

Cisco Unified Wireless Network ゲスト ア クセス サービス

企業が無線 LAN (WLAN) テクノロジーを導入することにより、従業員やネットワーク リソースが固 定ネットワーク接続の制約から解放され、大企業や中小企業の行動の取り方に変化が生じてきました。

また、WLAN によって、個人が公共の場所からインターネットや会社のネットワークにアクセスする 方法も変化しました。公衆 WLAN (ホットスポット)の出現により、モバイル ワーカーは、事実上ど こからでも会社のネットワークにアクセスできることが当たり前だと考えています。

概要

パブリック アクセスのパラダイムは、企業にも広がってきています。移動性の高い情報オンデマンド 文化には、オンデマンド ネットワーク接続が必要です。このような理由から、エンタープライズ ゲス ト アクセス サービスは、重要性を増し、企業環境に不可欠のものとなっています。

ゲスト ネットワーキングが重要性を増していることが広く知られている一方で、社内情報やインフラ ストラクチャ資産の安全性に対する不安があることも事実です。実装が適切であれば、たいていのゲス トアクセス ソリューションを実装した企業では、実装プロセスに関連したネットワーク監査によって、 全体的なセキュリティ状況が改善されます。

全体的なセキュリティの改善に加えて、ゲスト アクセス ネットワークの実装によって、次のような全 般的メリットが得られます。

- 日付、期間、帯域幅などの変数に基づく、ゲストの認証と権限付与の制御
- ネットワークを使用中または使用したことのあるユーザをトラックする監査メカニズム

さらに、無線ベースのゲストアクセスのメリットには、次のものが含まれます。

- かつては有線によるネットワーク接続もなかったロビーや共有施設などのエリアを含め、より広範 なカバレッジを提供します。
- ゲストアクセスの領域や部屋を設定する必要がなくなります。

スコープ

企業でゲストアクセスを提供する際、複数のアーキテクチャを実装できます。この章の目的は、考え られるソリューションをすべて紹介することではありません。その代わりに、この章では、Cisco Unified Wireless Network ソリューションを使用した無線ゲストネットワーキングの実装を中心に説明 します。その他のトポロジシナリオにおける有線および無線ゲストアクセスサービスの展開に関する 詳細は、次の URL を参照してください。 http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/GuestAcc.html.

無線ゲスト アクセスの概要

理想としては、無線ゲスト ネットワークの実装で、企業の既存の無線および有線インフラストラク チャを最大限活用して、物理オーバーレイ ネットワークを構築する際のコストや複雑さを回避します。 この場合は、次の要素と機能の追加が必要になります。

- 専用のゲスト WLAN/SSID: ゲスト アクセスを必要とするあらゆる場所で、キャンパス無線ネットワークを介して実装されます。
- ゲストトラフィックのセグメンテーション:ゲストの移動場所を制限するために、キャンパスネットワーク上のレイヤ2またはレイヤ3での実装テクニックを必要とします。
- アクセス コントロール:キャンパス ネットワーク内に組み込まれたアクセス コントロール機能の 使用、または企業ネットワークからインターネットへのゲスト アクセスを制御する外部プラット フォームの実装を伴います。
- ゲストユーザ資格情報の管理:スポンサーまたは Lobby 管理者がゲストの代わりに仮の資格情報 を作成できるプロセス。この機能は、アクセスコントロール プラットフォーム内に常駐している 場合と、AAA またはその他の管理システムのコンポーネントになっている場合があります。

Cisco Unified Wireless Network ソリューションを使用したゲスト アク セス

Cisco Unified WLAN ソリューションは、中央集中型アーキテクチャ内で Ethernet in IP (RFC3378) を使用することにより、柔軟で簡単な実装方法で無線ゲスト アクセスの展開を提供します。Ethernet in IP は、2 つの WLC エンドポイント間にあるレイヤ 3 トポロジ上のトンネルを作成する際に使用されます。このアプローチのメリットは、ゲスト トラフィックを企業から分離するために実装が必要となる、プロトコルやセグメンテーション テクニックを追加しなくていいことです。

中央集中型 WLAN アーキテクチャを使用したゲスト アクセス トポロジの例については、図 10-1 を参照してください。



図 10-1 中央集中型コントローラのゲスト アクセス

図 10-1 に示すように、アンカー コントローラが企業 DMZ 内に配置され、「アンカー」機能を実行し ます。アンカー コントローラは、ネットワーク上のその他のキャンパス コントローラを起点とする EoIP トンネルの終端処理に関与します。これらの「外部」コントローラは、企業全体にプロビジョン されたさまざまな WLAN (1 つ以上のゲスト WLAN を含む)の終端、管理、および標準の動作に関与 します。ゲスト WLAN は EoIP トンネルを経由してアンカー コントローラに転送されます。具体的に は、ゲスト WLAN のデータ フレームが、CAPWAP を使用して AP から外部コントローラにカプセル 化されてから、外部管理システムからアンカー WLC で定義されたゲスト VLAN に EoIP でカプセル化 されます。このように、ゲスト ユーザ トラフィックは、社内の他のトラフィックによって認識される ことなく、また相互作用することなく、透過的にインターネットに転送されます。

WLAN コントローラ ゲスト アクセス

ゲスト アクセス ソリューションは、内蔵型であり、アクセス コントロール、Web ポータル、または AAA サービスを実行するための外部プラットフォームを必要としません。これらの機能はすべて、ア ンカー コントローラ内で構成および実行されます。ただし、これらの機能のうち1つまたはすべてを 外部で実装するためのオプションがあり、これについてはこの章の後半で説明します。

サポートされるプラットフォーム

トンネル終端、Web 認証、およびアクセス コントロールを含むアンカー機能が、次の WLC プラット フォームでサポートされています (バージョン 6.0 以降を使用した場合)。

- WLC 2504
- WLC 5508
- WiSM-2
- WLC 7500

次の WLC プラットフォームは、アンカー機能に使用できませんが、標準のコントローラ展開と指定したアンカー コントローラへのゲスト モビリティ トンネルの起点(外部 WLC)として使用できます。

- サービス統合型ルータ用 Cisco WLAN コントローラ モジュール (ISR-SM)
- Cisco 2504

無線ゲスト アクセスをサポートする自動アンカー モビリティ

自動アンカー モビリティ、つまりゲスト WLAN モビリティは、Cisco Unified Wireless Network ソ リューションの主要な機能です。EoIP トンネルを使用して、プロビジョンされたゲスト WLAN を 1 つ 以上の(アンカー)WLC にマップできます。自動アンカー モビリティによって、ゲスト WLAN と関 連するすべてのゲスト トラフィックを、インターネット DMZ に常駐するアンカー コントローラに企 業ネットワークを通して透過的に転送できます(図 10-2 を参照)。



図 10-3 は、ゲスト WLAN がプロビジョンされた外部コントローラとローカル Web 認証を実行してい るアンカー コントローラ間の Ethernet in IP トンネル (強調表示部分)のスニファ トレースを示してい ます。図中の最初の IP 詳細は、外部コントローラとアンカー コントローラ間の Ethernet in IP トンネ ルを示しています。2 番目の IP 詳細は、ゲスト トラフィックの詳細です(この場合は、DNS クエ リー)。

Ø	(Untit	led) -	Ethere	al											k									
Eile	e Edit	⊻iew	/ <u>G</u> o	⊆apture	Analyz	e Stal	tistics E	lelp																
	ų õ	10	1		6		× ć	9 🗄	6) 🗇	🔿 🏟	7	⊉		4	Ð	Q	1:1	+ +			5	*	Ø
Eilb	er: (ip	addr	eq 10.2	0.31.10	3)					•	Expression	<u>⊆</u> le	ar <u>Appl</u>	y										
No.		Time		Sour	rce			Destina	ition		Protocol	Info	,											^
	17	12.7	45691	. 192	2.168.	1.1		10.2	0.31.1	03	DHCP	DHC	P ACK		- Tr	ansa	ction	ID	0x8db	4c53f				
	22	15.8	39516 40040	10.	20.31	103		224	0.31.2	55	NBNS	Reg	gistra Membe	tion	NB WI	RELE	ss-z<	(00>						_
	25	15.8	355503	10.	20.31	.103		239.	255.25	5.250	SSDP	M-9	SEARCH	і * HT	TP/1.	.1								
	27	15.9	39718	3 10.	20.31	103		171.	70.168	.183	DNS	Sta	andard	quer	YA t	time.v	windo	ws.c	om					
	28	15.9	65757	171	70.1	.68.18	33	10.2	0.31.1	03	DNS	Sta	andard	quer	y res	sponse	e A 2	07.4	6.232	.189	A 20	7.46.	130.10	0
	29	16.0	00184	10.	20.31	103		207.4	46.232	.189	NTP	NTF	2											
	20	16.5	88540	10.	20.31	103		10 20	10.130	55	NENS	Dec	nictra	tion	NR WI		cc_7/	005						
	39	16.7	59426	10	20.31	.103		224.1	0.0.22	55	IGMP	V3	Membe	rshin	Repo	ort	55424							
	40	17.3	39600	10.	20.31	.103		10.20	0.31.2	55	NBNS	Rec	gistra	tion	NB WI	RELE	ss-2<	<00>						
	41	18.0	90691	. 10.	20.31	.103		10.20	0.31.2	55	NBNS	Rec	gistra	tion	NB WI	RELE	ss-2<	<00>						
	43	18.8	342943	10.	20.31	103		10.20	0.31.2	55	NBNS	Reg	gistra	tion	NB WO	ORKGRO	OUP7<	:00>						
	44	18.8	675739	10.	20.31	103		239.4	255.25	5.250	SSDP	M-S	SEARCH	+ HT	TP/1.	1 DKCD		0.0 %						
	40	20.3	43966	10.	20.31	103		10.2	0.31.2	55	NBNS	Per	gistra	tion	NB WO	DRKGRO		00>						
	50	20.8	30010	10.	20.31	.103		171.	70.168	.183	DNS	Sta	andard	auer	VAV	ww.m	icros	oft.	com					
	51	20.9	50007	171	70 1	60 10	27	10 20	0 21 1	02	DMC	C+ -	andand	auor	ic not	none	O CNA	MF +	ogglo	unn	me of	kadhe	pot c	ылы 🌱
	Inter	net	Proto	col, s	Src: 1	0.20.	100.2	54 (1	0.20.1	00.254	1), Dst:	10.2	0.30.4	11 (10	0.20.	30.41)							^
	Ether	ΊΡ,	versi	on 0																				
	Ver	sion	: 0×0	0																				
	Ether	net	II, S	rc: 10	. 20.3	1.103	3 (00:	40:96	:a6:d5	:3a),	Dst: 10.	20.3	1.1 ((00:00	:0c:0	7:ac:	79)							
	Des	tina	tion:	10.20	0.31.1	(00:	00:00	:07:a	c:79)															
	200	ince:	02 10	U. 51.1		N (0)	90:40	:05:54	a)															
	802 1	o vi	rtual	LAN	ai LA	us (ox	(0100)																	
	000		, cour	LAN	. = P	riori	tv: 0																	
		0			. = C	FI: C)																	
		. 00	11 11	11 111	1 = I	D: 10	23																	
	тур	e: I	P (0x	(0080																				
•	Inter	net	Proto	col,	Src: 1	0.20.	31.10	3 (10	.20.31	.103),	Dst: 17	1.70	.168.1	183 (1	L71.7	0.168	.183))						
•	User	Data	gram	Protoc	iol, s	STC PO	ort: 1	122 (1122),	Dst F	Port: dom	ain	(53)											
•	Domai	n Na	me sv	stem (querv	0																		~
000	,	u ve	84).	г ре а	τυu.	т <u>э</u> р	2 15 4	9 50	U8 UU	40 UU	····Q^	, K	J.JU	E.										^
001	0 0	0 7e	67 93	7 00 0	0 ff :	2f 3	8 b6 (a 5d	8a ea	ac 1c	.~g	· ./ 8	3]	••										
002	20 a	9 9T F 02	00 0	0 08 0 4 64 f	0 45 1	00 0 14 1	0 00 0	15 eU	00 00	7e 61	· · · · · ·	.t	10	~a										
004	10 a	c 79	00 4	0 96 a	6 d5	3a 8	1 00 0	3 ff	08 00	45 00	.v.@.			Ε.										
005	50 O	0 3e	94 fl	b 00 0	0 80 3	11 2	8 3b ()a 14	1f 67	ab 46	.>	((;g	. F										
006	50 a	8 b7	04 6	2 00 3	5 00 3	2a 7	d fc 9	2 e9	01 00	00 01	b.	5.*]		nd.										×
File	"C:ipc	CLIME	~1\User	LOCALS	1)Temp)	etherXX	XXCZHC9	S" 115 K	B 00:00:5	9		P: 4	07 D: 32	6 M: 0 D	rops: 0									
14 100	citor	COME	10001	peo chebro	*1. subl	panorna		5 115 K	0 0010010			1	01 01 020		0,00									11



アンカー コントローラ展開ガイドライン

この項では、無線ゲストアクセスをサポートするためのアンカーコントローラの展開に関するガイド ラインを提供します。

アンカー コントローラの位置決め

アンカー コントローラは、ゲスト WLAN トラフィックの終端とそれに続くインターネットへのアクセ スに関与するため、通常は企業のインターネット DMZ 内に配置されます。これによって、社内の認証 されたコントローラとアンカー コントローラ間の通信を的確に管理するためのルールをファイア ウォール内に確立できます。このルールには、送信元または送信先のコントローラのアドレス、WLC 間通信用の UDP ポート 16666、およびクライアント トラフィック用の IP プロトコル ID 97 Ethernet in IP に対するフィルタリングが含まれます。その他に必要なルールは次のとおりです。

- SNMP 用の TCP 161 と 162
- TFTP 用の UDP 69
- HTTP 用または GUI アクセスの HTTPS 用の TCP 80 または 443
- Telnet 用、または CLI アクセスの SSH 用の TCP 23 または 22

トポロジによっては、ファイアウォールを使用して、外部の脅威からアンカー コントローラを保護で きます。 最大のパフォーマンスを引き出すために、また、ネットワーク内の位置決めが推奨されていることか ら、ゲスト アンカー コントローラをゲスト アクセス機能のサポートに専念させることを強く推奨しま す。つまり、アンカー コントローラを、ゲスト アクセスの他に、社内の他の CAPWAP AP の制御や管 理に使用しないようにします。

DHCP サービス

前述したように、ゲスト トラフィックは、EoIP を経由してレイヤ 2 に転送されます。したがって、 DHCP サービスを実装できる最初のポイントは、ローカルのアンカー コントローラ上か、クライアン トの DHCP 要求を外部サーバに中継できるコントローラ上になります。設定例については、「ゲスト アクセスの設定」(P.10-13) を参照してください。

ルーティング

ゲストトラフィックは、アンカー コントローラで出力されます。ゲスト WLAN は、アンカー上の動 的なインターフェイスまたは VLAN にマッピングされます。トポロジによって、このインターフェイ スが、ファイアウォール上のインターフェイスに接続される場合と、インターネット境界ルータに直接 接続される場合があります。したがって、クライアントのデフォルトゲートウェイ IP は、ファイア ウォールの IP か、または最初のホップ ルータ上の VLAN またはインターフェイスのアドレスになり ます。入力ルーティングの場合は、ゲスト VLAN が直接、ファイアウォール上の DMZ インターフェ イスに接続されるか、境界ルータ上のインターフェイスに接続されることが考えられます。いずれの場 合も、ゲスト (VLAN) サブネットは、直結ネットワークと認識され、それに応じてアドバタイズされ ます。

