



## **Cisco Aironet** アクセスポイント **Cisco IOS** ソフトウェア コンフィギュレーション ガイド

Cisco IOS リリース 15.2(4)JB3a

### **Cisco Systems, Inc.**

[www.cisco.com](http://www.cisco.com)

シスコは世界各国 200 箇所にオフィスを開設しています。  
Addresses, phone numbers, and fax numbers  
are listed on the Cisco website at  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco Aironet アクセス ポイント Cisco IOS ソフトウェア コンフィギュレーション ガイド  
© 1992-2013 Cisco Systems, Inc. All rights reserved.

Copyright © 2014. シスコシステムズ合同会社。  
All rights reserved.



## 目次

はじめに	xix
対象読者	i-xix
目的	i-xx
設定手順と例	i-xx
マニュアルの構成	i-xx
表記法	i-xxii
関連資料	i-xxiii
マニュアルの入手方法およびテクニカル サポート	i-xxiii

---

### 第 1 章

<b>アクセス ポイント機能の概要</b>	<b>1-1</b>
アクセス ポイントの無線	1-1
リリースの新機能およびプラットフォーム	1-2
管理オプション	1-2
クライアント デバイスのローミング	1-2
ネットワークの構成例	1-3
ルート アクセス ポイント	1-3
リピータ アクセス ポイント	1-3
ブリッジ	1-4
ワークグループブリッジ	1-5
全ワイヤレス ネットワークの中央ユニット	1-6

---

### 第 2 章

<b>Web ブラウザ インターフェイスの使用法</b>	<b>2-1</b>
初めて Web ブラウザ インターフェイスを使用する場合	2-2
Web ブラウザ インターフェイスの管理ページの使用法	2-2
アクション ボタンの使用法	2-3
入力フィールドの文字制限	2-4
安全なブラウザ利用のための HTTPS の有効化	2-5
HTTPS 証明書の削除	2-7
オンライン ヘルプの使用法	2-8
ヘルプ ファイルの場所の変更	2-8
Web ブラウザ インターフェイスの無効化	2-9

## 第 3 章

<b>コマンドライン インターフェイスの使用</b>	<b>3-1</b>
Cisco IOS コマンド モード	3-2
ヘルプの表示	3-3
コマンドの短縮形	3-4
コマンドの no 形式および default 形式の使用	3-4
CLI メッセージの概要	3-4
コマンド履歴の使用方法	3-5
コマンド履歴バッファ サイズの変更	3-5
コマンドの呼び出し	3-5
コマンド履歴機能のディセーブル化	3-6
編集機能の使用方法	3-6
編集機能のイネーブル化およびディセーブル化	3-6
キー入力によるコマンドの編集	3-7
画面幅よりも長いコマンドラインの編集	3-8
show および more コマンド出力の検索およびフィルタリング	3-9
CLI のアクセス	3-9
Telnet を使用して CLI を開く	3-9
セキュアシェルを使用して CLI を開く	3-10

## 第 4 章

<b>アクセス ポイントの最初の設定</b>	<b>4-1</b>
はじめる前に	4-2
デバイスのデフォルト設定へのリセット	4-2
MODE ボタンを使用したデフォルト設定へのリセット	4-2
GUI を使用したデフォルト設定へのリセット	4-3
CLI を使用したデフォルト設定へのリセット	4-3
アクセス ポイントへのログイン	4-4
IP アドレスの取得と割り当て	4-4
デフォルトの IP アドレスの動作	4-5
1130 シリーズのアクセス ポイントへのローカル接続	4-5
1040、1140、1240、1250、1260、および 2600 シリーズのアクセス ポイントへのローカル接続	4-6
1300 シリーズのアクセス ポイント / ブリッジへのローカル接続	4-7
デフォルトの無線設定	4-8
基本設定の割り当て	4-8
[Easy Setup] ページのデフォルト設定	4-12
セキュリティ設定の概要	4-13
VLAN の使用	4-14
SSID のセキュリティ タイプ	4-14



セキュリティ設定の制限事項	4-16
CLI の設定例	4-16
アクセス ポイントでのシステム電力の設定	4-23
AC 電源アダプタの使用	4-23
IEEE 802.3af 電力ネゴシエーションのスイッチ機能の使用	4-23
IEEE 802.3af 電力ネゴシエーションに対応していないスイッチの使用	4-23
電力インジェクタの使用	4-23
dot11 extension power native コマンド	4-24
802.3af 標準 PoE を備える 1250 シリーズ アクセス ポイントでの 802.11n パフォーマンスのサポート	4-24
1250 シリーズの電力モード	4-24
3600 シリーズ アクセス ポイントでの 802.11ac のサポート	4-25
802.11ac の電源管理	4-26
CLI を使用した IP アドレスの割り当て	4-27
Telnet セッションを使用した CLI へのアクセス	4-27
802.1X サブリカントの設定	4-28
クレデンシャルプロファイルの作成	4-28
インターフェイスまたは SSID にクレデンシャルを適用する方法	4-29
クレデンシャルプロファイルを有線ポートに適用する方法	4-29
アップリンクに使用する SSID にクレデンシャルプロファイルを適用する方法	4-30
EAP 方式プロファイルの作成と適用	4-30
IPv6 の設定	4-31
DHCPv6 アドレスの設定	4-32
IPv6 ネイバー探索	4-33
IPv6 アクセス リストの設定	4-34
RADIUS の設定	4-35
IPv6 WDS のサポート	4-35
CDPv6 サポート	4-36
RA フィルタリング	4-36

## 第 5 章

アクセス ポイントの管理	5-1
MODE ボタンの無効化	5-2
アクセス ポイントへの不正アクセスの防止	5-3
特権 EXEC コマンドへのアクセスの保護	5-3
デフォルトのパスワードおよび権限レベル設定	5-4
スタティック イネーブルパスワードの設定または変更	5-4
暗号化によるイネーブルおよびイネーブルシークレットパスワードの保護	5-5
ユーザ名とパスワードのペアの設定	5-7

複数の特権レベルの設定	5-8
コマンドの特権レベルの設定	5-9
特権レベルへのログインと終了	5-10
[Easy Setup] の設定	5-10
Spectrum Expert モードの設定	5-11
RADIUS によるアクセス ポイントへのアクセスの制御	5-12
RADIUS のデフォルト設定	5-12
RADIUS ログイン認証の設定	5-12
AAA サーバグループの定義	5-14
ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定	5-16
RADIUS の設定の表示	5-17
TACACS+ によるアクセス ポイントへのアクセスの制御	5-17
TACACS+ のデフォルト設定	5-18
TACACS+ ログイン認証の設定	5-18
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定	5-20
TACACS+ 設定の表示	5-20
イーサネットの速度およびデュプレックスの設定	5-21
アクセス ポイントの無線ネットワーク管理の設定	5-21
アクセス ポイントのローカル認証および許可の設定	5-22
認証キャッシュとプロファイルの設定	5-23
DHCP サービスを提供するためのアクセス ポイントの設定	5-25
DHCP サーバの設定	5-25
DHCP サーバアクセス ポイントのモニタリングと維持	5-27
show コマンド	5-27
clear コマンド	5-28
debug コマンド	5-28
アクセス ポイントのセキュア シェルの設定	5-28
SSH について	5-28
SSH の設定	5-29
セキュア コピー プロトコルのサポート	5-29
クライアント ARP キャッシングの設定	5-29
クライアント ARP キャッシングの概要	5-30
オプションの ARP キャッシング	5-30
ARP キャッシングの設定	5-30
システム日時の管理	5-31
簡易ネットワーク タイム プロトコルの概要	5-31
SNTP の設定	5-32

