 slot 1 Wed May 17 15:06:54 2006: Received LWAPP CONFIGURE REQUEST from AP 00:0b:85:51:5a:e0 to 00:0b:85:33:84:a0 Wed May 17 15:06:54 2006: Updating IP info for AP 00:0b:85:51:5a:e0 -- static 1, 192.168.1.5/255.255.255.0, gtw 192.168.1.1

## <u>トラブルシュート</u>

このセクションは、設定のトラブルシューティングを行う際に参照してください。

### <u>トラブルシューティングのためのコマンド</u>

次の debug コマンドを使用して、設定のトラブルシューティングを行うことができます。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- debug lwapp events enable: LAP と WLC の間で発生するイベントのシーケンスが表示され ます。
- debug lwapp errors enable: LWAPP 通信で発生するエラーが表示されます。
- debug lwapp packet enable: LWAPP パケット トレースのデバッグが表示されます。
- debug mac addr:指定したクライアントの MAC デバッグが有効になります。

### <u>関連情報</u>

- ・<u>ブランチオフィスでの REAP 導入ガイド</u>
- EAP 認証と WLAN コントローラ (WLC) の設定例
- ・ 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
- ・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>ワイヤレスに関するサポート ページ</u>
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。