アンカー コントローラのサイジングとスケーリング

企業における展開の多くで、ゲスト ネットワーキングを最も効率的にサポートするプラットフォーム は、Cisco 5508 シリーズ コントローラです。このコントローラを EoIP トンネル終端によるゲスト アク セスのサポートに限定して展開する場合、コントローラはネットワーク内の AP の管理に使用されない と考えられるため、12 個の AP をサポートする 5508 で十分です。

1 台の 5508 シリーズ コントローラで、社内にある最大 71 台の外部コントローラからの EoIP トンネル をサポートできます。さらに、5508 コントローラは、同時に最大 7,000 ユーザをサポートし、8 Gbps の転送能力があります。

ゲスト アンカー コントローラの選択は、アクティブなゲスト クライアント セッションの数によって定 義されているか、またはコントローラ上のアップリンク インターフェイスの容量によって定義されて いるか、あるいはその両方で定義されたとおりのゲスト トラフィック量に依存します。

ゲスト アンカー コントローラあたりの総スループットとクライアントの制限は次のとおりです。

- Cisco 2504 ワイヤレス LAN コントローラ:4 個の1 Gbps インターフェイスと 1000 個のゲスト クライアント
- Cisco 5508 ワイヤレス LAN コントローラ (WLC): 8 Gbps と 7,000 個のゲスト クライアント
- Cisco Catalyst 6500 シリーズ Wireless Services Module (WiSM-2): 20 Gbps と 15,000 個のクラ イアント
- Cisco 7500 ワイヤレス LAN コントローラ (WLC): 10 Gbps と 20,000 個のクライアント

アンカー コントローラの冗長性

Cisco Unified Wireless ソリューション ソフトウェアのリリース 4.1 からは、「ゲスト N+1」冗長性機 能が自動アンカー/モビリティ機能に追加されました。この機能には、自動 ping 機能が導入されてい ます。この機能によって、外部コントローラが積極的に ping をアンカー コントローラに送信して、コ ントロールとデータ パスの接続を確認できます。障害が発生したり、アクティブなアンカーに到達で きなくなった場合には、外部コントローラが次のことを行います。

- アンカーが到達できなくなっていることを自動的に検出
- 到達できないアンカーに以前にアソシエートされた無線クライアントを自動的に解除
- 無線クライアントを代替アンカー WLC に自動的に再びアソシエート

ゲスト N+1 冗長性により、所定のゲスト WLAN に 2 つ以上のアンカー WLC を定義できます。 図 10-4 は、アンカー コントローラの冗長性を備えた、一般的なゲスト アクセス トポロジを示してい ます。



図 10-4 ゲスト アンカーの N+1 冗長性を備えたゲスト アクセス トポロジ

ゲスト N+1 冗長性については、次のことに留意してください。

- 所定の外部コントローラの負荷は、ゲスト WLAN に設定されたアンカー コントローラのリスト全体で無線クライアント接続のバランスを取ります。1つのアンカーを、1つ以上のセカンダリアンカーを持つプライマリアンカーとして指定する方法は、現在のところありません。
- 到達できなくなっているアンカー WLC にアソシエートされた無線クライアントは、WLAN 用に 定義された別のアンカーに再びアソシエートされます。これが発生し、Web 認証が使用されている 場合には、クライアントは Web ポータル認証ページにリダイレクトされ、資格情報の再送信が要 求されます。

<u>》</u> (注)

Cisco Unified Wireless Network でマルチキャストが有効でも、fストトンネルではマルチキャストトラフィックはサポートされません。

Web ポータル認証

Cisco Centralized Guest Access ソリューションは、組み込み型の Web ポータルを備えています。この ポータルは、認証用のゲスト資格情報を要求するのに使用され、免責条項または利用規定情報の表示機 能と単純なブランディング機能を備えています(図 10-5 を参照)。

neb samemication	Preview - Microsoft Internet Exp	lorer provided b	y Cisco Systems,	Inc.		
jile <u>E</u> dit <u>Y</u> iew F <u>a</u> vo	nites Ilools Help 🛛 Links 🚞 TSE-	LAB 🍓 My Yahoo!	Customize Links	Ø VPN 3002 Hardware Client	🙆 Windows	» 🦧
3 Back - 🕤 - 💌	👔 🐔 🔎 Search 🔹 Favorites	🛛 🖉 🗣 🖗	🗆 🛍 🖸			
dress 🗃 https://10.20.1	110.254/screens/base/login_preview.htm	1				💌 🔁 Go
Login						uluulu cisco
Welcome to the Cisco is pleased to for your network. Ple	Cisco wireless network provide the Wireless LAN infrastruct ase login and put your air space to v	ure vork.				
User Name						
Password						
	Submit					

図 10-5 コントローラの Web 認証ページ

Web ポータル ページは、すべての Cisco WLAN Controller プラットフォーム上で使用でき、WLAN がレイヤ 3 Web ポリシーベースの認証用に設定された場合にデフォルトで呼び出されます。

よりカスタマイズされたページが必要な場合は、管理者が、カスタマイズされたページをインポートしてローカルに保存するオプションが用意されています。また、会社で外部 Web サーバを使用する場合は、内部サーバを使用せずに外部サーバにリダイレクトするようにコントローラを設定できます。Web ページの設定に関するガイドラインについては、「ゲストアクセスの設定」(P.10-13)を参照してください。

ユーザ リダイレクション

たいていの Web ベースの認証システムでは一般的なことですが、ゲスト クライアントを WLC の Web 認証ページにリダイレクトする場合は、ゲスト クライアントが Web ブラウザ セッションを起動して、 対象 URL を開く必要があります。リダイレクションが正常に動作するには、次の条件を満たす必要が あります。

 DNS 解決: ゲスト アクセス トポロジでは、有効な DNS サーバが DHCP 経由で割り当てられ、認 証前のユーザからその DNS サーバへアクセスできるようにする必要があります。クライアントが 認証で Web ポリシー WLAN にアソシエートすると、DHCP と DNS を除くすべてのトラフィック がブロックされます。そのため、DNS サーバは、アンカー コントローラから到達可能にする必要 があります。トポロジによっては、DNS を許可するためにファイアウォールを通してコンジット を開く必要がある場合と、インターネット境界ルータ上の ACL を変更する必要がある場合があり ます。

(注) 静的 DNS 設定のクライアントは、設定された DNS サーバがゲスト ネットワークからアクセス できるかどうかによって、機能しない場合があります。

- 解決可能なホームページ URL: ゲスト ユーザのホームページ URL は、DNS によってグローバル に解決可能である必要があります。たとえば、ユーザのホームページが、会社のイントラネットの 外側では解決できない社内用ホームページである場合、そのユーザはリダイレクトされません。こ の場合、ユーザは www.yahoo.com や www.google.com などの一般サイトへの URL を開く必要が あります。
- HTTP ポート 80: ユーザのホームページは解決可能ですが、HTTP ポート 80 以外のポート上にある Web サーバに接続された場合、ユーザはリダイレクトされません。また、ユーザが WLC の Web 認証ページにリダイレクトされるには、ポート 80 を使用する URL を開く必要があります。

(注)

ポート 80 に加え、コントローラがリダイレクションを監視できるように、追加ポート番号を1つ設定 するオプションは次のとおりです。この設定は、コントローラの CLI を通してのみ使用可能です。 <controller name> config> network web-auth-port port>

ゲスト資格情報の管理

ゲスト資格情報は、リリース 4.0 以降の管理システムを使用して、一元的に作成および管理できます。 ネットワーク管理者は、管理システム内に限定的な特権アカウントを作成し、ゲスト資格情報を作成す る目的の Lobby Ambassador アクセスを許可します。このようなアカウントでは、Lobby Ambassador に許可されている機能は、ゲスト資格情報を作成して、Web ポリシーが WLAN に設定されたコント ローラに割り当てることだけです。

管理システム内の多くの設定タスクと同様に、ゲスト資格情報はテンプレートを使用して作成されま す。次にいくつかの新しいゲストユーザ テンプレートのオプションおよび機能を示します。

- ゲストテンプレートには、2種類あります。1つは、有効期間を制限するかまたは無制限にした、 即時のゲストアクセスをスケジューリングするためのゲストテンプレートです。もう1つは、管理者が「将来の」ゲストアクセスをスケジューリングして、曜日と時間帯によるアクセス制限を 提供します。
- このソリューションにより、管理者はゲストユーザに資格情報をEメールで送信できるようになります。さらに、「スケジュール」ゲストテンプレートが使用されると、アクセスが提供される新しい日(間隔)ごとに、資格情報が自動的にEメールで送信されます。

(ゲスト) WLAN SSID および管理システムのマッピング情報(キャンパス/ビルディング/フロアの場所)に基づくか、または WLAN SSID および特定のコントローラまたはコントローラのリストに基づいて、ゲスト資格情報を WLC に適用できます。後者の方法は、この章で説明するように、ゲスト モビリティ アンカー方式でゲスト アクセスを展開する場合に使用されます。

Lobby Ambassador がゲスト テンプレートを作成すると、ゲスト アクセス トポロジに応じて1つ以上 のコントローラに適用されます。「Web」ポリシーで設定した WLAN を持つコントローラだけが、適用 可能なテンプレートの候補コントローラとして一覧表示されます。これは、ゲスト テンプレートを管 理システムのマップ ロケーションの基準に基づいてコントローラに適用する場合にも当てはまります。

適用されたゲスト資格情報は、(アンカー) WLC 上にローカルに保存され([Security]>[Local Net Users])、ゲスト テンプレートで定義された「ライフタイム」変数の期限までそこで保持されます。資格情報の有効期限が切れている場合でも、無線ゲストがアソシエートされアクティブな場合は、WLC がトラフィック転送を停止してそのユーザの WEBAUTH_REQD ポリシー状態に戻ります。ゲスト資格情報が(コントローラに)再適用されない場合、そのユーザは二度とネットワークにアクセスすることができません。



ゲスト資格情報に関連付けられたライフタイム変数は、WLAN セッション タイムアウト変数とは無関 係です。WLAN セッション タイムアウトの時間を過ぎてもユーザが接続したままの場合は、認証が解 除されます。その後、ユーザは、Web ポータルにリダイレクトされ、資格情報の有効期限が切れてい ない場合には、再度アクセスするためにログインをやり直す必要があります。面倒な認証のリダイレク トを避けるには、ゲスト WLAN セッション タイムアウト変数を適切に設定する必要があります。

ローカル コントローラのロビー管理者のアクセス

中央集中型 WCS 管理システムが展開されていないか使用できない場合、ネットワーク管理者は、ロ ビー管理者の特権だけを付与したローカル管理者のアカウントをアンカー コントローラ上に設定でき ます。ロビー管理者のアカウントを使用してコントローラにログインしたユーザは、ゲスト ユーザ管 理機能にアクセスできます。ローカル ゲスト管理で使用可能な設定オプションは、管理システムを通 して使用可能な機能とは対照的に、限られています。次のオプションが含まれます。

- ユーザ名
- 生成パスワード
- 管理者割り当てパスワード
- 確認パスワード
- 有効期間:日:時:分
- SSID
- レイヤ 3 Web ポリシー認証用に設定された WLAN だけを表示
- 説明

管理システムによってコントローラに適用された資格情報は、管理者がコントローラにログインしたと きに表示されます。ローカルのロビー管理者のアカウントには、管理システムによって以前に作成され たゲスト資格情報を変更または削除する特権が与えられます。WLC上でローカルに作成されるゲスト 資格情報は、コントローラの設定が管理システムで更新されない限り、管理システムに自動的に表示さ れません。WLC設定の更新の結果として管理システムにインポートされる、ローカルに作成されるゲ スト資格情報は、編集してWLCに再適用できる、新しいゲストテンプレートとして表示されます。

ゲスト ユーザの認証

「ゲスト資格情報の管理」(P.10-10) で説明したように、管理者が管理システムまたはコントローラ上 でローカルのアカウントを使用してゲスト ユーザ資格情報を作成した場合は、それらの資格情報は、 コントローラ上でローカルに保存されます。そのコントローラは、中央集中型ゲスト アクセス トポロ ジの場合、アンカー コントローラとなります。

無線ゲストが Web ポータルを通してログインした場合、コントローラは次の順番で認証を処理します。

- **1.** コントローラが、ユーザ名とパスワードをローカル データベースでチェックし、そこに存在すれば、アクセスを許可します。
- ユーザ資格情報が見つからなかった場合は、次のように処理されます。
- コントローラが、外部 RADIUS サーバがゲスト WLAN 用に設定されているかどうかチェックします(WLAN 構成設定の下)。そのように設定されている場合は、コントローラが、そのユーザ名とパスワードで RADIUS アクセス要求パケットを作成し、選択された RADIUS サーバに転送して認証します。

特定の RADIUS サーバがゲスト WLAN 用に設定されていない場合は、次のように処理されます。

 コントローラが、グローバルな RADIUS サーバの設定をチェックします。「ネットワーク」ユーザ を認証するように設定されたすべての外部 RADIUS サーバは、ゲスト ユーザ資格情報を使用して 照会されます。それ以外では、どの RADIUS サーバでも「ネットワーク ユーザ」がオンになって おらず、また上記1または2でユーザが認証されていない場合、認証は失敗します。

(注) RADIUS サーバは、[WLC Security] > [AAA] > [RADIUS] 設定でネットワーク ユーザのチェックボッ クスがオフになっている場合でも、ネットワーク ユーザ認証をサポートするために使用できます。た だし、これを実現するには、サーバが特定の WLAN の [Security] > [AAA Servers] 設定で明示的に選 択されている必要があります。

外部認証

WLC およびゲスト アカウント管理(Lobby Ambassador)機能は、WLC 上のローカル認証用にゲス ト ユーザ資格情報を作成して適用するためだけに使用できます。ただし、既存のゲスト管理/認証ソ リューションが、有線ゲスト アクセスまたは NAC ソリューションの一部として、すでに企業に展開さ れている場合があります。その場合は、ゲスト ユーザの認証で説明したように、Web ポータル認証を外 部 RADIUS サーバに転送するようにアンカー コントローラ/ゲスト WLAN を設定できます。

コントローラが Web ユーザを認証するために使用するデフォルトのプロトコルは、パスワード認証プ ロトコル (PAP) です。外部 AAA サーバに対して Web ユーザを認証している場合は、そのサーバが サポートしているプロトコルを確認する必要があります。また、Web 認証に CHAP または MD5-CHAP を使用するようにアンカー コントローラを設定できます。Web 認証プロトコル タイプは、 WLC のコントローラ設定で設定されます。

Cisco Secure ACS と Microsoft ユーザ データベースを使用した外部認証

ゲストアクセスの展開で、ゲストユーザの認証に Cisco ACS とともに Microsoft ユーザ データベース の使用を検討している場合は、次の Cisco ACS 設定に関する注意事項を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/ins tallation/guide/windows/postin.html

特に、次の URL を参照してください。

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.0/ins tallation/guide/windows/postin.html#wp1041223