手動での日時の設定	5-32
システムクロックの設定	5-32
日時設定の表示	5-33
タイムゾーンの設定	5-33
夏時間の設定	5-34
HTTP アクセスの定義	5-36
システム名およびプロンプトの設定	5-36
デフォルトのシステム名およびプロンプトの設定	5-36
システム名の設定	5-36
DNS の概要	5-37
DNS のデフォルト設定	5-38
DNS の設定	5-38
DNS の設定の表示	5-39
バナーの作成	5-39
バナーのデフォルト設定	5-39
MoTD ログインバナーの設定	5-39
ログインバナーの設定	5-40
自律 Cisco Aironet アクセスポイントを Lightweight モードにアップグレードする 方法	5-41
日本の W52 ドメインへの移行方法	5-42
移行の確認	5-43
ポイントツーマルチポイントブリッジにおける複数の VLAN とレート制限の 設定	5-43
CLI コマンド	5-44

## 第 6 章

## 無線の設定 6-1

無線インターフェイスのイネーブル化	6-2
無線ネットワークの役割の設定	6-2
ユニバーサルワークグループブリッジモード	6-5
802.11n プラットフォームのポイントツーポイントおよびマルチポイントブ リッジのサポート	6-5
デュアル無線フォールバックの設定	6-6
無線トラッキング	6-7
ファストイーサネットトラッキング	6-7
MAC アドレストラッキング	6-8
サポートされないブリッジ機能	6-8
無線データレートの設定	6-8
マルチキャストフレームと管理フレームを最高の Basic レートで送信するアクセ スポイント	6-9

MCS レートの設定	6-12
無線の送信電力の設定	6-13
アソシエートしたクライアント デバイスの電力レベルの制限	6-15
無線チャネルの設定	6-17
802.11n のチャネル幅	6-18
Dynamic Frequency Selection (動的周波数選択)	6-19
DFS チャネルでのレーダー検出	6-20
CLI コマンド	6-21
DFS が有効に設定されているかどうかの確認	6-21
チャネルの設定	6-21
DFS 選択によるチャネルブロック	6-22
802.11n ガード間隔の設定	6-23
位置情報サービスの設定	6-24
位置情報サービスの概要	6-24
アクセスポイントへの LBS の設定	6-25
ワールド モードのイネーブル化とディセーブル化	6-26
short 無線プリアンプルのイネーブル化とディセーブル化	6-27
送受信アンテナの設定	6-27
Gratuitous Probe Response の有効化と無効化	6-29
Aironet 拡張機能のディセーブル化およびイネーブル化	6-30
イーサネット カプセル化変換方式の設定	6-31
ワークグループ ブリッジへの信頼性のあるマルチキャストの有効化と無効化	6-32
Public Secure Packet Forwarding のイネーブル化とディセーブル化	6-33
保護ポートの設定	6-34
ビーコン間隔と DTIM の設定	6-34
RTS しきい値と再試行回数の設定	6-35
最大データ再試行回数の設定	6-36
フラグメンテーションしきい値の設定	6-36
802.11g 無線の short スロット時間のイネーブル化	6-37
キャリア話中検査の実行	6-37
VoIP パケット処理の設定	6-37
VoWLAN メトリックの表示	6-38
音声レポートの表示	6-39
無線クライアントレポートの表示	6-41
音声障害の要約の表示	6-42
音声の QoS 設定	6-43
音声障害の設定	6-44

ClientLink の設定	6-45
CLI を使用した ClientLink の設定	6-45
無線機能のデバッグ	6-46

## 第 7 章

<b>複数の SSID の設定</b>	<b>7-1</b>
複数の SSID の概要	7-2
ソフトウェア バージョンの SSID に対する影響	7-2
複数の SSID の設定	7-4
デフォルトの SSID 設定	7-4
SSID のグローバルな作成	7-4
グローバルに設定された SSID の表示	7-7
SSID でのスペースの使用	7-7
RADIUS サーバを使用した SSID の制限	7-8
複数の基本 SSID の設定	7-9
複数 BSSID の設定要件	7-9
複数の BSSID を使用する際のガイドライン	7-9
複数の BSSID の設定	7-10
CLI の設定例	7-11
設定済み BSSID の表示	7-12
SSID に対する IP リダイレクションの割り当て	7-12
IP リダイレクションを使用する際のガイドライン	7-13
IP リダイレクションの設定	7-13
SSID IE への SSID の追加	7-15
MBSSID の NAC サポート	7-15
MBSSID への NAC 設定	7-17

## 第 8 章

<b>スパニングツリー プロトコルの設定</b>	<b>8-1</b>
スパニングツリー プロトコルの概要	8-2
STP の概要	8-2
1300 および 350 シリーズ ブリッジの相互運用性	8-3
アクセス ポイント / ブリッジのプロトコル データ ユニット	8-3
スパニングツリー ルートの選択	8-4
スパニングツリー タイマー	8-5
スパニングツリー トポロジの作成	8-5
スパニングツリー インターフェイス ステート	8-6
ブロッキング ステート	8-7
リスニング ステート	8-8
ラーニング ステート	8-8
フォワーディング ステート	8-8

ディセーブルステート	8-8
STP 機能の設定	8-9
STP のデフォルト設定	8-9
STP の設定	8-10
STP の設定例	8-11
VLAN を使用しないルートブリッジ	8-11
VLAN を使用しない非ルートブリッジ	8-12
VLAN を使用するルートブリッジ	8-12
VLAN を使用する非ルートブリッジ	8-14
スパンニングツリーステータスの表示	8-15

## 第 9 章

<b>ローカル認証サーバとしてのアクセスポイントの設定</b>	<b>9-1</b>
ローカル認証の概要	9-2
ローカル認証サーバの設定	9-2
ローカル認証サーバに対するガイドライン	9-3
コンフィギュレーションの概要	9-3
ローカル認証サーバアクセスポイントの設定	9-4
他のアクセスポイントがローカル認証サーバを使用するための設定	9-6
EAP-FAST の設定	9-7
PAC の設定	9-7
機関 ID の設定	9-8
サーバキーの設定	9-9
アクセスポイントのクロックが原因で発生する PAC の失敗	9-9
ローカル認証サーバにおける認証タイプの制限	9-9
ロックされたユーザ名のロック解除	9-10
ローカル認証サーバ統計情報の表示	9-10
デバッグメッセージの使用	9-11

## 第 10 章

<b>暗号スイートと WEP の設定</b>	<b>10-1</b>
暗号スイートと WEP の概要	10-2
暗号スイートと WEP の設定	10-3
WEP キーの作成	10-4
WEP キーの制限	10-5
WEP キーの設定例	10-6
暗号スイートと WEP の有効化	10-6
WPA または CCKM に一致する暗号スイート	10-7
ブロードキャストキーローテーションの有効化と無効化	10-8

## 第 11 章

**認証タイプの設定** 11-1

## 認証タイプの概要 11-2

アクセスポイントに対する Open 認証 11-2

アクセスポイントに対する Shared Key 認証 11-3

ネットワークに対する EAP 認証 11-4

ネットワークに対する MAC アドレス認証 11-5

MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ 11-6

認証されたクライアントの CCKM の利用 11-6

WPA キー管理の使用 11-7

WPA、CCKM、CKIP、および WPA-TKIP のソフトウェアおよびファームウェア要件 11-8

## 認証タイプの設定 11-10

SSID への認証タイプの割り当て 11-10

WPA 移行モードの設定 11-13

追加の WPA の設定 11-14

MAC 認証キャッシングの設定 11-15

認証のホールドオフ、タイムアウト、間隔の設定 11-16

802.1X サブリカントの EAP 方式プロファイルの作成と適用 11-18

EAP 方式プロファイルの作成 11-18

ファスト イーサネット インターフェイスに対する EAP プロファイルの適用 11-18

アップリンク SSID に対する EAP プロファイルの適用 11-19

アクセスポイントとクライアント デバイスの認証タイプのマッチング 11-19

ゲスト アクセス管理 11-23

ゲスト アカウントの作成 11-25

## 第 12 章

**WDS、高速安全ローミング、無線管理、および Wireless Intrusion Detection Service の設定** 12-1

## WDS の概要 12-2

WDS デバイスの役割 12-2

WDS デバイスを使用したアクセスポイントの役割 12-3

高速安全ローミングの概要 12-3

無線管理の概要 12-5

レイヤ 3 モビリティの概要 12-5

Wireless Intrusion Detection Service の概要 12-7

## WDS の設定 12-8

WDS のガイドライン 12-8

WDS の要件 12-8

コンフィギュレーションの概要 12-9



アクセスポイントを潜在的な WDS デバイスとして設定する	12-10
CLI の設定例	12-13
アクセスポイントを WDS デバイスを使用するように設定する	12-14
CLI の設定例	12-15
認証サーバが WDS をサポートするように設定する	12-15
WDS 専用モードの設定	12-19
WDS 情報の表示	12-20
デバッグメッセージの使用	12-21
高速安全ローミングの設定	12-21
高速安全ローミングの要件	12-21
高速安全ローミングをサポートするアクセスポイントの設定	12-22
CLI の設定例	12-24
802.11r のサポート	12-24
管理フレーム保護の設定	12-25
Management Frame Protection	12-26
概要	12-26
ユニキャスト管理フレームの保護	12-26
ブロードキャスト管理フレームの保護	12-27
ルートモードのアクセスポイントのクライアント MFP	12-27
クライアント MFP の設定	12-27
802.11w による管理フレーム保護	12-29
無線管理の設定	12-30
CLI の設定例	12-31
WIDS に参加するようにアクセスポイントを設定する	12-32
アクセスポイントをスキャナモードに設定する	12-32
アクセスポイントをモニタモードに設定する	12-32
モニタモード統計の表示	12-33
モニタモード制限の設定	12-34
認証失敗制限の設定	12-34

## 第 13 章

**RADIUS サーバと TACACS+ サーバの設定** 13-1

RADIUS の設定と有効化	13-1
RADIUS の概要	13-2
RADIUS の動作	13-2
RADIUS の設定	13-3
RADIUS のデフォルト設定	13-4
RADIUS サーバホストの識別	13-4
RADIUS ログイン認証の設定	13-7
AAA サーバグループの定義	13-9

ユーザイネーブルアクセスおよびネットワーク サービスに関する RADIUS 許可の設定	13-11
パケット オブ ディスコネクトの設定	13-12
RADIUS アカウンティングの開始	13-13
CSID 形式の選択	13-14
すべての RADIUS サーバの設定	13-15
ベンダー固有の RADIUS 属性を使用するアクセス ポイントの設定	13-16
ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定	13-17
WISPr RADIUS 属性の設定	13-18
RADIUS の設定の表示	13-19
アクセス ポイントが送信する RADIUS 属性	13-19
TACACS+ の設定と有効化	13-22
TACACS+ の概要	13-22
TACACS+ の動作	13-23
「Configuring TACACS+」	13-24
TACACS+ のデフォルト設定	13-24
TACACS+ サーバホストの特定および認証キーの設定	13-24
TACACS+ ログイン認証の設定	13-25
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定	13-27
TACACS+ アカウンティングの起動	13-28
TACACS+ 設定の表示	13-28
<b>第 14 章</b>	
<b>VLAN の設定</b>	<b>14-1</b>
VLAN の概要	14-2
関連資料	14-3
VLAN への無線デバイスの組み込み	14-4
VLAN の設定	14-4
VLAN の設定	14-5
VLAN への名前の割り当て	14-7
VLAN 名を使用する際のガイドライン	14-7
VLAN 名の作成	14-8
Remote Authentication Dial-In User Service (RADIUS) サーバを使用した VLAN へのユーザの割り当て	14-8
RADIUS サーバを使用した動的モビリティグループ割り当て	14-9
アクセス ポイントに設定された VLAN の表示	14-9
VLAN の設定例	14-10

## 第 15 章

**QoS の設定** 15-1

無線 LAN の QoS の概要	15-2
無線 LAN の QoS と有線 LAN の QoS	15-2
無線 LAN への QoS の影響	15-3
QoS 設定の優先順位	15-3
Wi-Fi Multimedia モードの使用方法	15-4
バンド選択の使用	15-5
QoS の設定	15-6
設定時の注意事項	15-6
Web ブラウザ インターフェイスを使用した QoS の設定	15-7
[QoS Policies Advanced] ページ	15-11
QoS Element for Wireless Phones	15-11
IGMP スヌーピング	15-12
AVVID 優先順位マッピング	15-12
WiFi Multimedia (WMM)	15-12
Rate Limiting	15-12
無線アクセス カテゴリの調整	15-13
公称レートの設定	15-14
最適化された音声設定	15-15
コールアドミッション制御の設定	15-15
QoS 設定例	15-16
音声トラフィックの優先指定	15-17
ビデオトラフィックの優先指定	15-18

## 第 16 章

**フィルタの設定** 16-1

フィルタの概要	16-2
CLI を使用したフィルタの設定	16-2
Web ブラウザ インターフェイスを使ったフィルタの設定	16-3
MAC アドレス フィルタの設定と有効化	16-3
MAC アドレス フィルタの作成	16-4
MAC アドレス ACL を使用したアクセス ポイントへのクライアント アソシエーションの許可と禁止	16-7
Time-Based ACL の作成	16-9
ACL ロギング	16-10
CLI の設定例	16-10
IP フィルタの設定と有効化	16-10
IP フィルタの作成	16-12
EtherType フィルタの設定と有効化	16-14
EtherType フィルタの作成	16-15

## 第 17 章

**CDP の設定** 17-1

- CDP の概要 17-2
- CDP の設定 17-2
  - CDP のデフォルト設定 17-2
  - CDP 特性の設定 17-2
  - CDP のディセーブル化およびイネーブル化 17-3
  - インターフェイス上での CDP のディセーブル化およびイネーブル化 17-4
- CDP のモニタおよびメンテナンス 17-5

## 第 18 章

**SNMP の設定** 18-1

- SNMP の概要 18-2
  - SNMP バージョン 18-2
  - SNMP マネージャ機能 18-3
  - SNMP エージェント機能 18-4
  - SNMP コミュニティストリング 18-4
  - SNMP を使用して MIB 変数にアクセスする方法 18-4
- SNMP の設定 18-5
  - SNMP のデフォルト設定 18-5
  - SNMP エージェントのイネーブル化 18-6
  - コミュニティストリングの設定 18-6
  - SNMP サーバグループ名の指定 18-8
  - SNMP サーバホストの設定 18-8
  - SNMP サーバユーザの設定 18-8
  - トラップ マネージャの設定とトラップの有効化 18-9
  - エージェント コンタクトおよびロケーションの設定 18-11
  - snmp-server view コマンドの使用 18-11
  - SNMP での例 18-11
- SNMP ステータスの表示 18-13