ゲスト パススルー

無線ゲストアクセスのもう1つの形態は、ユーザ認証をすべて省略して、オープンアクセスを可能に することです。ただし、企業は、アクセスを許可する前に利用規定または免責条項のページをユーザに 表示することが必要になる場合があります。そのような場合は、Web ポリシーをパススルーするよう にゲスト WLAN を設定できます。このシナリオでは、ゲストユーザが、免責情報を含むポータル ページにリダイレクトされます。

また、パススルー モードには、ユーザが接続する前に E メール アドレスを入力するオプションもあり ます(サンプル ページについては、図 10-6 および図 10-7 を参照)。設定例については、「ゲスト アク セスの設定」(P.10-13)を参照してください。

	义	10-6	Welcome AUP ページのパススルー
--	---	------	-----------------------

🥭 Web Authentication - Windows Internet Explorer		_ 8 ×
🚱 🕞 👻 https://1.1.1.1/login.html?redirect=www.yahoo.com/	💌 🔒 🦘 🗙 Google	- ۹
😪 🕸 🏉 Web Authentication	🚹 • 🗟 - 🖶 • 🖻	Page - 🕥 Tools - »
Connect		*
Welcome to the Cisco wireless network Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please logical and put your air space to work.		
L ₂		

図 10-7 E メールを含むページのパススルー

Guest	Users Details	E-mail Print Back
	Email To Subject Send Cancel	
Cr	edentials for Guest User Gu	est1
Guest User Name	Guest1	
Password	test	
Profile	Guest	
Start Time	8: 17: 07/19/2007	
End Time	9: 0: 07/19/2007	
Disclaimer	Guests understand and acknowledge to exercise no control over the nature, cor reliability of the information and/or data through our network.	hat we ntent or passing

ゲスト アクセスの設定

この項では、Cisco Unified Wireless Network ソリューション内で無線ゲスト アクセス サービスを有効 にする方法について説明します。設定作業では、Web ブラウザを使用する必要があります。コント ローラとの Web セッションは、次のコントローラの管理 IP アドレスへの HTTPS セッションを開くこ とによって、確立されます。https://management_IP またはオプションでコントローラのサービス ポート IP アドレス。

次の手順では、アンカー WLC を除き、コントローラと LAP のインフラストラクチャがすでに展開さ れているものとします。詳細については、「アンカー コントローラ展開ガイドライン」(P.10-6)を参 照してください。 <u>》</u> (注)

この項で説明する設定手順は、記載された順序に従って実行することを推奨します。

設定セクション全体を通じて、次の用語が使用されます。

- 外部 WLC:企業のキャンパス全体またはブランチ ロケーションに展開され、AP のグループの管理および制御に使用される1つ以上のWLCを指します。外部コントローラが、ゲスト WLAN を ゲスト モビリティ EoIP トンネルにマッピングします。
- アンカー WLC:企業 DMZ 内に展開され、ゲスト モビリティ EoIP トンネル終端、Web リダイレ クション、およびユーザ認証を実行するために使用される1つ以上の WLC を指します。



この項では、特定の設定画面キャプチャの関連する部分だけを示します。

Cisco Unified Wireless Network ゲスト アクセス ソリューションの実装は、次の設定カテゴリに分類で きます。

- アンカー WLC の設置およびインターフェイス設定:ここでは、1 つ以上のアンカー WLC の実装 に関する設置の要件、手順、および注意点について簡単に説明します。既存の Cisco Unified Wireless Network 展開にゲスト アクセスを初めて実装する場合、アンカー WLC は通常、企業 ネットワークのインターネット エッジに設置される新しいプラットフォームです。
- モビリティグループの設定:ここでは、外部 WLC が、1 つ以上のゲスト アンカー WLC への EoIP トンネルの起点となるように設定する必要があるパラメータについて説明します。モビリ ティグループの設定自体で EoIP トンネルが作成されるわけではなく、ゲスト アクセス WLAN サービスをサポートするために、外部 WLC とアンカー WLC 間のピア関係が確立されます。
- ゲスト WLAN の設定: ゲスト WLAN (外部 WLC を起点とする) をアンカー WLC にマッピング するのに必要な WLAN 固有の設定パラメータに焦点を当てます。ゲスト アクセス ソリューション の設定のこの部分において、外部 WLC とアンカー WLC 間に EoIP トンネルが作成されます。こ こでは、Web ベースの認証のレイヤ 3 リダイレクションを起動するために必要な設定についても 説明します。
- ゲストアカウント管理:ここでは、コントローラまたはアンカーWLCのロビー管理者インター フェイスを使用して、アンカーWLCでローカルにゲストユーザ資格情報を設定および適用する方 法の概要について説明します。
- その他の機能とソリューションオプション:次のような、設定が可能なその他の機能について説 明します。
 - Web ポータル ページの設定と管理
 - 外部 Web リダイレクションのサポート
 - 事前認証 ACL
 - アンカー WLC DHCP の設定
 - 外部 RADIUS 認証
 - 外部アクセス コントロール

アンカー WLC の設置およびインターフェイスの設定

「アンカー コントローラの位置決め」(P.10-6) で説明したように、アンカー WLC は、ゲスト アクセ スだけに使用して、社内の LAP の制御および管理には使用しないことを推奨します。 この項では、アンカー WLC 上のインターフェイス設定のすべてを扱っているわけではありません。読 者は、初期ブート時に必要な、シリアル コンソール インターフェイスを使用した WLC の初期化と設 定プロセスに精通していることを前提とします。

この項では、ゲストアクセストポロジ内にアンカーとして展開する WLC 上でのインターフェイスの 設定に関する特定の情報と注意事項を記載します。

シリアル コンソール インターフェイスを使用した初期設定の一環として、次の3つの静的インターフェイスを定義する必要があります。

- コントローラ管理:このインターフェイス/IPは、ネットワーク上の他のコントローラとの通信に 使用されます。また、外部コントローラを起点とする EoIP トンネルの終端にも使用されるイン ターフェイスです。
- AP マネージャインターフェイス: AP 管理にコントローラを使用しない場合でも、このインターフェイスは設定する必要があります。シスコでは、管理インターフェイスと同じ VLAN およびサブネット上に、AP マネージャインターフェイスを設定することを推奨します。
- 仮想インターフェイス:コントローラのクイックスタートインストールマニュアルでは、1.1.1.1 などのアドレスの仮想 IP を定義するように推奨されています。このアドレスは、同じモビリティ グループのメンバであるすべてのコントローラで同じアドレスにする必要があります。また、仮想 インターフェイスは、コントローラがクライアントを Web 認証のためにリダイレクトするときの ソース IP アドレスとしても使用されます。

ゲスト VLAN インターフェイスの設定

前述したインターフェイスは、コントローラに関連付けられた動作と管理機能に使用されます。ゲスト アクセス サービスを実装するには、もう1つのインターフェイスを定義する必要があります。これは、 ゲスト トラフィックをインターネットにルーティングするためのインターフェイスです。「アンカー コ ントローラの位置決め」(P.10-6) で説明したように、ゲスト インターフェイスは、ファイアウォール 上のポートに接続される場合と、インターネット境界ルータ上のインターフェイスに切り替えられる場 合があります。

新しいインターフェイスの定義

次の手順を実行して、ゲスト トラフィックをサポートするインターフェイスを定義および設定します。

- **ステップ1** [Controller] タブをクリックします。
- **ステップ2** 左側のペインで、[Interfaces] をクリックします(図 10-8 を参照)。

図 10-8

8 コントローラ インターフェイス

ululu cisco		VLANS CONTROLLE	ER WIRELESS	SECURITY	MANAGEMENT CO	Saye Conf MMANDS	iguration <u>P</u> ing HELP	Logout <u>R</u> efre
Controller	Interfaces							New
General	Interface Na	ame	VLAN Identifier	IP Address	Interface Type	Dynamic	AP Management	
Inventory Interfaces Network Routes	ap-manager		9	10.15.9.253	Static	Enabled		
	management		9	10.15.9.11	Static	Not Suppo	rted	
	service-port		N/A	172.28.217.13	31 Static	Not Suppo	rted	
Internal DHCP Server	virtual		N/A	1.1.1.1	Static	Not Suppo	rted	
Mobility Management								

ステップ3 [New] をクリックします。

インターフェイス名と VLAN ID の定義

ステップ4 インターフェイス名と VLAN ID を入力します。(図 10-9 を参照)。

図 10-9

インターフェイス名と VLAN ID

ahaha									Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	Interface	s > New						< Back	Apply
General	Interface	Name g	uest-dmz						
Inventory Interfaces	VLAN Id	3	1						
Network Routes									
Internal DHCP Server Mobility Management									

インターフェイス プロパティの定義

ステップ 5 次のプロパティを定義します。

- インターフェイス IP
- マスク
- ゲートウェイ(アンカーコントローラに接続されたファイアウォールまたはネクストホップルー タの場合)
- DHCP サーバ IP (外部 DHCP サーバを使用している場合は、[Primary DHCP Server] フィールドのそのサーバの IP アドレスを使用します)。

図 10-10を参照してください。

ahaha						Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout <u>R</u> efres
CISCO	MONITOR WLA		R WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	Interfaces > E	dit					< Back	Apply
General Inventory	General Inform	nation						
Interfaces Network Routes	Interface Name MAC Address	guest 00:0b	dmz :85:40:7e:e0					
Internal DHCP Server Mobility Management	Interface Addr	ess						
Spanning Tree Ports	VLAN Identifier	31	20.31.11					
Master Controller Mode	Netmask	25	5.255.255.0					
Network Time Protocol	Gateway	10	20.31.1					
▶ QoS	Physical Inform	nation						
▶ CDP	Port Number	1						
	Backup Port	0						
	Active Port	0						
	Enable Dynamic Management	AP 🔲						
	Configuration							
	Quarantine							
	DHCP Informat	ion						
	Primary DHCP S	Server 10	20.30.11					
	Secondary DHC	P Server						

図 10-10 インターフェイス プロパティの定義

(注)

DHCP サービスをアンカー コントローラ上でローカルに実装する必要がある場合は、[Primary DHCP Server] フィールドにコントローラの管理 IP アドレスを入力します。ゲスト N+1 冗長性が DMZ に実装されている場合、展開されている追加のアンカー WLC ごとに、上記のインターフェイス設定を繰り返します。

モビリティ グループの設定

次のデフォルトのモビリティ グループ パラメータは、標準の中央集中型 WLAN 展開の一部として、 外部 WLC に定義しておく必要があります。ゲスト アクセスの自動アンカー モビリティをサポートす るには、モビリティ グループ ドメイン名でアンカー WLC も設定する必要があります。

アンカー WLC のデフォルト モビリティ ドメイン名の定義

アンカー WLC のデフォルト モビリティ ドメイン名を設定します。アンカーのモビリティ ドメイン名 は、外部 WLC に設定した名前と異なる必要があります。以下の例では、企業の無線展開にアソシエー トされている WLC (外部コントローラ) は、すべてモビリティ グループ「SRND」のメンバです。一 方、ゲスト アンカー WLC は、別のモビリティ グループ名「ANC」で設定されます。これは、企業の 無線展開にアソシエートされているプライマリ モビリティ ドメインから、アンカー WLC を論理的に 区別しておくために行われます。

- **ステップ1** [Controller] タブをクリックします。
- ステップ 2 [Default Mobility Domain Name] フィールドに名前を入力します。
- **ステップ3** [Apply] をクリックします。(図 10-11 を参照)。

uluili. cisco	MONITOR WLANS	ONTROLLER	WIRELESS ;	SECURITY	MANAGEMENT	Saxe Co C <u>O</u> MMANDS	nfiguration <u>P</u> in HELP	ig Logout <u>R</u> efre
Controller	General							Apply
General Inventory Interfaces Network Routes Internal DHCP Server Mobility Management Spanning Tree Ports Master Controller Mode Network Time Protocol QOS CDP	802.3x Flow Control Mod LWAPP Transport Mode LAG Mode on next reboo Ethernet Multicast Mode Broadcost Forwarding Aggressive Load Balanci Peer to Peer Blocking Mo Over The Air Provisionini AP Fallback Apple Talk Bridging Fast SSID change Default Mobility Domain I RF-Network Name User Idle Timeout (seconds)	te ng ode g of AP Name nds)	Disabled w Layer 3 w Disabled w Disabled w Disabled w Enabled w Disabled w		(Curre (LAG M	nt Operating Mo Aode is currently	rde is Layer3) r disabled).	
	Web Radius Authentication 802.3 Bridging	on	CHAP V Disabled V					
	Operating Environment Internal Temp Alarm Lim	nits	Commercial (0 to 65 C	to 40 C)				

図 10-11 アンカー WLC 上のデフォルト モビリティ ドメイン名の定義

アンカー WLC のモビリティ グループ メンバの定義

ゲスト WLAN をサポートする企業での展開内のすべての外部 WLC は、ゲスト アンカー WLC のモビ リティ グループ メンバとして定義する必要があります。

- **ステップ1** [Controller] タブをクリックします。
- **ステップ 2** 左側のペインで、[Mobility Management] をクリックし、[Mobility Groups] をクリックします。 (図 10-12 を参照)。
 - 図 10-12 モビリティグループメンバの定義

ababa							Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS SECURI	TY MANAGEMENT	COMMANDS	HELP	
Controller	Static Mobility Gro	up Members				New	EditAll
General	Default Mobility G	roup SRND					
Inventory Interfaces Network Routes Internal DHCP Server Mobility Management	MAC Address	IP Address	Group Name				
	00:0b:85:40:7e:e0	10.15.9.11	(Local)				
	00:0b:85:40:23:a0	10.15.9.14	SRND				
	00:0b:85:40:40:00	10.20.2.2	SRND				
Mobility Groups	00:0b:85:40:41:40	10.20.2.3	SRND				6
Mobility Statistics	00:0b:85:40:7f:c0	10.20.110.254	SRND				2

モビリティ グループ メンバとして外部コントローラを追加

ステップ3 [New] をクリックして、ゲスト アクセス WLAN をサポートする各外部コントローラの MAC と IP ア ドレスを定義します。(図 10-13 を参照)。 図 10-13 アンカー WLC への外部コントローラの追加

ululu cisco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration Ping HELP	Logout <u>R</u> efresh	
Controller	Mobility G	Group Me	ember > New					< Back	Apply	
General	Member IP	Address								
Interfaces	Member M/	AC Addres	s							
Network Routes	Group Nam	e	SRND							
Internal DHCP Server										64
Mobility Groups										2218



上に示した図 10-13 の [Group Name] は、外部 WLC の [Default Mobility Domain Name] で設定され る名前です。これは、アンカー WLC に使用される名前と異なる必要があります。メンバの IP アドレ スと MAC アドレスは、外部 WLC の管理インターフェイスにアソシエートされたアドレスです。ゲス ト WLAN をサポートする追加の各外部 WLC に対して、上記の手順を繰り返します。複数のアンカー が展開されている場合(ゲスト N+1 冗長性)、アンカー WLC のデフォルト モビリティ ドメイン名の 定義とアンカー WLC のモビリティ グループ メンバの定義の手順を繰り返します。

外部 WLC のモビリティ グループ メンバとしてアンカー WLC を追加

無線ゲストアクセスをサポートする自動アンカーモビリティで説明したように、各外部 WLC は、ア ンカー WLC 上で終端する EoIP トンネルにゲスト WLAN をマッピングします。そのため、アンカー WLC は、各外部コントローラのモビリティ グループのメンバとして定義する必要があります。下の例 で、アンカー WLC のグループ名エントリが「ANC」で(「アンカー WLC のモビリティ グループメン バの定義」(P.10-18) を参照)、企業の無線展開を構成しているもう一方の WLC がモビリティ グルー プ「SRND」のメンバであることに注意してください。