## 第 19 章

**リピータ/スタンバイ アクセス ポイントおよびワークグループブリッジ モードの設定** 19-1

- リピータ アクセス ポイントの概要 19-2
- リピータ アクセス ポイントの設定 19-3
  - デフォルト設定 19-4
  - リピータのガイドライン 19-4
  - リピータの設定 19-5
- アンテナの位置合わせ 19-7
  - リピータ操作の確認 19-7
  - リピータの LEAP クライアントとしての設定 19-7

リピータの WPA クライアントとしての設定	19-9
ホットスタンバイの概要	19-9
ホットスタンバイアクセスポイントの設定	19-10
スタンバイ操作の確認	19-13
ワークグループブリッジモードの概要	19-14
インフラストラクチャデバイスまたはクライアントデバイスとしてのワークグループブリッジの扱い	19-16
ローミング用ワークグループブリッジの設定	19-16
限定チャンネルスキャン用のワークグループブリッジの設定	19-17
限定チャンネルセットの設定	19-17
CCX ネイバーリストの無視	19-18
クライアント VLAN の設定	19-18
ワークグループブリッジの VLAN タギング	19-18
ワークグループブリッジモードの設定	19-19
Lightweight 環境でのワークグループブリッジの使用	19-21
ワークグループブリッジを Lightweight 環境で使用する際のガイドライン	19-21
ワークグループブリッジの設定例	19-23
ワークグループブリッジでの VideoStream サポートの有効化	19-24

## 第 20 章

<b>ファームウェアと設定の管理</b>	20-1
フラッシュファイルシステムの操作	20-1
使用可能なファイルシステムの表示	20-2
デフォルトファイルシステムの設定	20-3
ファイルシステム上のファイル情報の表示	20-3
ディレクトリの変更および作業ディレクトリの表示	20-4
ディレクトリの作成と削除	20-4
ファイルのコピー	20-5
ファイルの削除	20-5
tar ファイルの作成、表示、および抽出	20-6
tar ファイルの作成	20-6
tar ファイルの内容の表示	20-7
tar ファイルの抽出	20-7
ファイルの内容の表示	20-8
コンフィギュレーションファイルの操作	20-8
コンフィギュレーションファイルの作成および使用上の注意事項	20-9
コンフィギュレーションファイルのタイプおよび場所	20-10
テキストエディタによるコンフィギュレーションファイルの作成	20-10

TFTP によるコンフィギュレーション ファイルのコピー	20-10
TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	20-11
TFTP によるコンフィギュレーション ファイルのダウンロード	20-11
TFTP によるコンフィギュレーション ファイルのアップロード	20-12
FTP によるコンフィギュレーション ファイルのコピー	20-13
FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	20-13
FTP によるコンフィギュレーション ファイルのダウンロード	20-14
FTP によるコンフィギュレーション ファイルのアップロード	20-15
RCP によるコンフィギュレーション ファイルのコピー	20-16
RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備	20-17
RCP によるコンフィギュレーション ファイルのダウンロード	20-17
RCP によるコンフィギュレーション ファイルのアップロード	20-18
設定情報の消去	20-19
格納されたコンフィギュレーション ファイルの削除	20-20
ソフトウェア イメージの操作	20-20
アクセス ポイントのイメージの場所	20-21
サーバまたは Cisco.com 上のイメージの tar ファイル形式	20-21
TFTP によるイメージ ファイルのコピー	20-21
TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備	20-22
TFTP によるイメージ ファイルのダウンロード	20-23
TFTP によるイメージ ファイルのアップロード	20-24
FTP によるイメージ ファイルのコピー	20-25
FTP によるイメージ ファイルのダウンロードまたはアップロードの準備	20-25
FTP によるイメージ ファイルのダウンロード	20-26
FTP によるイメージ ファイルのアップロード	20-29
RCP によるイメージ ファイルのコピー	20-30
RCP によるイメージ ファイルのダウンロードまたはアップロードの準備	20-30
RCP によるイメージ ファイルのダウンロード	20-31
RCP によるイメージ ファイルのアップロード	20-34
Web ブラウザ インターフェイスによるイメージのリロード	20-35
ブラウザ HTTP インターフェイス	20-35
ブラウザ TFTP インターフェイス	20-35

## 第 21 章

<b>システム メッセージ ログिंगの設定</b>	<b>21-1</b>
システム メッセージ ログिंगの概要	21-2
システム メッセージ ログिंगの設定	21-2
システム ログ メッセージのフォーマット	21-2
システム メッセージ ログिंगのデフォルト設定	21-3
メッセージ ログिंगのディセーブル化とイネーブル化	21-4
メッセージ表示宛先デバイスの設定	21-5
ログ メッセージのタイムスタンプのイネーブル化とディセーブル化	21-6
ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化	21-7
メッセージ重大度の定義	21-7
履歴テーブルおよび SNMP に送信される Syslog メッセージの制限	21-9
ログングレート制限の設定	21-10
UNIX Syslog サーバの設定	21-10
UNIX Syslog デーモンへのメッセージのログング	21-10
UNIX システム ログング機能の設定	21-11
ログング設定の表示	21-12

## 第 22 章

<b>トラブルシューティング</b>	<b>22-1</b>
LED インジケータ	22-2
電力チェック	22-2
低電力状態	22-2
基本設定の確認	22-3
SSID	22-3
WEP キー	22-3
セキュリティ設定	22-3
デフォルト設定へのリセット	22-4
MODE ボタンの使用	22-4
Web ブラウザ インターフェイスの使用法	22-5
CLI の使用	22-6
アクセス ポイントのイメージのリロード	22-7
MODE ボタンの使用	22-7
Web ブラウザ インターフェイスの使用法	22-8
ブラウザ HTTP インターフェイス	22-8
ブラウザ TFTP インターフェイス	22-9
CLI の使用	22-10
アクセス ポイントのイメージ ファイルの入手	22-12
TFTP サーバソフトウェアの入手	22-12
1520 アクセス ポイントでのイメージの復元	22-12



## 付録 A

## プロトコルフィルタ A-1

## 付録 B

## サポート対象 MIB B-1

MIB の一覧 B-1

FTP による MIB ファイルへのアクセス B-2

## 付録 C

## エラーメッセージおよびイベント メッセージ C-1

表記法 C-2

ソフトウェア自動アップグレード メッセージ C-3

アソシエーション管理メッセージ C-5

解凍メッセージ C-7

システム ログ メッセージ C-7

802.11 サブシステム メッセージ C-8

アクセス ポイント間プロトコル メッセージ C-22

ローカル認証サーバ メッセージ C-23

WDS メッセージ C-25

ミニ IOS メッセージ C-26

アクセス ポイントまたはブリッジについてのメッセージ C-27

Cisco Discovery Protocol メッセージ C-28

外部 RADIUS サーバエラー メッセージ C-28

LWAPP エラー メッセージ C-28

センサー メッセージ C-29

SNMP エラー メッセージ C-30

SSH エラー メッセージ C-31

## 用語集





## はじめに

---

### 対象読者

このガイドは、自律モードの Cisco Aironet アクセス ポイントをインストールして管理するネットワークの専門家を対象にしています。このガイドを読むには、Cisco IOS ソフトウェアの操作経験があり、無線ローカル エリア ネットワークの概念と用語をよく知っている必要があります。

このガイドは、Cisco IOS リリース 15.2(4)JB3a について説明しています。サポートされているアクセス ポイント プラットフォームは以下のとおりです。

- AP 702
- AP 802
- AP 1040
- AP 1140
- AP 1260
- AP 1530
- AP 1550
- AP 1600
- AP 2600
- AP 3500
- AP 3600
- AP 3700 (サイト調査のみ)

Cisco Aironet 1530 シリーズのアクセス ポイントの場合のみ、Cisco IOS バージョン 15.2(4)JB3b をロードする必要があります。この IOS バージョンは、Cisco Aironet 1530 シリーズのアクセス ポイントにのみ適用されます。



(注)

このガイドには、Lightweight アクセス ポイントについての説明はありません。これらのデバイスの設定方法については、Cisco.com で該当するインストール ガイドおよびコンフィギュレーション ガイドを参照できます。

## 目的

このガイドには、アクセス ポイントをインストールして、設定するために必要な情報を記載してあります。また、アクセス ポイントで使用するために作成され、変更された Cisco IOS ソフトウェア コマンドを使用する手順について説明します。これらのコマンドの詳細は扱いません。これらのコマンドに関する詳細については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。標準の Cisco IOS ソフトウェア コマンドについては、Cisco.com のホームページの [Support] > [Documentation] から入手できる Cisco IOS ソフトウェアのドキュメンテーションを参照してください。

このガイドでは、コマンドライン インターフェイス (CLI) の全機能をカバーしている Access Point Web-based Interface (APWI; アクセス ポイントの Web ベース インターフェイス) の概要についても説明します。このガイドには、APWI ウィンドウのフィールドレベルの説明、および APWI からアクセス ポイントを設定する手順については記載していません。APWI ウィンドウのすべての説明と操作手順については、アクセス ポイントのオンライン ヘルプを参照してください。オンライン ヘルプは、APWI ページの [Help] ボタンをクリックすると表示されます。

## 設定手順と例

このマニュアルに記載されている手順と例は、Cisco Aironet 3600 シリーズ アクセス ポイントに基づいて文書化されています。

最新の設定例を確認するには、Cisco Tech Zone (<https://techzone.cisco.com>) にアクセスしてください。Tech Zone の [Navigator] で、[Wireless LAN] > [Autonomous APs (IOS)] の自律 (IOS) 無線展開に関するナレッジ ベースを参照してください。



(注)

Cisco Tech Zone にアクセスするには、Cisco.com のアカウントが必要です。アカウントがない場合は、[Log In] ページで [Register Now] をクリックすると、アカウントを作成できます。

## マニュアルの構成

このガイドは次の章にわかれています。

**第 1 章「アクセス ポイント機能の概要」**では、アクセス ポイントのソフトウェアとハードウェアの機能を挙げ、ネットワークでのアクセス ポイントの役割について説明します。

**第 2 章「Web ブラウザ インターフェイスの使用法」**では、Web ブラウザ インターフェイスを使用してアクセス ポイントを設定する方法について説明します。

**第 3 章「コマンドライン インターフェイスの使用」**では、コマンドライン インターフェイス (CLI) を使用してアクセス ポイントを設定する方法について説明します。

**第 4 章「アクセス ポイントの最初の設定」**では、新しいアクセス ポイントに基本設定を行う手順について説明します。

**第 5 章「アクセス ポイントの管理」**では、アクセス ポイントへの不正なアクセスの防止、システムの日時の設定、システム名とプロンプトの設定など、アクセス ポイントを管理する 1 限りの操作を実行する方法について説明します。

**第 6 章「無線の設定」**では、無線ネットワーク内での役割、送信電力、チャネル設定など、アクセス ポイント無線の設定方法について説明します。

[第 7 章「複数の SSID の設定」](#)では、アクセスポイントに複数のサービスセット ID (SSID) と複数の基本サービスセット ID (BSSID) を設定して、管理する方法について説明します。アクセスポイントには最大 16 個の SSID と最大 8 個の BSSID を設定できます。

[第 8 章「スパニングツリープロトコルの設定」](#)では、アクセスポイント、ブリッジ、またはブリッジモードで稼働するアクセスポイントにスパニングツリープロトコル (STP) を設定する方法について説明します。STP を使用すると、ネットワーク内でのブリッジループの発生を防ぐことができます。

[第 9 章「ローカル認証サーバとしてのアクセスポイントの設定」](#)では、無線 LAN 用のローカル Remote Authentication Dial-In User Service (RADIUS) サーバとして機能するアクセスポイントの設定方法について説明します。メインの RADIUS サーバへの WAN 接続に障害が発生した場合、アクセスポイントはバックアップサーバとして機能し、無線デバイスを認証します。

[第 10 章「暗号スイートと WEP の設定」](#)では、認証済みキー管理に必要な暗号スイート、Wired Equivalent Privacy (WEP)、および Message Integrity Check (MIC; メッセージ完全性チェック)、Cisco Message Integrity Check (CMIC)、Temporal Key Integrity Protocol (TKIP)、Cisco Key Integrity Protocol (CKIP)、ブロードキャストキーローテーションなどの WEP 機能の設定方法について説明します。

[第 11 章「認証タイプの設定」](#)では、アクセスポイントに認証タイプを設定する方法について説明します。クライアントデバイスは、これらの認証方式を使用してネットワークに接続します。

[第 12 章「WDS、高速安全ローミング、無線管理、および Wireless Intrusion Detection Service の設定」](#)では、WDS に参加し、クライアントサービスのローミングで高速な再アソシエーションを可能にしたうえ、無線管理に参加させるためのアクセスポイントの設定方法について説明します。

[第 13 章「RADIUS サーバと TACACS+ サーバの設定」](#)では、RADIUS と Terminal Access Controller Access Control System Plus (TACACS+) を有効にして設定する方法について説明します。RADIUS と TACACS+ は、認証プロセスと許可プロセスに詳細なアカウント情報と柔軟な管理制御を提供します。

[第 14 章「VLAN の設定」](#)では、有線 LAN で設定された VLAN と相互運用するようにアクセスポイントを設定する方法について説明します。

[第 15 章「QoS の設定」](#)では、Web ブラウザ インターフェイスを使用してアクセスポイントに MAC アドレス、IP、および EtherType のフィルタを設定して管理する方法について説明します。

[第 16 章「フィルタの設定」](#)では、Web ブラウザ インターフェイスを使用してアクセスポイントに MAC アドレス、IP、および EtherType のフィルタを設定して管理する方法について説明します。

[第 17 章「CDP の設定」](#)では、アクセスポイントに Cisco Discovery Protocol (CDP) を設定する方法について説明します。CDP はすべてのシスコ ネットワーク装置で稼働するデバイス検出プロトコルです。

[第 18 章「SNMP の設定」](#)では、アクセスポイントに簡易ネットワーク管理プロトコル (SNMP) を設定する方法について説明します。

[第 19 章「リピータ/スタンバイ アクセスポイントおよびワークグループブリッジモードの設定」](#)では、アクセスポイントをホットスタンバイユニットまたはリピータユニットとして設定する方法について説明します。

[第 20 章「ファームウェアと設定の管理」](#)では、フラッシュファイルシステムの操作方法、コンフィギュレーションファイルのコピー方法、ソフトウェアイメージのアーカイブ (アップロードとダウンロード) 方法について説明します。