- **ステップ1** [New] をクリックして、アンカー WLC の IP、MAC アドレス、およびグループ名をモビリティ メンバ テーブルに追加します。
- **ステップ2** 追加の外部コントローラごとにこの手順を繰り返します (図 10-14 を参照)。

ahaha						guration Ping	Logout Refresh
cisco	MONITOR WLANS		WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	Static Mobility Gr	oup Members				New	EditAll
General	Default Mobility	Group SRND					
Inventory	MAC Address	IP Address	Group Name				
Interfaces	00:18:73:44:f6:a0	10.15.9.19	(Local)				
Internal DHCP Server	00:0b:85:40:23:a0	10.15.9.14	SRND				
▼ Mobility Management	00:0b:85:40:40:00	10.20.2.2	SRND				
Mobility Groups	00:0b:85:40:41:40	10.20.2.3	SRND				
Mobility Anchor Config Mobility Statistics	00:0b:85:40:7e:e0	10.15.9.11	ANC				
Spanning Tree	00:0b:85:40:7f:c0	10.20.110.254	SRND	•			
Ports	00:0b:85:40:80:00	10.15.9.12	SRND				
Master Controller	00:0b:85:40:8a:a0	10.15.9.13	SRND				
Mode	00:18:73:45:07:40	10.15.9.17	SRND				
Network Time	00:18:73:45:28:80	10.15.9.20	SRND	•			
Protocol	00:18:73:45:39:00	10.15.9.18	SRND				
▶ QoS	00:d0:2b:fc:28:40	10.20.100.254	SRND				
▶ CDP							

図 10-14 外部 WLC へのアンカー コントローラの追加

222544



ゲスト N+1 冗長性機能が展開されている場合、2 つ以上のアンカー WLC エントリが各外部 WLC のモ ビリティ グループ メンバ リストに追加されます。

ゲスト WLAN の設定

この項では、単一のゲスト WLAN の設定方法について説明します。ゲスト WLAN は、ゲスト アクセ スが必要な AP を管理するすべての外部 WLC 上で設定します。アンカー WLC が明らかにゲスト WLAN にアソシエートされた LAP の管理に使用されない場合でも、アンカー WLC は、ゲスト WLAN を使用して設定する必要があります。なぜならば、アンカー WLC は、WLAN の論理拡張機能 で、そこでユーザ トラフィックがアンカー WLC 上のインターフェイス/VLAN に最終的にブリッジさ れるためです (AP と外部コントローラ間では CAPWAP、外部コントローラとアンカー コントローラ 間では EoIP を使用)。 <u>》</u> (注)

(WLAN Security]、[QoS]、および [Advanced] 設定タブで定義する ナベてのパラメータは、アンカー および外部 WLC の両方で 同じ設定にする必要があることに注意することが非常に重要です。図 10-15 は、以下で説明する WLAN 設定のハイレベルの概略図を示しています。



(注)

[WLAN Security]、[QoS]、および [Advanced] 設定タブで定義するパラメータは、アンカーおよび外部コントローラの両方で同じ設定にする必要があります。

外部 WLC:ゲスト WLAN の設定

ステップ1 [WLANs] タブをクリックして、[New] をクリックします。(図 10-16 を参照)。

図 10-16 ゲスト WLAN の設定

սիսիս cisco	MONITOR WLANS CO	NTROLLER WIR	ELESS SECURITY MANAG	Sa IEMENT C <u>O</u> MMA	we Configuration <u>P</u> ing Logout NDS HELP	<u>R</u> efres
WLANs	WLANs				New	
WLANS	Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies	
AP Groups VLAN	CCKM	3	CCKM	Enabled	[WPA2][Auth(802.1X + CCKM)]	
	* WLAN IDs 9-16 will not be	3 nushed to 11xx, 12	CCKM	Enabled	[WPA2][Auth(802.1X + CCKM)]	

ゲスト WLAN SSID の定義

- ステップ2 将来のゲストユーザが、直感的に理解できるか、または認識しやすい SSID を定義します。
 コントローラで自動的に VLAN ID を割り当てます。管理者は、他の SSID/WLAN で使用されていなければ、1~16の ID を選択できます。
- ステップ 3 [Profile Name] を指定します。
- **ステップ4** [Apply] をクリックします。(図 10-17 を参照)。

図 10-17 ゲスト WLAN SSID の定義

սիսիս						Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	WLAN ID	1 💌						
AP Groups VLAN	Profile Name	Guest Acces	55					
	WLAN SSID	Guest						

新しい WLAN の作成後に、図 10-18 に示すように、設定ページが表示されます。



図 10-18 WLAN の設定ページ

(注) ゲスト WLAN のために外部 WLC によって使用されるデフォルト インターフェイスは、管理インターフェイスです。EoIP トンネルがアンカーによって確立できない場合、外部コントローラは、以前に到達不能なアンカーとアソシエートされていた無線クライアントのアソシエーションを解除してから新しいクライアントを割り当て、外部ゲスト WLAN 自体の下で設定されたインターフェイスにクライアントを再度アソシエートします。このため、外部のゲスト WLAN をルーティング不可能なネットワークにリンクするか、あるいは到達不能 IP アドレスを持つ管理インターフェイスの DHCP サーバを設定することを推奨します。アンカーが到達不能になった場合、管理ネットワークへのゲスト クライアントのアクセスを防止します。

ゲスト WLAN のパラメータおよびポリシーの定義

[General Configuration] タブで、次の手順を実行します。

- ステップ1 [WLAN Status] の隣のボックスをクリックして WLAN を有効にします。
- **ステップ 2** ゲスト アクセスをサポートする帯域を制限する場合は、必要に応じて、無線ポリシーを設定します。
 - a. [Broadcast SSID] はデフォルトで有効になるので、有効なままにします。
 - **b.** デフォルトでは、WLAN は WLC の [management] インターフェイスに割り当てられます。これは変更しないでください。

ステップ3 [Security] タブをクリックします (図 10-19 を参照)。

図 10-19 ゲスト WLAN の一般ポリシーの定義

սիսիս cisco	MONITOR WLANS CO	Save Configuration <u>P</u> ing Logout <u>B</u> efrest NTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit General Security Profile Name WLAN SSID WLAN Status Security Policies Radio Policy Interface Broadcast SSID	Q95 Advanced Q95 Advanced Guest Guest Image: Control of the second secon

ステップ4 レイヤ2セキュリティを、デフォルトの設定(802.1x WPA/WPA2)から[none]に設定します (図 10-20 を参照)。

図 10-20 WLAN のレイヤ 2 セキュリティ設定

սիսիս									Logout <u>R</u> efre	
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP		
WLANS WLANS WLANS AP Groups VLAN	WLANs > General Layer Laye	Edit Secur 2 Lay r 2 Security	ity QoS er 3 AAA Se None MAC Filterin	Advanced ervers				< Back	Apply	~

ステップ 5 [Layer 3] タブをクリックします (図 10-21 を参照)。

図 10-21	ゲスト WLAN のレイヤ 3 セキュリティ設定

սիսիս	Sa <u>v</u> e Cor	figuration
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	HELP
WLANs	WLANs > Edit	< Ba
* WLANS	General Security QoS Advanced	
WLANS AP Groups VLAN	Layer 2 Layer 3 AAA Servers	
	Layer 3 Security None	
	Web Policy 2	
	Authentication Passthrough	
	Preauthentication ACL	

- ステップ6 [Web Policy] チェックボックスをオンにします(追加オプションのリストが表示されます)。
 WLC が認証前にクライアント間で DNS トラフィックを受け渡しすることを示す、警告のダイアログボックスが表示されます。
- **ステップ7** Web ポリシーに [Authentication] または [Pass-through] を選択します (「ゲストユーザの認証」 (P.10-12) を参照)。

S,

- (注) 事前認証 ACL は、認証されていないクライアントが、認証前に特定のホストまたは URL の宛先に接続することを許可する ACL を適用するために使用できます。ACL は、[Security] > [Access Control Lists] で設定されます。事前認証 ACL が Web 認証ポリシーとともに使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト/URL に解決して接続することができなくなります。
- **ステップ8** [QoS] タブを選択します(図 10-22 を参照)。

cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration Ping	Logout <u>R</u> efre
WLANS WLANS AP Groups VLAN	WLANs > Edit General Security Quality of Service (QoS	QoS Advanced	×			< Back	Apply
	WMM Policy 7920 AP CAC 7920 Client CAC	Disabled M Enabled Enabled					

図 10-22 ゲスト WLAN QoS 設定

ステップ9 オプションで、ゲスト WLAN にアップストリーム QoS プロファイルを設定します。デフォルトは 「Silver (Best Effort)」です。この例では、ゲスト WLAN は最低の QoS クラスに再割り当てされていま す。 図 10-23

ステップ 10 [Advanced] タブをクリックします。(図 10-23 を参照)。

ゲスト WLAN の高度な設定

cisco	MONITOR WLANS CONTR	OLLER WIRE	LESS <u>S</u> ECURITY	MANAGEMENT C	OMMANDS	HELP	
VLANS	WLANs > Edit General Security	QoS Advan	ced			< Back	Apply
WLANS AP Groups VLAN	Allow AAA Override H-REAP Local Switching ² Session Timeout (secs)	Enabled Enabled		DHCP Server		Override	
	Aironet IE Diagnostic Channel	Enabled		DHCP Addr. Assignm Management Frame I	nent 🗹 ; Protection	Required (MFP)	
	Override Interface ACL	None	~	Infrastructure MFP Protection	(Glo	bal MFP Disabled)	
	Client Exclusion 4	Enabled 6) meout Value (secs)	MFP Client Protection 2	Optional	~	

ステップ11 セッションタイムアウトを設定します(オプション)。

(注)

- セッション タイムアウトが 0(デフォルト)より大きくなると、有効期限後に強制的に認証が解除され、ユーザは Web ポータルで再認証を要求されます。
- ステップ 12 [DHCP Addr. Assignment] を [Required] に設定します。
 - <u>》</u> (注)

ゲスト ユーザが、静的 IP 設定を使用してゲスト ネットワークの使用を試みるのを防ぐため、[DHCP Addr. Assignment] を [Required] に設定することを推奨します。

ステップ 13 最後に、[Apply] をクリックします

ゲスト WLAN モビリティ アンカーの設定

- ステップ1 外部 WLC 上の [WLAN] メニューから、新しく作成されたゲスト WLAN を探します。
- ステップ2 右側のプルダウン選択リストから、[Mobility Anchors] を強調表示してクリックします (図 10-24 を 参照)。

ululu cisco	MONITOR WLANS	CONTROLLER WIR	ELESS SECURITY	Saya M <u>a</u> nagement C <u>o</u> mman	Configuration <u>P</u> ing	Logout <u>R</u> efree
WLANs	WLANs					New
WLANS	Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies	
AP Groups VLAN	Guest Access WLAN	1	Guest	Enabled	Web-Auth	
	CCKM	3	CCKM	Enabled	[WPA + WPA2][Auth	Remove
						Mobility Anchois
	* WLAN IDs 9-16 will i	not be pushed to 11xx, 1	2xx and 13xx model Al	Ps.		

図 10-24 WLAN モビリティ アンカー

- ステップ3 [Switch IP Address (Anchor)] プルダウン選択リストで、ネットワーク DMZ 内で展開されたアンカー WLC の管理インターフェイスに対応する IP アドレスを選択します。これは、「外部 WLC のモビリ ティ グループ メンバとしてアンカー WLC を追加」(P.10-19) で設定されたものと同じ IP アドレスで す。
- **ステップ 4** [Mobility Anchor Create] をクリックします (図 10-26 を参照)。

図 10-25 [Switch IP Address (Anchor)] からの管理インターフェイスの選択

	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	Sage Configuration E COMMANDS HELP	ing Logout Befree
WLANs	Mobility Anchors				< Back
* WLANS	WLAN SSID Guest				
AP Groups VLAN	Switch IP Address (Anchor)		Data Path	Control Path	
	Nobility Anchor Create				
	Switch IP Address (Anchor)	10.15.9.19(local) × 10.15.9.19(local) 10.15.9.14 10.20.2.2 10.20.2.3 10.15.9.11 10.20.110.254 10.15.9.12 10.15.9.12			
		10.15.9.17 10.15.9.20 10.15.9.18 10.20.100.254			

図 10-26 WLAN モビリティ アンカーの選択

. cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT	Sa <u>v</u> e Configuration . C <u>O</u> MMANDS HELP	<u>P</u> ing Logout <u>R</u> efresh
WLANs	Mobility Anchors			< Back
▼ WLANS WLANS AP Groups VLAN	WLAN SSID Guest Switch IP Address (Anchor)	Data Path	Control Path	
	Mobility Anchor Create			
	Switch IP Address (Anchor)			

ゲスト WLAN モビリティ アンカーの確認

設定されると、図 10-27 に示す画面には、ゲスト WLAN に割り当てられたモビリティ アンカー(上記 で選択)が表示されます。

図 10-27 ゲスト WLAN モビリティ アンカーの確認

սիսիս								<u>P</u> ing Logout <u>R</u> efres
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
WLANs	Mobility Anchors							< Back
WLANS	WLAN SSID G	uest						
AP Groups VLAN	Switch IP Address	(Anchor)			Data Path	Cont	rol Path	
	10.15.9.11				up	up		
	Mobility Anch	or Create						
	Switch IP Address	(Anchor)	10.15.9.19	(local) 🔽				

確認作業を容易にするために、ページには、モビリティトンネルデータパスと CAPWAPP 制御パス がアンカーで設定されているかどうかが表示されます。両方または片方が「down」と表示されている 場合には、「ゲストアクセスのトラブルシューティング」(P.10-57)でトラブルシューティングのヒン トを参照してください。右側のプルダウン選択リストには、宛先アンカー WLC に ping を送信するオ プションがあります。

- **ステップ 5** 終了する場合は、[Back] をクリックします。
- ステップ 6 展開されている追加の各アンカー WLC (ゲスト N+1 冗長性) に対して、上記の手順を繰り返します。

これで、ゲスト WLAN の設定は終了です。ゲスト WLAN をサポートする追加の各外部 WLC に対し て、外部 WLC: ゲスト WLAN の設定からゲスト WLAN モビリティ アンカーの確認のすべての手順 を繰り返します。

アンカー WLC 上でのゲスト WLAN の設定

アンカー コントローラ上でのゲスト WLAN の設定は、WLAN インターフェイスおよびモビリティアンカー設定(以下で詳細を説明)で多少の違いがある点を除き、外部コントローラの設定と同じです。

(注)

ゲスト WLAN に定義する SSID は、外部 WLC 上で定義される SSID とまったく同じにする必要があります。

アンカー WLC:ゲスト WLAN インターフェイス

上記のように、アンカー WLC 上でゲスト WLAN に設定するパラメータは、WLAN がマッピングされ るインターフェイスを除いて同じです。この場合、ゲスト WLAN はアンカー WLC 上でインターフェ イスまたは VLAN に割り当てられ、アンカー WLC によってファイアウォール上のインターフェイス またはインターネット境界ルータに接続されます。

- **ステップ1** [WLANs] タブをクリックします。
- **ステップ 2** 次の点を除いて、外部 WLC 上で設定した場合と同様に、ゲスト WLAN を作成、設定、および有効化します。

WLAN の一般的な設定の [Interface] で、ゲスト VLAN インターフェイスの設定で作成されたインター フェイス名を選択します (図 10-28 を参照)。

ステップ 3 [Apply] をクリックします。

図 10-28 アンカー WLC ゲスト WLAN インターフェイスの設定



アンカー WLC:ゲスト WLAN モビリティ アンカーの定義

外部 WLC とは設定が異なる 2 つ目のパラメータは、WLAN モビリティ アンカー設定です。ゲスト WLAN モビリティ アンカーは、アンカー WLC 自体です。

- **ステップ1** [WLANs] タブをクリックします。
- **ステップ2** ゲスト WLAN を探して、[Mobility Anchors] をクリックします。
- **ステップ3** プルダウン選択リストから、アンカー コントローラを表す IP アドレスを選択します。この IP アドレ スの隣に「(Local)」と表示されています。
- **ステップ 4** [Mobility Anchor Create] をクリックします。 (図 10-29 を参照)。

図 10-29 ゲスト WLAN モビリティ アンカーの定義

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT	COMMANDS HELP	Rud rodors Feue
WLANs	Mobility Anchors			< Back
WLANS AP Groups VLAN	Switch IP Address (Anchor) Hobility Anchor Create	Data Path	Control Path	
	Switch IP Address (Anchor) (10.15.9.11(local)	>		

ゲスト WLAN モビリティ アンカーは、ローカルであることに注意してください (図 10-30 を参照)。

図 10-30 ゲスト モビリティ アンカーの確認

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT	Sa <u>v</u> e Configuration	<u>P</u> ing Logout <u>R</u> efresh
WLANS	Mobility Anchors			< Back
WLANS AP Groups VLAN	Switch IP Address (Anchor)	Data Path	Control Path	
	Iocal Nobility Anchor Create Switch IP Address (Anchor) 10.15.9.14	up -	up	

ゲスト WLAN のモビリティ アンカーはアンカー WLC 自体なので、データとコントロール パスのス テータスは常に「up」と表示されます。「up」と表示されない場合、ローカル WLC をアンカーとして [Switch IP Address (Anchor)] ドロップダウン メニューから選択したことを確認します。

ステップ 5 ゲスト N+1 冗長性を実装している場合、展開されている追加のアンカー WLC ごとに WLAN の設定を 繰り返します。それ以外の場合、これでゲスト WLAN をアンカー WLC 上で作成するのに必要な設定 手順が完了します。

ゲスト アカウント管理

- ゲスト資格情報をローカルのアンカーコントローラ上で管理する場合は、次のいずれかの方法で 資格情報を作成して適用できます。
- Lobby Ambassador 管理者またはスーパー ユーザ/ルート管理者アカウントを使用する
- コントローラ上で直接、ローカルのロビー管理者アカウントまたは読み取り/書き込みアクセスで きるその他の管理アカウントを使用する

管理システムを使用したゲスト管理

次の設定例では、管理システム 4.1.83 以降がインストールおよび設定され、Lobby Ambassador のアカ ウントが作成されているものとします。

(注)

ゲスト テンプレートを作成する前に、個々の WLC 設定が管理システムと同期していることを確認し てください。

システム管理者が割り当てた Lobby Ambassador の資格情報を使用して管理システムにログインします (図 10-31 を参照)。

図 10-31 Lobby Ambassador



ログインすると、図 10-32 に示すような画面が表示されます。

図 10-32 Cisco Prime Infrastructure のロビー管理者インターフェイス

ahaha	Wireless Control Sys	stem	Usern	ame: lobbyadmin Logout	Refresh Print V	liew
cisco	Help 🖛					
Guest Users	Guest Users			Add Gu	est User 💌	GO
	User Name	Profile	Description	Applied To	Status	

(注)

Cisco Prime Infrastructure は、正式には WCS および NCS と呼ばれていました。

ゲスト テンプレートには、次の2種類があります。

- [Add Guest User] テンプレートを使用すると、管理者がゲスト資格情報を作成し、ただちに1つ以上のアンカー WLC に適用できます。
- [Schedule Guest User] テンプレートを使用すると、管理者が将来の月、日、時刻に1つ以上のアン カー WLC に適用されるゲスト資格情報を作成できます (図 10-33 を参照)。

図 10-33 ゲスト ユーザ テンプレート オプション

ababa	Wireless Control Sy	stem	Usern	ame: lobbyadmin Logout Refresh Print	View
cisco	Help 🖛				
Guest Users	Guest Users			Add Guest User 🛛 🖌	60
	User Name	Profile	Description	Applied Delete Guest User Schedule Guest User Print/Email User Details	-

ゲスト ユーザの追加テンプレートの使用

ステップ1 プルダウン選択リストから、[Add Guest User]を選択して [GO] をクリックします。

ステップ 2 図 10-34 に示すようなテンプレートが表示されます。

図 10-34 ゲスト ユーザの追加テンプレート

ababa	Wireless Control System	Username: lobbyadmin Logout Refresh Print View
cisco	Help ▼	
st Users	Guest Users > New User	
	Guest Information	
	User Name	
	Generate Password	
	Password	
	Confirm Password	
	Account Configuration	
	Profile	None
	Life Time	Limited O Unlimited
	End Time	16 W Hour 55 W Min. 07/19/07 💽 Day
	Apply To	Indoor Area
	Campus	Root Area 💌
	Building	None
	Floor	All Floors
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or
		Make this Disclaimer default
	Save Cancel	

図 10-35 は、ゲスト ユーザ アカウント作成の例を示しています。

ahaha	Wireless Control System	Username: lobbyadmin Logout Refresh Print View
cisco	Help 🕶	
uest Users	Guest Users > New User	
	Guest Information	
	User Name	guesti
	Generate Password	
	Password	•••••
	Confirm Password	•••••
	Account Configuration	
	Profile	Guest
	Life Time	
	End Time	8 💌 Hour 4 💌 Min. 07/20/07 🗔 Day
	Apply To	Controller List
		IP Address Name
		✓ 10.15.9.11 Controller1
		V 10.15.9.13 Controller3
		10.15.9.19 Controller9
	Description	Wireless Network Guest Ac
Disclaimer	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or
		Make this Disclaimer default
	Save Cancel	

図 10-35 ゲスト ユーザ アカウントの作成

ステップ3 [Guest Information] にユーザ名とパスワードを入力します。

パスワードは大文字と小文字が区別されます。ユーザ名は、24 文字以下に制限されています。管理者 には、[Generate Password] チェックボックスをオンにすることによって、パスワードの自動生成を許 可するオプションもあります。

- ステップ 4 [Account Configuration] で、次の項目を選択します。
 - [Profile]: プルダウン選択リストに、L3 Web ポリシーが設定された WLAN (SSID) のリストが 表示されます。
 - [Life Time]: [Limited] または [Unlimited] を選択します。
 - [End Time]: ゲストアカウントが [Limited] の場合、資格情報の有効期限が切れる月、日、時刻を 選択します。
 - [Apply To]: プルダウン選択リストから [Controller List] を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをオンにします。他に表示されるコントローラがありますが、これらは外部 WLC を表すことに注意してください。外部 WLC 上でユーザ資格情報を適用する必要はありません。認証強制ポイントがアンカー WLC であるからです。

(注)

図 10-35 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物理的/地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領域、屋内領域、ビルディング、フロアなどが含まれます。このロケーションベースのアクセス方法を使用できるのは、1) WLAN 展開が管理システム マッピング データベースに統合されている場合、2) ゲスト WLAN (Web ポリシーが設定された WLAN) がモビリティ アンカーを使用しない場合に限られます。

- [Description]:説明を入力します説明は、[Security]>[Local Net Users]で資格情報を適用するWLCに表示されます。これはゲストに送信できるEメールにも含まれ、ネットワークへのアクセスにどのような資格情報を使用するかを知らせます。
- [Disclaimer]: ゲスト ユーザに送信できる E メールで使用され、ネットワークへのアクセスにどの ような資格情報を使用するかを知らせます。
- **ステップ5** 完了したら、[Save] をクリックします。図 10-36 に示すサマリ画面が表示され、資格情報がアンカー コントローラに適用されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか Eメールで送信するオプションも表示されます。

図 10-36 ゲスト アカウントの正常な作成

ahaha	Wireless (Wireless Control System						
cisco	Help 🕶							
Users	Guest User	Account application result to t	the Selected controllers					
	IP Address	Controller Name	Operation Status	Reason				
	10.15.9.11	Controller1	Success	-				
	10.15.9.13	Controller3	Success					
			Guest User Credentials					
	Guest User Name	Guest1						
	Password	test						
	Profile	Guest						
	Start Time	8: 17: 07/19/2007						
	End Time	9: 0: 07/19/2007						
	Disclaimer	Guests understand and acknowledge and/or data passing through our netw	that we exercise no control over ork.	r the nature, content or reliability of	the information			
	Print/Email Gu	est User Credentials						

ステップ 6 [Print/Email Guest User Credentials] をクリックします。図 10-37 に示すような画面が表示されます。

Guest	Jsers Details E-ma
Cn	Email To
Guest User Name	Guest1
Password	test
Profile	Guest
Start Time	8: 17: 07/19/2007
End Time	9: 0: 07/19/2007
Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the information and/or data passing through our network.

図 10-37 ゲスト ユーザ詳細の印刷または E メールでの送信



ゲストアカウント情報のユーザへのEメール送信をサポートするように SMTP メール サーバを設定す る方法の詳細は、『Wireless Control System Configuration Guide』 (http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/WCS60cg.html) を参照して ください。

アカウントの詳細を印刷または E メールで送信すると、図 10-38 に示すような画面が表示されます。 [User Name] をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、[User Name] の隣のボックスをオンにしてプルダウン選択リストから [Delete Guest User] を選択することに より、ゲスト アカウントを削除できます。

図 10-38 Cisco Prime Infrastructure ゲスト ユーザのサマリ

CliSCO Help ~ Guest Users Add Guest User V 00 User Name Profile Description Applied To Status Guest Guest User Wireless Network Guest Access Controller List Active	ababa	Wir	eless Contro	ol System	Username: I	lobbyadmin Logout Re	sfresh Print	View
Guest Users Add Guest User V GO	cisco	Hel	p 🕶					
User Name Profile Description Applied To Status Guest1 Guest Wireless Network Guest Access Controller List Active	Guest Users	Gu	est Users			Add Guest U	ser 💌	GO
Guest Guest Wireless Network Guest Access Controller List Active			User Name	Profile	Description	Applied To	Status	
			Guest1	Guest	Wireless Network Guest Access	Controller List	Active	



ユーザがアクティブな状態で Cisco Prime Infrastructure からユーザ テンプレートを削除すると、その ユーザの認証が解除されます。

ゲスト ユーザのスケジュール テンプレートの使用

ゲストアカウントの設定の詳細は、『Wireless Control System Configuration Guide』 (http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcsadmin.html) を参照して ください。

図 10-39 は、ゲスト ユーザ テンプレート オプションを示しています。

図 10-39 ゲスト ユーザ テンプレート オプション

սիսիս	Wireless Control Sy	stem	Username: lobbyadmin	Logout Refresh Print View 📥
cisco	Help 🔻			
Guest Users	Guest Users			Schedule Guest User 🔽 GO
	User Name	Profile D	escription Applied	To Status

ステップ1 プルダウン選択リストから、[Schedule Guest User] を選択して [Go] をクリックします。 図 10-40 に示すようなテンプレートが表示されます。

図 10-40 ゲスト ユーザのスケジュール テンプレート

ababa	Wireless Control System	Username: lobbyadmin Logout Refresh Print View
cisco	Help ▼	
Guest Users	Guest Users > Scheduling	
	Guest Information	
	User Name	
		Generate new on every schedule
	Account Configuration	
	Profile	None
	Life Time	⊙ Limited ○ Unlimited
	Start Time	10 🗸 (Hours) 15 🖌 (Minutes) 07/19/07
	End Time	10 💙 (Hours) 15 💙 (Minutes) 07/20/07
		Days of the week
	Apply to	Indoor Area
	Campus	Root Area 👻
	Building	None
	Floor	All Floors
	Email credentials to	
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or
		Make this Disclaimer default
	Save Cancel	

図 10-41 は、ゲスト ユーザ アカウントのスケジュールの作成例を示しています。

abab	Wireless Control System	Username: lobbyadmin Logout Refresh Print View
cisco	<u>H</u> elp ▼	
lucst Users	Guest Users > Scheduling	
	Guest Information	
	User Name	test2
		Generate new on every schedule
	Account Configuration	
	Profile	Guest
	Life Time	 Limited Unlimited
	Start Time	8 Y (Hours) 0 Y (Minutes) 07/19/07
	End Time	17 V (Hours) 0 V (Minutes) 07/27/07
		Days of the week
	Apply to	Controller List
		IP Address Name
		✓ 10.15.9.11 Controller1
		✓ 10.15.9.13 Controller3
		10.15.9.19 Controller9
	Email credentials to	johndoe@crisco.com
	Description	Wireless Network Guest Ac
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or
		Make this Disclaimer default
	Save Cancel	

図 10-41 ゲスト ユーザ アカウントのスケジュールの作成

- ステップ2 [Guest Information] にユーザ名を入力します。ユーザ名の長さは、24 文字まで可能です。スケジュー ルベースのテンプレートを使用する場合、管理者には、アクセスが提供される新しい日ごとに、ユーザ 名が自動生成できるようになるオプションもあります。また、このテンプレートを使用する場合、ユー ザパスワードが自動生成されます。手動でパスワードを割り当てるオプションはありません。
- **ステップ3** [Account Configuration] で、次の項目を選択します。
 - [Profile]: プルダウン選択リストに、L3 Web ポリシーが設定された WLAN (SSID) のリストが 表示されます。
 - [Life Time]: [Limited] または [Unlimited] を選択します。
 - [Start Time]: アカウントがアクティブになる時刻、月、日を選択します。

(注)

開始時刻は、アカウントが作成される当日に開始することはできません。開始日は、アカウントが作成される日から1日以上過ぎている必要があります。

• [End Time]: アカウントが制限されている場合、終了時刻、月、日を選択します。



開始日から終了日までの期間は、30日を超えることはできません。

 [Days of Week]:アカウントの有効期間に応じて、管理者はアクセスできる曜日を管理できます。 アクセスが許可される曜日の隣のチェックボックスをクリックします。

<u>》</u> (注)

- [Days of the Week] が選択されている場合、開始および終了時刻は、それぞれの日のうちでアクセス可能な期間を表します。有効期限が切れるとその日のうちに、Cisco Prime Infrastructure は適用可能なコントローラから資格情報を削除します。アクセスが許可される新しい日/間隔ごとに、Cisco Prime Infrastructure によって新しいパスワード(必要に応じてユーザ名)が自動生成され、ゲストユーザに E メールで送信され、新しい資格情報が適用可能な WLC に再適用されます。[Days of the Week] が定義されていない場合、開始日時に基づいてアクセスが開始され、終了日時まで常にアクティブになります。
 - [Apply To]: プルダウン選択リストから [Controller List] を選択して、アンカー WLC を表すコントローラの隣にあるチェックボックスをオンにします。他に表示されるコントローラがありますが、これらは外部 WLC を表すことに注意してください。外部 WLC 上でユーザ資格情報を適用する必要はありません。認証強制ポイントがアンカー WLC であるからです。