[第 21 章「システム メッセージ ロギングの設定」](#)では、アクセスポイントにシステム メッセージ ロギングを設定する方法について説明します。

第 22 章「トラブルシューティング」では、アクセス ポイントの基本的な問題に対するトラブルシューティング手順を説明します。

付録 A「プロトコルフィルタ」では、アクセス ポイントでフィルタリングできるプロトコルのリストを示します。

付録 B「サポート対象 MIB」では、アクセス ポイントがこのソフトウェア リリースでサポートする簡易ネットワーク管理プロトコル (SNMP) の管理情報ベース (MIB) のリストを示します。

付録 C「エラー メッセージおよびイベント メッセージ」では、CLI エラー メッセージおよびイベント メッセージのリストを示し、各メッセージの説明とその推奨処置を提示します。

## 表記法

このマニュアルでは、次の表記法を使用して説明および情報を表示しています。

コマンドの説明では、次の表記法を使用しています。

- コマンドおよびキーワードは、**太字**で示しています。
- ユーザが値を指定する引数は、*イタリック体*で示しています。
- 角カッコ ([ ]) の中の要素は、省略可能です。
- 必ずいずれか 1 つを選択しなければならない要素は、波カッコ ({ }) で囲み、縦棒 (|) で区切って示しています。
- 任意で選択する要素の中で、必ずどれか 1 つを選択しなければならない要素は、角カッコと波カッコで囲み、縦棒で区切って ({|}) 示しています。

対話形式の例では、次の表記法を使用しています。

- 端末セッションおよびシステムの表示は、`screen` フォントで示しています。
- ユーザが入力する情報は、**太字の screen** フォントで示しています。
- パスワードやタブのように、出力されない文字は、山カッコ (<>) で囲んで示しています。

(注)、注意、およびワンポイントアドバイスには、次の表記法および記号を使用しています。



(注)

「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



ヒント

問題の解決に役立つ情報です。ヒントは、トラブルシューティングの方法や実行すべきアクションを示すものではなくても、役立つ情報を提供している場合があります。

## 関連資料

- 『Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.2(4)JB3a』
- サポートされるアクセス ポイントごとに、必要に応じて、Cisco.com の対応するサポート ページに以下のタイプのガイドが提供されています。
  - 『Access Point Getting Started Guide』
  - 『Access Point Hardware Installation Guide』 (『Getting Started Guide』 でハードウェアの設置について説明されていない場合のみ)
  - 『Installation Instructions for Cisco Aironet Power Injectors』
  - 『Access Point Deployment Guide』
  - 『Cisco Aironet 802.11 a/b/g/n/ac Radio Installation and Upgrade Instructions』

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>







# 第 1 章

## アクセス ポイント 機能の概要

Cisco Aironet アクセス ポイント（これ以降はアクセス ポイントまたは略して AP と呼ぶ）は、安全で安価な使いやすい無線 LAN ソリューションを提供します。これはモビリティと柔軟性のほかに、ネットワーキングの専門家が必要とする企業クラスの機能を併せ持っています。Cisco IOS ソフトウェアをベースにした管理システムでは、Cisco Aironet アクセス ポイントは、Wi-Fi 認定済みであり、特定のモデルによって、802.11a 準拠、802.11b 準拠、802.11g 準拠、802.11n 準拠、または 802.11ac 準拠の無線 LAN トランシーバになります。



(注)

1532 シリーズ AP は、初回の起動時に、統合モードのソフトウェア イメージを使用して起動されます。自律ネットワークに AP を展開するには、AP コンソールまたは Telnet から次のコマンドを使用して、自律モードのソフトウェア イメージで AP を再起動させます。

**capwap ap autonomous**

AP のソフトウェア イメージの詳細については、「ソフトウェア イメージの操作」(P.20-20) を参照してください。

ワイヤレス デバイスは、コマンドライン インターフェイス (CLI)、ブラウザベースの管理システム、または 簡易ネットワーク管理プロトコル (SNMP) を使用して設定およびモニタできます。

この章の内容は、次のとおりです。

- 「アクセス ポイントの無線」(P.1-1)
- 「リリースの新機能およびプラットフォーム」(P.1-2)
- 「管理オプション」(P.1-2)
- 「クライアント デバイスのローミング」(P.1-2)
- 「ネットワークの構成例」(P.1-3)

## アクセス ポイントの無線

アクセス ポイントは、無線ネットワークと有線ネットワーク間の接続ポイントとして、またはスタンドアロンの無線ネットワークのセントラル ポイントとして機能します。大規模な導入環境では、アクセス ポイントの無線範囲内であれば、無線ユーザは構内を移動しながらシームレスで遮断されないネットワーク アクセスを維持できます。

各アクセス ポイント プラットフォームには、1 台、2 台、または 3 台の無線が含まれます。各アクセス ポイント モデルでサポートされている無線の詳細については、そのモデルに対応するアクセス ポイント データ シートを参照してください。

# リリースの新機能およびプラットフォーム

このリリースでの新機能および既存の機能に対するアップデートについては、『*Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.2(4)JB3a*』を参照してください。

## 管理オプション

ワイヤレス デバイス管理システムは、次のインターフェイスから使用できます。

- Cisco IOS コマンドライン インターフェイス (CLI)。このインターフェイスはコンソールポートまたは Telnet セッションを通じて使用します。無線デバイスを無線コンフィギュレーション モードにするには、**interface dot11radio** グローバル コンフィギュレーション コマンドを使用します。このマニュアルのほとんどの例は、CLI から引用されています。[第3章「コマンドライン インターフェイスの使用」](#)に、CLI についての詳細が記載されています。
- Web ブラウザ インターフェイスは、Web ブラウザを介して使用します。[第2章「Web ブラウザ インターフェイスの使用方法」](#)に、Web ブラウザ インターフェイスについての詳細が記載されています。
- 簡易ネットワーク管理プロトコル (SNMP) .SNMP 管理のためのワイヤレス デバイスの設定方法については、[第18章「SNMP の設定」](#)を参照してください。

## クライアント デバイスのローミング

無線 LAN に複数のワイヤレス デバイスがある場合、無線クライアント デバイスは、あるワイヤレス デバイスから別の無線デバイスへとシームレスにローミングできます。ローミング機能は、近接度ではなく、信号の品質に基づきます。クライアントからの信号品質が低下すると、ローミングは別のアクセス ポイントに切り替わります。

クライアント デバイスが近くのアクセス ポイントにローミングせずに、遠くのアクセス ポイントにアソシエートしたままになることを懸念する無線 LAN ユーザがいます。ただし、遠隔のアクセス ポイントへのクライアントの信号が強度に維持され、信号品質が高い場合、クライアントはより近いアクセス ポイントにローミングしません。近接するアクセス ポイントを常にチェックするのは非効率であり、無線のトラフィックの増加により無線 LAN のスループットを低下させます。

無線分散システム (WDS) を提供するデバイスで Cisco Centralized Key Management (CCKM) または 802.11r を使用すると、クライアント デバイスはアクセス ポイント間をすばやくローミングできるため、音声やその他の時間が重要なアプリケーションで、知覚できるほどの遅延は生じません。