- 図 10-41 に示すように、資格情報を適用できる場所には、ユーザがゲスト WLAN にアクセスできる物 理的/地理的ロケーションを制御できるなど、さまざまなオプションがあります。これには、屋外領 域、屋内領域、ビルディング、フロアなどが含まれます。このロケーションベースのアクセス方法を 使用できるのは、1) WLAN 展開が Cisco Prime Infrastructure マッピング データベースに統合されて いる場合、2) ゲスト WLAN (Web ポリシーが設定された WLAN) がモビリティ アンカーを使用しな い場合に限られます。
 - [E-mail Credentials to]: アカウントを設定するユーザの E メール アドレスを入力します。これは 必須フィールドです。



- (注) SMTP メール サーバは、ゲスト アカウント情報の送信に使用できるように、Cisco Prime Infrastructure で設定する必要があります。詳細については、次の項を参照してください。 http://www.cisco.com/en/US/docs/wireless/wcs/6.0/configuration/guide/6_0admin.html
- [Description]:説明を入力します。説明は、[Security]>[Local Net Users]で資格情報を適用する WLC に表示されます。説明は、ゲストに送信できる E メールにも含まれ、どのような資格情報を ネットワークへのアクセスに使用するかを知らせます。
- [Disclaimer]: ゲストユーザに送信される E メールで使用され、ネットワークへのアクセスにどの ような資格情報を使用するかを知らせます。

ステップ4 完了したら、[Save] をクリックします。図 10-42 に示す画面が表示され、スケジュールされたアカウントが作成されたことを確認できます。管理者には、資格情報をゲスト ユーザに印刷するか E メールで送信するオプションも表示されます。

ababa	Wireless	Control System Username: lobbyadmin Logout Refresh Print View							
cisco	Help 🕶								
Guest Users	Guest User Account Scheduled on the selected controllers								
		Guest User Credentials							
	Guest User Name	test2							
	Password	Frla4urF							
	Profile	Guest							
	Start Time	8: 0: 07/20/2007							
	End Time	17: 0: 08/03/2007							
	Disclaimer	Guests understand and acknowledge that we exercise no control over the nature, content or reliability of the informa and/or data passing through our network.							
	Print/Email G	est Hear Cradentials							
	Fringental de	escoser credendais							

図 10-42 スケジュールされたアカウントの正常な作成

ステップ 5 必要に応じて、[Print/Email Guest User Credentials] をクリックします。図 10-43 に示すような画面が 表示されます。

図 10-43	ゲスト ユーザ詳細の印刷または E メールでの送信

Guest	Users Details	E-mail Print Ba
C	Email To	12
Guest User Name	test2	
Password	Fria4urF	
Profile	Guest	
Start Time	8: 0: 07/20/2007	
End Time	17: 0: 08/03/2007	
Disclaimer	Guests understand and acknowledge that exercise no control over the nature, conter reliability of the information and/or data pa through our network	t we int or ussing

アカウントの詳細を印刷または E メールで送信すると、図 10-44 に示すようなサマリ画面が表示され ます。[User Name] をクリックすることにより、管理者はゲスト アカウントに戻って編集したり、 [User Name] の隣のボックスをオンにしてプルダウン選択リストから [Delete Guest User] を選択するこ とにより、ゲスト アカウントを削除できます。

図 10-44 Cisco Prime Infrastructure ゲスト ユーザのサマリ

ababa	Wireless Contro	ol System	Usernam	Username: lobbyadmin Logout Refresh Print View					
cisco	Help -								
Guest Users	Guest Users			Add Gue	st User 🔽 🖸				
	User Name	Profile	Description	Applied To	Status				
	T test2	Guest	Wireless Network Guest Access	Controller List	Scheduled				



ユーザがアクティブな状態で Cisco Prime Infrastructure からユーザ テンプレートを削除すると、その ユーザの認証が解除されます。

これで、Cisco Prime Infrastructure の Lobby Ambassador インターフェイスを使用したゲスト アカウントの作成に必要な手順は終了です。

アンカー コントローラ上でのゲスト資格情報の直接管理

次の手順では、ネットワーク管理者が、ロビー管理者の特権を使用して1つ以上のアンカーコント ローラ上にローカル管理アカウントを設定しているものとします。

ステップ1 システム管理者が割り当てたロビー管理者の資格情報を使用してアンカー コントローラにログインします。コントローラの Web 管理に対して HTTP/HTTPS を許可するには、ファイアウォールを通してコンジットを開く必要があります。「アンカー コントローラの位置決め」(P.10-6)を参照してください。

ログインすると、図 10-53 に示すような画面が表示されます。

図 10-45 アンカー コントローラのログイン

ululu cisco	Lobby Ambassador Guest Management	Logout Refresh
Guest Management	Guest Users List	New
	User Name WLAN SSID Account Remaining Time Description	

ステップ 2 [New] をクリックします。

図 10-46 に示すような画面が表示されます。

図 10-46 ローカル WLC ゲスト資格情報の作成

 cisco	Lobby Ambassador Gues	it Management	Logout Refresh
Guest Management	Guest Users List> N User Name Generate Password Password Confirm Password Lifetime	ew	CBack Apply
	WLAN SSID	Guest V Guest Access WLAN	

ステップ3 ユーザ資格情報を作成するには、次の手順を実行します。

- a. ユーザ名とパスワードを入力します(手動または自動)。
- **b.** ゲストアカウントを適用する WLAN/SSID を選択します。その際、L3 Web ポリシーが設定され た WLAN だけが表示されます。
- C. 資格情報の有効期間を入力します。
- **d.** ユーザの説明を入力します。
- **ステップ 4** [Apply] をクリックします。

図 10-47 に示すような画面に、新しく追加されたゲスト ユーザが表示されます。

図 10-47 アンカー WLC ゲスト ユーザのリスト

սիսիս cisco	Lobby Ambassador Gue	est Management		Logout Refres
Guest Management	Guest Users List			New
				Items 1 to 1 of 1
	User Name	WLAN SSID	Account Remaining Time	Description
	test3	Guest	1 d	Guest Access WLAN

この画面では、次の機能を実行できます。

- 既存のユーザの編集(右端のリンク。非表示)
- 既存のユーザの削除(右端のリンク。非表示)
- 新規ユーザを追加します。

ユーザ アカウントの最大数の設定

コントローラ上で指定可能なゲスト ユーザ アカウントのデフォルト数は 512 です。この値は、次の手順を実行することによって変更できます。

ステップ1 [Security] タブをクリックします。(図 10-48 を参照)。

図 10-48 ユーザ アカウントの最大数の設定

ahaha					Sa <u>v</u> e Conf	iguration	<u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security	General						Apply
▼ AAA General ▼ RADIUS Authentication	Maximum Local Database	e entries (on next reboot).	512	(Current Maximum	is 512)		

- ステップ2 左側のペインで、AAA プロパティの下の [General] をクリックします。
- ステップ3 ユーザデータベースエントリの最大数を設定します(512~2,048の間)。

ステップ 4 [Apply] をクリックします。

最大同時ユーザ ログイン

WWLC 上のローカル ユーザ アカウントの同時ログインの最大数は、設定が可能です。同時ログイン 数を無制限にする場合は、値を0にします。値を1~8に制限することもできます。ユーザ ログイン の最大数は、次の手順で設定されます。

ステップ1 [Security] タブをクリックします。(図 10-49 を参照)。

図 10-49 ユーザ ログイン ポリシー

ahaha							Sa <u>v</u> e Con	figuration	Ping	Logout <u>R</u> efre
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP		
Security	User Poli	cies								Apply
AAA General RADIUS Authentication Accounting TACACS+ LOAP Local Het Users MAC Filtering Disabled Clients User Login Policies AP Policies	Maximum	n Number of	f Concurrent Logi	ns for a single	user name				0	

- **ステップ2** 左ペインで、[AAA]の[User Login Policies] をクリックします。
- **ステップ3** 同時ユーザ ログインの最大数を設定します(0~8の間)。
- **ステップ 4** [Apply] をクリックします。

ゲスト ユーザの管理に関する注意事項

次の警告に注意してください。

- ゲストアカウントは、上記の方法か、2つの方法を同時に使用して追加できます。
- Cisco Prime Infrastructure の使用時に、コントローラの設定が最近 Cisco Prime Infrastructure と同期されていない場合、ロビー管理者はローカルのアンカー コントローラ上で作成された可能性のあるユーザアカウントを表示できないことがあります。この場合に、すでに WLC で設定されているユーザ名で Cisco Prime Infrastructure のロビー管理者がアカウントを追加しようとすると、ローカル設定が Cisco Prime Infrastructure 設定で上書きされます。
- ローカル管理者がユーザアカウントをローカルのコントローラ上に追加するときには、Cisco Prime Infrastructure 経由で作成されたものも含めて、作成されたすべてのアカウントを表示できます。
- ゲストユーザが WLAN に対して認証された状態で、資格情報が Cisco Prime Infrastructure または ローカルのコントローラ上から削除されると、ユーザトラフィックのフローが停止し、ユーザの 認証が解除されます。

その他の機能とソリューション オプション

Web ポータル ページの設定と管理

内部 Web サーバと関連機能は、ローカルのアンカー コントローラ上でホストされます。認証またはパ ススルー用の Web ポリシーを使用するように WLAN を設定した場合は、デフォルトで内部 Web サー バが呼び出されます。それ以上の設定は必要ありません。内部ポータルには、オプションの設定パラ メータがいくつか用意されています。

内部 Web ページの管理

- **ステップ1** [Security] タブをクリックします。
- **ステップ 2** 左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。

図 10-50 に示すような設定画面が表示されます。ポータルページに表示される見出しとメッセージ情報を変更できます。また、認証後のリダイレクト URL を選択することもできます。

図 10-50 Web ログイン ページ設定画面

ahaha						Sa <u>v</u> e Co	nfiguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR WLANS	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security	Web Login Page						Preview	Apply
▼ AAA General ▼ RADIUS Authentication	Web Authentication This page allows you to cu page. The Login page is pi WLAN if 'Web Authenticati	Type ustomize the co resented to web on' is turned on	Internal (intent and approved a service of the ser	Default) earance of the st time they ac Security Polici	Login cess the es).			
 TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	Cisco Logo Redirect URL after Iogin	Show	O Hide					
Local EAP	Headline	Welcome to	the Cisco wir	eless network				
 Priority Order Access Control Lists IPSec Certs Wireless Protection Work Less Protection Web Laun Pade Certificate CIDS 	Message	Cisco is ple for your net	ased to provid work. Please l	ie the Wireless login and put y	LAN infrastructure our air space to wo	rk.		
						2		

- **ステップ3** [Apply] をクリックします。
- ステップ4 必要に応じて、[Preview] をクリックして、ユーザに表示されるリダイレクト先のページを確認します。

Web ページのインポート

カスタマイズされた Web ページをダウンロードして、ローカルのアンカー コントローラ上に保存でき ます。カスタマイズされた Web ページをインポートするには、次の手順を実行します。 **ステップ1** [Commands] タブをクリックします (図 10-51 を参照)。

図 10-51 Web ページのインポート

،، ،،، ،، cısco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP	Logout <u>R</u> efresh
Commands	Downloa	d file to (Controller					Clear	Download
Download File Upload File	File Type			Webauth	Bundle	~			
Reboot	TFTP Serv	er							
Reset to Factory Default	IP Addres	is		10.20.30	200				
Set Time	Maximum	retries		10					
	Timeout (seconds)		6					
	File Path			1					
	File Name								

- **ステップ2** [File Type] で [Web Auth Bundle] を選択します。
- **ステップ 3** ファイルが存在する TFTP サーバの IP アドレスとファイル パスを指定します。
- ステップ4 [Download] をクリックして、ダウンロードを開始します。

Web 認証バンドルをダウンロードする際には、次の点に注意してください。

- プルダウン選択リストから [Web Auth Bundle] を選択して、ファイルがコントローラ上の正しい ディレクトリに保存されるようにします。
- [Web Auth Bundle] は、カスタム Web ログインページにアソシエートされている、HTML ファイ ルとイメージファイルの.tar ファイルである必要があります。ダウンロード後に、WLC によって ファイルが untar され、適切なディレクトリに格納されます。
- [Web Auth Bundle] (.tar ファイル) は、1MB より大きくてはなりません。
- HTML ログイン ページのファイル名は、login.html にする必要があります。

カスタマイズされた Web ページのダウンロードと使用方法の詳細は、次の URL を参照してください。 http://www.cisco.com/en/US/docs/wireless/wcs/4.1/configuration/guide/wcssol.html#wp1065703

インポートした Web 認証ページの選択

コントローラにダウンロードしたカスタマイズ済みの Web 認証ページを使用するには、次の手順を実行します。

- **ステップ1** [Security] タブをクリックします。
- ステップ2 左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。
- **ステップ3** [Web Authentication Type] プルダウン選択リストから [Customized (Downloaded)] を選択します。
- ステップ4 [Preview] をクリックして、ダウンロードしたページを表示します。

ステップ5 最後に、[Apply] をクリックします (図 10-52 を参照)。

 cısco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP	Logout <u>R</u> efres
Security AAA General * RADIUS Authentication Accounting	Web Logir Web Authe This page allo page. The Log WLAN if 'Web	n Page entication ows you to o gin page is Authentica	a Type customize the co presented to well tion' is turned or	Internal () Internal () Inter Customice b us External () (under WLAN	Default) Default) d (Downloade Redirect to ext Security Polici	d) ernal server) es).		Preview	Apply
TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP	Cisco Logo Redirect Ul Iogin Headline	RL after	 Show Welcome to 	• Hide	less network				
 Priority Order Access Control Lists IPSec Certs Wireless Protection Policies Web Auth Web Login Page Certificate CIDS 	Message		Cisco is ple for your net	ased to provid, twork. Please li	the Wireless	LAN infrastructure our air space to w	ork. 🛆		
							8		

図 10-52 インポートした Web 認証ページの選択

内部 Web 証明書の管理

Web 認証ログイン ページでは、ユーザ資格情報を保護するために SSL が使用されます。コントローラ では、簡単な自己署名証明書が使用されます。証明書が自己署名されたものであるため、ゲスト ユー ザが図 10-53 に示すような認証ページにリダイレクトされると、次のようなポップアップ アラートが 表示されます。



図 10-53 Web 証明書セキュリティ アラート(IE6)

この時点で、[Yes] をクリックして先に進むか、[View Certificate] を選択してそのページを信頼された サイトとして手動でインストールできます。Web サーバでは、「アンカー WLC の設置およびインター フェイスの設定」(P.10-14) で設定された仮想インターフェイスの IP アドレスが発信元アドレスとし て使用されます。ホスト名を IP アドレスと共に指定する場合は、ホスト名が DNS によって解決される ときに、次の条件を満たすようにする必要があります。

- クライアントが Web 認証ページにリダイレクトされる。
- ユーザが、ホスト名とホスト IP アドレスの矛盾が原因の Web 認証エラーに遭遇しない。

外部 Web 証明書のインポート

信頼できるルート CA によって発行された正式な Web 証明書が必要な場合は、次の手順を実行することによって、コントローラにダウンロードできます。

ステップ1 [Security] タブをクリックします。

左側のペインで、[Web Auth] をクリックして、[Certificate] をクリックします (図 10-54 を参照)。

図 10-54 外部 Web 証明書のインポート

սիսիս								n <u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR V	<u>N</u> LANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security	Web Authe	ntication Certificate				Appl	,	Regenerate Certificate
▼ AAA General	Current Certificate							
 RADIUS Authentication Accounting 	Name:	bsnSslWebauthCert						
 TACACS+ LDAP Local Net Users 	Serial Number:	2882400190						
MAC Filtering Disabled Clients	Valid:	From 2006 May 31st, 00	0:00:01 GMT U	ntil 2016 May 3	31st, 00:00:01 GMT	r)		
User Login Policies AP Policies	Subject Name:	C=US, O=Cisco System	ns Inc., OU=De	viceSSL (WebA	with), CN=1.1.1.1			
Local EAP	Issuer Name:	C=US, O=Cisco System	ns Inc., OU=De	viceSSL (WebA	auth), CN=1.1.1.1			
Access Control Lists	Fingerprint:	98:11:37:65:ea:07:2c:	e1:31:3c:bd:eb	:e0:a4:d9:9a				
▶ IPSec Certs	Fingerprint:	87:de:35:80:96:1f:51:2	d:19:7d:b8:57	:a5:4a:6f:57:9	3:f0:db:2d			
 Wireless Protection Policies 								
Web Auth Web Login Page	SSL Certificate *							
Certificate	* Controller							
¢ cibs	rebooted for							
	certificate to							
	tune eneet.							
	<							>

- **ステップ 2** [Download SSL Certificate] チェックボックスをオンにします。
- ステップ3 証明書のダウンロードに必要な情報を各フィールドに入力します。
- **ステップ 4** [Apply] をクリックします。
- ステップ 5 証明書をダウンロードしたら、サーバを再起動します。

外部 Web リダイレクションのサポート

企業では、有線のゲスト アクセスまたは NAC 機能をサポートする Web ポータル システムがすでに展開されている場合があります。そのような場合は、無線ゲスト ユーザを外部 Web ポータルにリダイレ クトするように、アンカー コントローラを次の手順で設定できます。

- ステップ1 [Security] タブをクリックします。
- **ステップ 2** 左側のペインで、[Web Auth] をクリックして、[Web Login Page] をクリックします。(図 10-55 を参照)。

								Logour Keiresii
CISCO 🛛	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Security V	Web Login Page						Preview	Apply
AAA General Control C	Web Authenticatio URL https://10.20.30. External Web Serve Web Server IP Add	n Type 41 rss	External (8	ver	ana) seneri			

図 10-55 外部 Web リダイレクションのサポート

- ステップ3 [Web Server IP] フィールドと [URL] フィールドに入力します。
- **ステップ 4** [Apply] をクリックします。

アンカー WLC 事前認証 ACL

事前認証 ACL は、ゲスト WLAN に適用できます。これにより、認証されていないクライアントが、 認証前に特定のホストまたは URL の宛先に接続できます。事前認証 ACL はゲスト WLAN のレイヤ 3 セキュリティ設定で適用されます。有効になっている場合、アンカー WLC 上でのみ実行されます (図 10-56 を参照)。

図 10-56 WLAN 事前認証 ACL

abab	Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs	WLANs > Edit Apply
WI ANS	General Security QoS Advanced
WLANs AR Groups VII AN	Layer 2 Layer 3 AAA Servers
AF Groups VLAN	
	Layer 3 Security None
	web Policy = Authentication
	O Passthrough
	O Conditional Web Redirect
	Preauthentication ACL Cisco Open Garden
	Cisco Open Garden

特定の ACL は、[Security] > [Access Control Lists] で設定されます(図 10-57 および図 10-58 を参照)。

図 10-57 WLC アクセス コントロール リスト

abab							Sa <u>v</u> e Co	nfiguration	l <u>P</u> ing	Logout Refr
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	Access C	ontrol Li	ists							New
AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Name <u>Cisco Open</u>	Garden								
Local EAP										
Priority Order										
Access Control Lists Access Control Lists CPU Access Control Lists										

<u>入</u> (注)

事前認証 ACL が Web 認証ポリシーと共に使用される場合、DNS 要求を許可するルールが含まれている必要があります。含まれていない場合、クライアントは、ACL によって許可される宛先ホスト/URL に解決して接続することができません。

ululu cisco	MONI	TOR :	<u>W</u> LANs		LLEF	R WIRELESS	ş	ECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration HELP	<u>P</u> ing	.ogout <u>R</u> efresl
Security	Acce	ess Co	ntrol Li	sts > Ed	it					< Ba	ck	Add Nev	v Rule
- AAA	Gene	eral											
General RADIUS Authentication Accounting TACACS+ LDAP	Acces	s List Na Action	me Sour	Cisco C)pen sk	Garden Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
LDAP Local Net Users MAC Filtering	4	Permit	10.20	.31.0 55.255.0	1	0.0.0.0	1	UDP	Any	DNS	Any	Any	
Disabled Clients User Login Policies	_2	Permit	0.0.0	.0	1	10.20.31.0 255.255.255.0	1	UDP	DNS	Any	Any	Any	
Local EAP	2	Permit	10.20	.31.0 55.255.0	1	171.71.181.19 255.255.255.255	1	тср	Any	HTTP	Any	Any	
 Priority Order Access Control Lists 	4	Permit	171.7 255.2	1.181.19 55.255.255	/	10.20.31.0 255.255.255.0	1	тср	HTTP	Any	Any	Any	
Access Control Lists CPU Access Control Lists													

図 10-58 事前認証 ACL の例

アンカー コントローラ DHCP 設定

アンカー コントローラがゲスト アクセス WLAN の DHCP サービスを管理する場合は、次の手順を実行します。

(注)

アンカー コントローラは、ゲスト N+1 冗長性を実装している場合、DHCP サービスを管理するために 使用することはできません。なぜなら、2 つ以上の WLC 間で単一のゲスト VLAN/サブネットのアド レス リースを同期するメカニズムがないからです。

新しい DHCP スコープのアンカー コントローラへの追加

- **ステップ1** [Controller] タブをクリックします。
- **ステップ 2** 左側のペインで、[Internal DHCP Server] をクリックします。

ステップ3 [New] をクリックします。(図 10-59 を参照)。

図 10-59 新しい DHCP スコープの追加

 cısco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration HELP	<u>P</u> ing	Logout	<u>R</u> efresh
Controller	DHCP So	opes						New	1		
General Inventory Interfaces	Scope Na	me	Addres	s Pool	Lea	ase Time	Status				
Network Routes Internal DHCP Server Mobility Management											

スコープ名の定義

ステップ 4 スコープ名を定義して、[Apply] をクリックします。(図 10-60 を参照)。

図 10-60 スコープ名の定義

ahaha			Save Configuration Ping Logout Refre						
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	DHCP So	cope > N	ew					< Back	Apply
General	Scope Na	me Guest	t Scope						
Inventory									
Interfaces									
Network Routes									
Internal DHCP Server									
Mobility Management									

- **ステップ5** [Scope Name] をクリックして、編集します (図 10-61 を参照)。
 - 図 10-61 DHCP スコープの編集

abab									ing Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	
Controller	DHCP Sc	opes						New	
General	Scope Nac	ac	Ad	dress Pool		Lease Time		Status	
Inventory	Guest Scop	•)	0.0	0.0.0 - 0.0.0		1 d		Disabled	
Interfaces	-								
Network Routes									
Internal DHCP Server									
Mobility Management									

スコープ プロパティの定義

- ステップ6 最低限必要な次の情報を定義します。
 - プールの開始と終了
 - ネットワーク
 - マスク
 - デフォルトルータ
 - DNS サーバ

ステップ7 [Status] として [Enabled] を選択し、[Apply] をクリックします (図 10-62 を参照)。

cisco	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Cor C <u>Q</u> MMANDS	HELP	Logout <u>R</u> efrest
Controller	DHCP Scope > Edit					< Back	Apply
General Inventory Interfaces Network Routes Internal DHCP Server Mobility Management Spanning Tree	Scope Name Pool Start Address Pool End Address Network Netmask Lease Time (seconds)	Guest Scope 10.20.31.100 10.20.31.200 10.20.31.0 255.255.255.0 86400					
Ports Master Controller Mode Network Time Protocol	Default Routers DNS Domain Name DNS Servers	10.20.31.1	0.0.0.0	168.183	0.0.0.0		
▶ QoS ▶ CDP	Netbios Name Servers Status	0.0.00 Disabled V Enabled Disabled	0.0.0.0		0.0.0		

図 10-62 スコープ プロパティの設定と有効化

外部 RADIUS 認証

ゲスト ユーザの認証で説明したように、ゲスト資格情報をローカルのアンカー コントローラ上に作成 して保存する代わりに、外部 RADIUS サーバを使用してゲスト ユーザを認証できます。この方法を使 用する場合は、ゲスト アカウント管理で説明したロビー管理機能は使用できません。その他のいくつ かのゲスト管理システムと外部 RADIUS サーバの併用が考えられます。

外部 RADIUS サーバを使用するようにゲスト WLAN を設定するには、アンカー コントローラ上で次の設定手順を実行します。

RADIUS サーバの追加

ステップ1 [Security] タブをクリックします。 サマリ画面が表示されます (図 10-63 を参照)。

집 10-63	[\$	Summ	ary] 🛙	画面					
uhuhu cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS	ECURITY	MANAGEMENT	Sa <u>v</u> e Conf C <u>O</u> MMANDS	iguration <u>P</u> HELP	ing Lo <u>q</u> out <u>R</u> efresl
Security	RADIUS	Authenticat	tion Serve	S		10		Apply	New
AAA General RADIUS Authentication Accounting TACACS+ IDAP	Call Stati Credenti Use AES	ion ID Type als Caching Key Wrap	IP Address	ed for FIPS custom	ers and re	quires a key wrap o	ompliant RADIU	S server)	
Local Net Users MAC Filtering Disabled Clients	Network User	Managemen	Server Index	Server Address	Port	IPSec	Adm	in Status	
User Login Policies AP Policies		V	1	10.20.30.16	1812	Disabled	Enab	led	
Local EAP			2	10.20.30.15	1812	Disabled	Enab	led	
Priority Order									

ステップ 2 [New] をクリックします。

図 10-64

図 10-64 に示すような画面が表示されます。

RADIUS サーバ設定の定義

cisco		OLLER WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguration <u>P</u> ing HELP	Logout <u>R</u> efresh
Security AAA General Adhentication Accounting TACACS+ LDAP Load Net Uerrs Method Cons Uerr Login Policies AP Policies Local EAP Priority Order Access Control Lists IPSec Certs Web Auth > CIDS	RADIUS Authentication S Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Retransmit Timeout Network User Management IPSec	Servers > New 3 × 10.20.30.17 ASCII × ASCII × × •••••• • (Designed for f 1812 Enabled × 2 seconds Enable Enable Enable Enable	IPS customer	s and requires a k	ey wrsp. complia	< Back	Арріу

ステップ3 RADIUS サーバの設定を定義するには、RADIUS サーバ上で指定したように、IP アドレス、共有秘密、および認証ポート番号を設定します。

[Network User] チェックボックスがオフになっていると、RADIUS サーバは、特定の WLAN の RADIUS 設定でそのサーバが明示的に選択されているときにだけユーザ認証に使用されます。また、 [Network User] チェックボックスがオンになっていると、RADIUS サーバが、そのサーバの優先順位 に基づいて、すべてのユーザ認証に使用されます。

ステップ 4 [Apply] をクリックします。図 10-65 に示すサマリ画面には、新しく追加されたサーバが表示されます。

図 10-65

cisco		<u>W</u> LANs <u>C</u> (ONTROLLER	WIRELESS S		MANAGEMENT	Sa <u>v</u> e Cor C <u>O</u> MMANDS	figuration Pi	ing Logout <u>R</u> efi
ecurity	RADIUS	Authenticati	ion Serve	rs				Apply	New
General	Call Stati	ion ID Type	IP Address	۲					
RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering	Credenti Use AES Network	als Caching Key Wrap	C (Design	ed for FIPS custom	ers and requi	res a key wrap c	mpliant RADIU	S server)	
 ▼ RADIUS Authentication Accounting ▼ TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies 	Credenti Use AES Network User	als Caching Key Wrap Management	C (Design	Server Address	Port	res a key wrap o IPSec	Admi	S server) in Status	_
 RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies 	Credenti Use AES Network User	als Caching Key Wrap Management	C (Design Server Index	Server Address 10.20.30.16	Port 1812	res a key wrap c IPSec Disabled	empliant RADIU: Admi Enabl	S server) in Status ed	3
RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP	Credenti Use AES Network User	als Caching Key Wrap Management V	C (Design Server Index 1 2	Server Address 10.20.30.16 10.20.30.15	Port 1812 1812	res a key wrap c IPSec Disabled Disabled	empliant RADIU Admi Enabl Enabl	S server) in Status ed S	

ステップ 5 RADIUS サーバを選択するには、[WLANs] タブをクリックします。図 10-66 に示すような画面が表示されます。

[Summarv] 画面

းပါးပါး cisco	MONITOR WLANS CO	NTROLLER WIR	ELESS <u>S</u> ECURITY MANA	Sa GEMENT C <u>O</u> MMA	ve Configuration Bing Logout NDS HELP	Refi
/LANs	WLANs				New	
WLANS WLANS	Profile Name	WLAN ID	WLAN SSID	Admin Status	Security Policies	
AP Groups VLAN	SRND	1	SRND	Enabled	802.1X	E
	WEP	2	WEP	Enabled	WEP	E
	CCKM	3	CCKM	Enabled	[WPA + WPA2][Auth(802.1X)]	
	PKC	4	PKC	Enabled	[WPA + WPA2][Auth(802.1×)]	
	WPA	5	WPA	Enabled	[WPA + WPA2][Auth(PSK)]	
	Guest	6	Guest	Enabled	Web-Auth, MAC Filtering	E
	Guert?	7	Guest2	Enabled	Web-Auth MAC Filtering	

図 10-66 [WLANs] タブ

ステップ6 ゲスト WLAN を探して、その [Profile Name] をクリックします。
 図 10-67 に示すように、ゲスト WLAN の設定画面が表示されます。

45	General	Security Q	S Adva	inced				< Back	Арр
ANS ANS Groups VLAN	Layer 2	Layer 3 A	AA Servers						
	Radius Ser	vers Authentication S	iervers	Accounting Servers		Server 1 Server 2	None V		
	Server	IP:10.20.30.17, F	ort:1812 🗸	None	~	Server 3	None 💌		
	Server 2	None	~	None	~				
	Server 3	None	~	None	V				
	Local EAP	Authentication							
	Local EA	P Authentication	Enabled						

図 10-67 ゲスト WLAN の設定画面

- **ステップ7** [WLAN Security] タブで [AAA Servers] を選択します。
- **ステップ8** [Authentication Servers] のプルダウン選択リストから、Web 認証に使用する RADIUS サーバを選択します。

外部アクセス コントロール

この章で説明した中央集中型ゲスト アクセス トポロジは、Cisco NAC Appliance などの外部アクセス コントロール プラットフォームと統合できます。

このシナリオでは、企業で、有線ゲスト アクセス サービスをサポートするためのアクセス コントロール プラットフォームがインターネットの DMZ に展開されているものとします(図 10-68 を参照)。