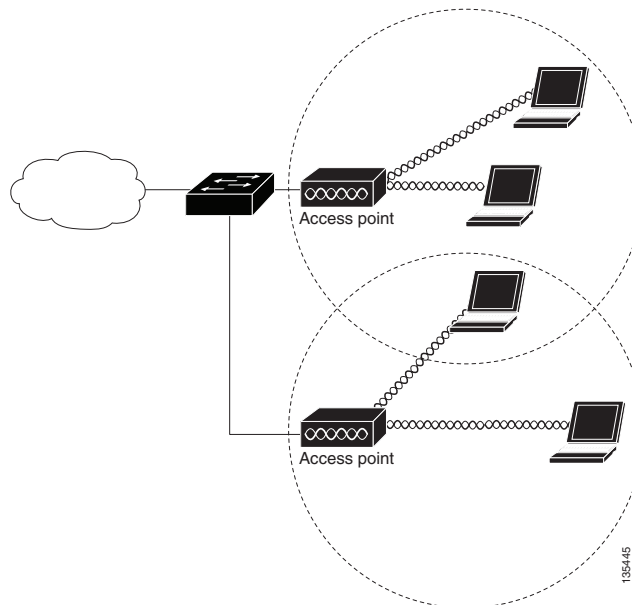
# ネットワークの構成例

この項では、一般的な無線ネットワーク構成でのアクセスポイントの役割について説明します。デフォルトでは、アクセスポイントは、ワイヤード LAN に接続したルートユニットとして、または完全なワイヤレス ネットワーク内のセントラル ユニットとして構成されます。アクセスポイントは、リピータ アクセスポイント、ブリッジ、およびワークグループとしても設定できます。これらの役割には特定の設定が必要です。

## ルート アクセスポイント

有線 LAN に直接接続されるアクセスポイントは、無線ユーザへの接続ポイントとして機能します。LAN に複数のアクセスポイントが接続されている場合、ユーザはネットワークへの接続を維持したまま、構内のエリアをローミングできます。1つのアクセスポイントの範囲外に移動したユーザは、自動的に別のアクセスポイントを経由してネットワークに接続（アソシエート）されます。ローミングプロセスはシームレスで、ユーザには意識されません。図 1-1 は、有線 LAN 上でルート ユニットとして機能するアクセスポイントを示しています。

図 1-1 有線 LAN 上でルート ユニットとして機能するアクセスポイント



## リピータ アクセスポイント

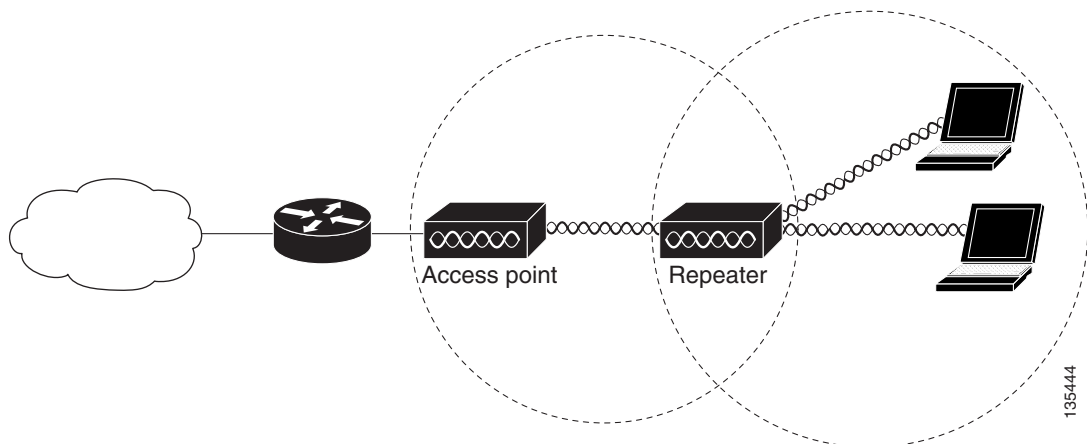
アクセスポイントは、インフラストラクチャの範囲を拡張したり、無線通信を妨害する障害を克服したりするスタンドアロン リピータとして設定できます。リピータは、別のリピータや、有線 LAN に接続されているアクセスポイントにパケットを送信することによって、無線ユーザと有線 LAN との間でトラフィックを転送します。データは、クライアントに最高のパフォーマンスを提供するルートを経由して送信されます。図 1-2 は、リピータとして機能するアクセスポイントを示しています。アクセスポイントをリピータとして設定する方法については、『「リピータ アクセスポイントの設定」(P.19-3)』を参照してください。



(注)

シスコ以外のクライアント デバイスを使用すると、リピータ アクセス ポイントとの通信に問題が生じる可能性があります。

図 1-2 リピータとして機能するアクセスポイント

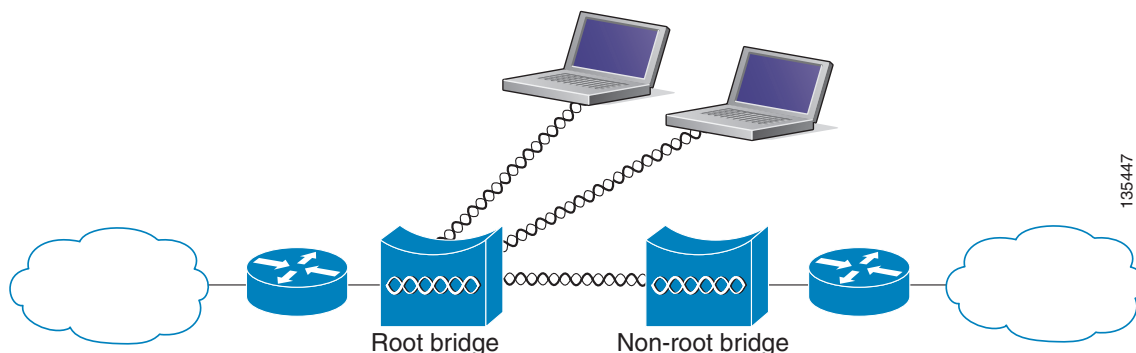


## ブリッジ

アクセスポイントは、ルートブリッジまたは非ルートブリッジとして設定できます。この役割では、アクセスポイントは非ルートブリッジとの無線リンクを確立します。トラフィックはリンク経由で有線 LAN に転送されます。ルートブリッジおよび非ルートブリッジの役割を持つアクセスポイントは、クライアントからのアソシエーションを受け入れるように設定できます。図 1-3 は、クライアントとのルートブリッジとして設定されたアクセスポイントを示しています。図 1-4 は、ルートブリッジおよび非ルートブリッジとして設定され、いずれもクライアントアソシエーションを受け付ける 2 つのアクセスポイントを示しています。アクセスポイントをブリッジとして設定する方法については、「無線ネットワークの役割の設定」(P.6-2) を参照してください。

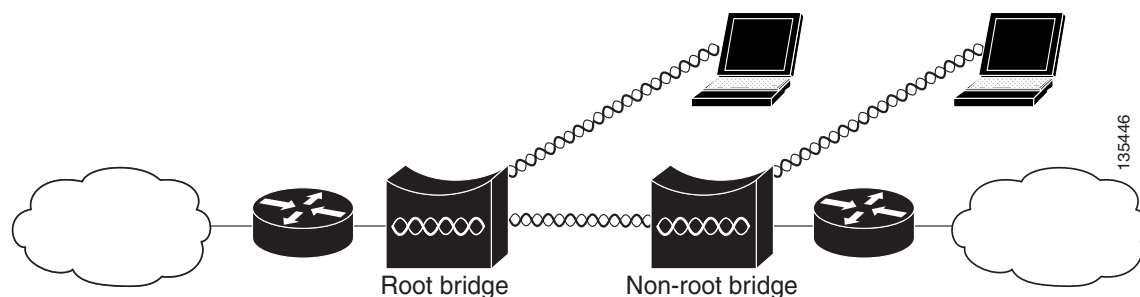
無線ブリッジがポイントツーマルチポイント構成に使用される場合、ルートブリッジにアソシエートする非ルートブリッジの数に応じてスループットは減少します。リンクのデータレートが 54 Mbps の場合、ポイントツーポイントリンクでの最大スループットは約 25 Mbps です。3 つのブリッジを追加してポイントツーマルチポイントネットワークを形成すると、スループットは約 12.5 Mbps に減少します。