図 10-68 外部アクセス コントロールを使用した無線ゲスト アクセス

図 10-68 に示すように、無線ゲスト アクセス トポロジは、アンカー コントローラ上のゲスト VLAN インターフェイスが、ファイアウォールや境界ルータに接続する代わりに Cisco NAC Appliance など のアクセス コントロール プラットフォームの inside インターフェイスに接続する点を除いて同じです。

このシナリオでは、NAC Appliance が、リダイレクション、Web 認証、およびその後のインターネットへのアクセスを処理します。キャンパス コントローラとアンカー コントローラは、NAC アプライアンスまたはその他のいくつかのプラットフォームを使用してゲスト アクセスを制御している DMZ に 全社的なゲスト WLAN トラフィックをトンネルするためだけに使用されます。

ゲスト WLAN、キャンパス、およびアンカー コントローラの設定は、上記の例と同じです。

唯一の違いは、ゲスト WLAN のセキュリティ設定でレイヤ 3 Web ポリシーが有効になっていない点で す(図 10-69 および図 10-70 を参照)。

	义	10-69	ゲスト WLAN のレイヤ 3 セキュリティ	ポリシー
--	---	-------	------------------------	------

սիսիս		ogout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit < Back General Security QaS Advanced Layer 3 Layer 3 AAA Servers Layer 3 Security None Web Policy 2	Apply

図 10-70 ゲスト WLAN L2 セキュリティ設定

սիսիս								Logout <u>R</u> efre	sh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP		
WLANS WLANS WLANS AP Groups VLAN	WLANS > Edit General Sect Layer 2 La Layer 2 Securi	yer 3 AAA Se ty None MAC Filterin	Advanced ervers				< Back	Apply	~

上記の設定では、セキュリティ ポリシーを使用せずに WLAN が設定されます。ゲスト トラフィック は、アンカー コントローラを通過して、Cisco NAC Appliance の inside インターフェイスまたは信頼 されていないインターフェイスに到達し、ユーザが認証されるまでブロックされます。

DHCP は、ローカルのコントローラ上でホストするか、外部の NAC Appliance または専用サーバ経由 でホストできます。

Cisco NAC Appliance またはその他の外部アクセス コントロール プラットフォーム固有の設定につい ては、この章では説明しません。詳しい設定ガイドラインについては、プラットフォーム固有のマニュ アルを参照してください。

ゲスト アクセス機能の確認

ゲスト アクセス サービスは、ユーザが次の条件を満たしている場合に正しく機能します。

- ゲスト WLAN にアソシエートできる。
- DHCP 経由で IP アドレスを受信する。
- ブラウザを開くと、Web 認証ページにリダイレクトされる。
- 資格情報を入力して、インターネット(またはその他の許可されたアップストリーム サービス) に接続する。

ゲスト アクセスのトラブルシューティング

以降の確認作業とトラブルシューティング作業は、次のことを前提としています。

- このソリューションでは、アンカー コントローラ上の Web 認証機能が使用されている。
- ユーザ資格情報が、ローカルのアンカーコントローラ上で作成および保存されている。

次のようなさまざまな症状のトラブルシューティングを実行するには、少なくとも、外部のキャンパス コントローラからアンカー コントローラに ping できる必要があります。それが不可能な場合は、ルー ティングを確認します。

その次に、次の高度な ping コマンドを実行できる必要があります。これらのコマンドは、コントローラのシリアル コンソール インターフェイスを通してだけ実行できます。

• **mping** neighbor WLC ip

このコマンドは、CAPWAP 制御チャネルを通して近隣のコントローラに ping します。

• eping neighbor WLC ip

このコマンドは、CAPWAP データ チャネルを通して近隣のコントローラに ping します。

標準の ICMP ping が通っても mping が通らない場合は、各 WLC のデフォルトのモビリティ グループ 名が同じであることと、各 WLC の IP、MAC、およびモビリティ グループ名がすべての WLC のモビ リティ メンバ リストに入力されていることを確認します。

ping と mping は通っても eping が通らない場合は、ネットワークで IP プロトコル 97 (Ethernet-over-IP) がブロックされていないことを確認します。

ユーザがゲスト WLAN に接続できない

- ゲスト WLAN をサポートするアンカー コントローラとすべての外部コントローラでゲスト WLAN が有効になっていることを確認します。
- ゲスト WLAN SSID がブロードキャストされていることを確認します。
- クライアントアダプタまたはソフトウェアの設定を確認します。

ユーザが DHCP 経由で IP アドレスを取得できない

- WLAN の設定がアンカー コントローラ上と外部コントローラ上で同じであることを確認します (WLAN インターフェイスおよびモビリティ アンカーを除く。「アンカー WLC 上でのゲスト WLAN の設定」(P.10-28)を参照)。
- ゲスト WLAN がアンカー WLC 上で有効になっていることを確認します。
- アンカー コントローラのゲスト VLAN インターフェイスの設定で、DHCP サーバのアドレスが適切かどうかをチェックします。
 - 外部 DHCP サーバを使用している場合は、IP アドレスが外部サーバのアドレスになっている 必要があります。
 - アンカー コントローラから外部 DHCP サーバにアクセスできることを確認します。
 - DHCP サービスにアンカー コントローラを使用している場合は、DHCP サーバの IP アドレス がコントローラの管理 IP アドレスになっている必要があります。
 - コントローラ上で DHCP スコープが設定され有効になっていることを確認します。
 - DHCP スコープのネットワークマスクとゲスト VLAN インターフェイスのマスクが一致していることを確認します。

 DHCP スコープが、ネットワーク インフラストラクチャに割り当てられたすべてのアドレス と重複していないことを確認します。

ユーザが Web 認証ページにリダイレクトされない

次の解決方法では、ユーザがゲスト WLAN にアソシエートして IP アドレスを取得できることを想定 しています。

- 有効な DNS サーバが DHCP を介してクライアントに割り当てられていることを確認します。
- DNS サーバがアンカー コントローラから接続可能なことを確認します。
- Web ブラウザで開かれている URL が解決可能なことを確認します。
- Web ブラウザで開かれている URL が HTTP ポート 80 に接続していることを確認します。

(注) 内部 Web 認証サーバは、80 およびユーザが定義したもう1つのポート番号以外のポート上の 入力要求をリダイレクトしません(「ユーザ リダイレクション」(P.10-10)参照)。

ユーザが認証されない

• アンカーコントローラ上のユーザ資格情報がアクティブなことを確認します。

通常は、ゲスト資格情報に対して有効期間が設定されます。資格情報は、期限が切れていると、ア ンカー コントローラ上の [Security] > [Local Net Users] リストに表示されません。Cisco Prime Infrastructure を使用して、ローカルのコントローラ上でユーザ テンプレートを適用し直すか、 ユーザ資格情報を作成し直してください。管理システムを使用したゲスト管理およびゲスト資格情 報の管理を参照してください。

ユーザパスワードを確認します。

ユーザがインターネットまたはアップストリーム サービスに接続できない

- アンカーコントローラと、アンカーコントローラに接続されているファイアウォールまたは境界 ルータ間のルーティングを確認します。
- 必要に応じて、ファイアウォールまたはインターネット境界ルータの NAT 設定を確認します。

システム モニタリング

以降では、トラブルシューティングに役立つ可能性のあるいくつかの監視コマンドについて説明しま す。

アンカー コントローラ

シリアル コンソール ポートから、次のコマンドを実行します。

Cisco Controller)	>show client summar	У				
Number of Clients.		1				
MAC Address	AP Name	Status	WLAN	Auth	Protocol	Port
00:40:96:ac:5f:f8	10.15.9.19	Associated	3	Yes	Mobile	1

プロトコルが Mobile になっていることに注目してください。Auth フィールドには、実際のユーザの状態が反映されます。ユーザが Web 認証をパスすると、このフィールドに YES と表示されます。パスしなかった場合は、このフィールドに NO と表示されます。

AP 名にも注目してください。これは、外部コントローラ(起点コントローラ)の管理 IP アドレスです。

サマリ情報に示されたクライアントの MAC アドレスを使用して、詳細を表示します。

(Cisco Controller) > show client detail 00:40:96:ac	:5f:f8
Client MAC Address	00:40:96:ac:5f:f8
Client Username	romaxam
AP MAC Address	00:00:00:00:00
Client State	Associated
Wireless LAN Id	3
BSSID	00:00:00:00:00:02
Channel	N/A
IP Address	10.20.31.100
Association Id	0
Authentication Algorithm	Open System
Reason Code	0
Status Code	0
Session Timeout	86316
Client CCX version	No CCX support
Mirroring	Disabled
QoS Level	Silver
Diff Serv Code Point (DSCP)	disabled
802.1P Priority Tag	disabled
WMM Support	Disabled
Mobility State	Export Anchor
Mobility Foreign IP Address	10.15.9.19
Mobility Move Count	1
Security Policy Completed	Yes
Policy Manager State	RUN
Policy Manager Rule Created	Yes
NPU Fast Fast Notified	Yes
Policy Type	N/A
Encryption Cipher	None
Management Frame Protection	No
EAP Type	Unknown
Interface	wlan-user
VLAN	31
Client Capabilities:	
CF Pollable	Not implemented
CF Poll Request	Not implemented
Short Preamble	Not implemented
PBCC	Not implemented
Channel Agility	Not implemented
Listen Interval	0
Client Statistics:	
Number of Bytes Received	0
Number of Bytes Sent	0
Number of Packets Received	0
Number of Packets Sent	0
Number of Policy Errors	0
Radio Signal Strength Indicator	Unavailable
Signal to Noise Batio	Unavailable
Nearby AP Statistics:	0114104110010
TxExcessiveRetries: 0	
TxRetries: 0	
RtsSuccessCnt: 0	
RtsFailCnt: 0	
TxFiltered: 0	
TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]	

コントローラの Web 設定、および管理インターフェイスの [Clients] > [Detail] で同じ情報を得ること ができます (図 10-71 を参照)。



					Sa <u>v</u> e Configuration P	ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY N	MANAGEMENT (C <u>o</u> mmands He <u>l</u> p	
Monitor	Clients > Detail			< Back	Apply Link Te	est Remove
Summary	Client Properties		AP	Properties		
Statistics	MAC Address	00:40:96:ac:5f:f8		AP Address	Unknown	
h Wireless	IP Address	10.20.31.100		AP Name	10.15.9.19	
· · · · · · · · · · · · · · · · · · ·	Client Type	Regular		АР Туре	Mobile	
	User Name	romaxam		WLAN Profile	Guest2	
	Port Number	1	1	Status	Associated	
	Interface	wlan-user		Association ID	0	
	VLAN ID	31	1	802.11 Authenticat	tion Open System	
	CCX Version	Not Supported	1	Reason Code	0	
	E2E Version	Not Supported	:	Status Code	0	
	Mobility Role	Export Anchor		CF Pollable	Not Implemented	
	Mobility Peer IP Address	10.15.9.19		CF Poll Request	Not Implemented	
	Policy Manager State	RUN	:	Short Preamble	Not Implemented	
	Mirror Mode	Disable 💌		PBCC	Not Implemented	
	Management Frame Protection	No		Channel Agility	Not Implemented	
	Requility Information		1	Timeout	0	
	security information			WEP State	WEP Disable	
	Security Policy Completed	Yes				
	Policy Type	N/A				
	Encryption Cipher	None				
	EAP Type	N/A				
	Quality of Service Propert	ies				
	WMM State	Disabled				

外部のキャンパス コントローラ

シリアル コンソール ポートから、次のコマンドを実行します。

(WiSM-slot3-1) >sh	low client summary					
Number of Clients.		2				
MAC Address	AP Name	Status	WLAN	Auth	Protocol	Port
00:40:96:ac:5f:f8	AP318e5.7fdc	Associated	1	Yes	802.11g	29

アンカー コントローラでは Protocol フィールドが Mobile になっていましたが、同じクライアントに対 してこの Protocol フィールドは 802.11g になっていることに注目してください。外部のキャンパス コ ントローラでは、必ずユーザが Authenticated として表示され、AP name にはクライアントがアソシ エートされている実際の AP が反映されます。

次のコマンドを実行すると、さらに詳しい情報を得られます。

(WiSM-slot3-1) >show client detail 00:40:96:ac:5f	:f8
Client MAC Address	00:40:96:ac:5f:f8
Client Username	N/A
AP MAC Address	00:17:df:35:86:50
Client State	Associated
Wireless LAN Id	1
BSSID	00:17:df:35:86:50
Channel	11
IP Address	Unknown
Association Id	1
Authentication Algorithm	Open System
Reason Code	0
Status Code	0
Session Timeout	0
Client CCX version	No CCX support
Mirroring	Disabled
QoS Level	Silver

Diff Serv Code Point (DSCP)	disabled disabled Disabled Export Foreign 10.15.9.13 0 Yes RUN Yes N/A None No Unknown management 9 Not implemented Not implemented Implemented
PBCC	Not implemented
Channel Agility	Not implemented
Client Statistics:	0
Number of Bytes Received Number of Bytes Sent Number of Packets Received Number of Packets Sent Number of Policy Errors Radio Signal Strength Indicator Signal to Noise Ratio	308244 700059 2527 1035 0 -75 dBm 25 dB
<pre>Nearby AP Statistics: TxExcessiveRetries: 0 TxRetries: 0 RtsSuccessCnt: 0 RtsFailCnt: 0 TxFiltered: 0 TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0] AP3 .18e5.7fdc(slot 0)</pre>	
antenna0: 37 seconds ago -73 dBm	antennal: 4294510568 seconds

ago

コントローラの Web 設定、および管理インターフェイスの [Clients] > [Detail] で同じ情報を取得できます(図 10-72 を参照)。

ululu cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECU	S RITY M <u>A</u> NAGEMENT C <u>O</u> MN	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efre AANDS HE <u>L</u> P	
Monitor Summary > Statistics > CDP > Wireless	Clients > Detail		< Back	Apply Link Test Remove	
	Client Properties		AP Properties	AP Properties	
	MAC Address	00:40:96:ac:5f:f8	AP Address	00:17:df:35:86:50	
	IP Address	0.0.0.0	AP Name	AP318e5.7fdc	
	Client Type	Regular	AP Type	802.11g	
	User Name		WLAN Profile	Guest2	
	Port Number	29	Status	Associated	
	Interface	management	Association ID	1	
	VLAN ID	9	802.11 Authentication	Open System	
	CCX Version	Not Supported	Reason Code	0	
	E2E Version	Not Supported	Status Code	0	
	Mobility Role	Export Foreign	CF Pollable	Not Implemented	
	Mobility Peer IP Address	10.15.9.13	CF Poll Request	Not Implemented	
	Policy Manager State	RUN	Short Preamble	Implemented	
	Mirror Mode	Disable 💌	PBCC	Not Implemented	
	Management Frame Protection	No	Channel Agility	Not Implemented	
			Timeout	0	
	Security Information	(15.74)	WEP State	WEP Disable	
	Security Policy Completed	Yes			
	Policy Type	N/A			
	Encryption Cipher	None			
	EAP Type	N/A			
	Quality of Service Properties				
	WMM State	Disabled			

図 10-72 [Foreign WLC Monitor] > [Client Detail]

debug コマンド

シリアル コンソールからは、次のデバッグ コマンドも使用できます。

debug mac addr <client mac address>
debug mobility handoff enable
debug mobility directory enable
debug dhcp packet enable
debug pem state enable
debug pem events enable
debug dot11 mobile enable
debug dot11 state enable