図 1-3 クライアントとのルートブリッジとして機能するアクセスポイント



135447

図 1-4 クライアントとのルートブリッジおよび非ルートブリッジとして機能するアクセスポイント



135446

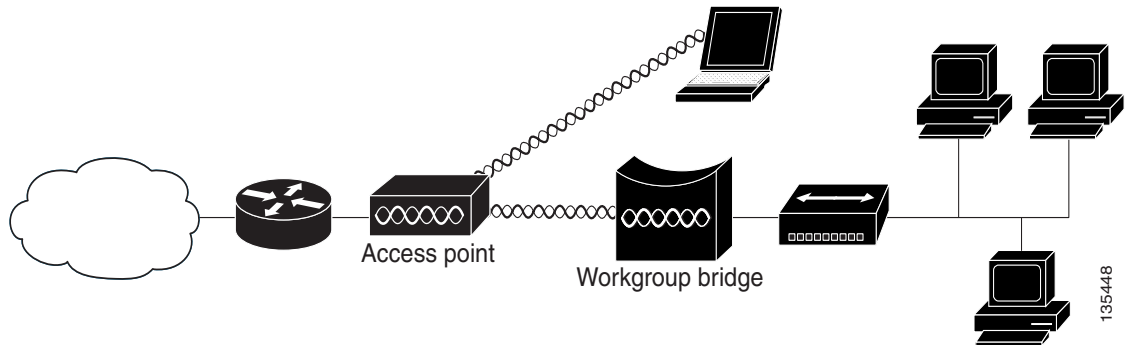
## ワークグループブリッジ

アクセスポイントをワークグループブリッジとして設定できます。ワークグループブリッジモードのアクセスポイントは、別のアクセスポイントにクライアントとしてアソシエートして、イーサネットポートに接続されたデバイスをネットワークに接続します。たとえば、ネットワークプリンタのグループを無線で接続する必要がある場合は、プリンタをハブまたはスイッチに接続し、ハブまたはスイッチをアクセスポイントのイーサネットポートに接続し、そのアクセスポイントをワークグループブリッジとして設定します。ワークグループブリッジはネットワーク上のアクセスポイントにアソシエートします。

アクセスポイントに複数の無線がある場合、いずれかの無線がワークグループブリッジモードとして機能できます。

図 1-5 は、ワークグループブリッジとして設定されたアクセスポイントを示しています。アクセスポイントをワークグループブリッジとして設定することについては、「[ワークグループブリッジモードの概要](#)」(P.19-14) および「[ワークグループブリッジモードの設定](#)」(P.19-19)を参照してください。

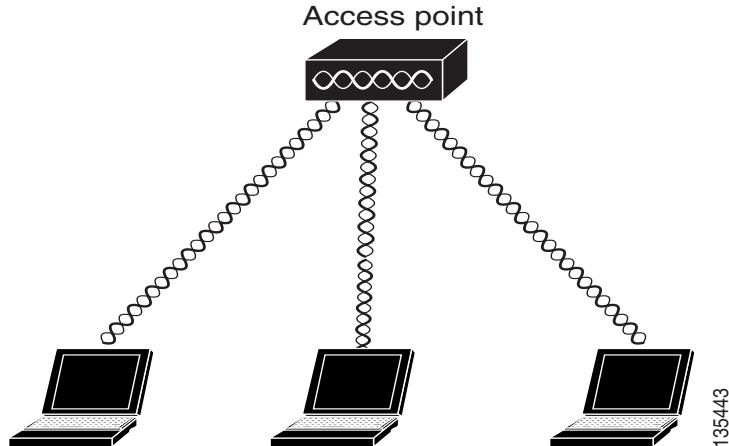
図 1-5 ワークグループブリッジとして機能するアクセスポイント



## 全ワイヤレス ネットワークの中央ユニット

完全なワイヤレス ネットワークでは、アクセス ポイントはスタンドアロンのルート ユニットとして機能します。アクセス ポイントは有線 LAN には接続されません。全ステーションをまとめてリンクするハブとして機能します。アクセス ポイントは通信の中心として機能し、無線ユーザの通信範囲を拡張します。図 1-6 は、完全なワイヤレス ネットワークでのアクセス ポイントを示しています。

図 1-6 完全なワイヤレス ネットワークでセントラル ユニットとして機能するアクセスポイント







## 第 2 章

# Web ブラウザ インターフェイスの使用方法

この章では、ワイヤレス デバイスの設定に使用できる Web ブラウザ インターフェイスについて説明します。この章の内容は、次のとおりです。

- 「初めて Web ブラウザ インターフェイスを使用する場合」 (P.2-2)
- 「Web ブラウザ インターフェイスの管理ページの使用方法」 (P.2-2)
- 「安全なブラウザ利用のための HTTPS の有効化」 (P.2-5)
- 「オンライン ヘルプの使用方法」 (P.2-8)
- 「Web ブラウザ インターフェイスの無効化」 (P.2-9)

Web ブラウザ インターフェイスには、ワイヤレス デバイスの設定の変更、ファームウェアのアップグレード、およびネットワーク上の他の無線デバイスのモニタと設定に使用する管理ページが含まれます。



(注)

ワイヤレス デバイスの Web ブラウザ インターフェイスは、Microsoft Internet Explorer バージョン 9.0 と Mozilla Firefox バージョン 17 と完全に互換性があります。



(注)

ワイヤレス デバイスの設定に、CLI と Web ブラウザ インターフェイスの両方を使用することは避けてください。CLI を使用してワイヤレス デバイスを設定した場合、Web ブラウザ インターフェイスでは、設定が正しく表示されない場合があります。しかし、正しく表示されない場合でも、ワイヤレス デバイスは正しく設定されていることがあります。

## 初めて Web ブラウザ インターフェイスを使用する場合

ワイヤレス デバイスの IP アドレスを使用して、管理システムを参照します。IP アドレスをワイヤレス デバイスに割り当てる方法は、「[アクセス ポイントへのログイン](#)」(P.4-4) を参照してください。Web ブラウザ インターフェイスの使用を開始する手順は、次のとおりです。

- 
- ステップ 1 ブラウザを起動します。
  - ステップ 2 アドレス バーにワイヤレス デバイスの IP アドレスを入力し、**Enter** キーを押します。  
[Summary Status] ページが表示されます。
- 

## Web ブラウザ インターフェイスの管理ページの使用方法

システム管理ページでの設定情報の表示と保存には、一貫性のある手法が使用されています。ページの上にあるナビゲーション バーを使用して、メイン メニューのオプションを選択できます。ページの左側にもナビゲーション バーがあります。これは、サブ メニューをナビゲートするために使用します。ナビゲーション バーは他の管理ページへ移動する場合に使用し、設定アクション ボタンは設定の変更を保存またはキャンセルする場合に使用します。



- 
- (注) Web ブラウザの [Back] ボタンをクリックすると前のページに戻りますが、変更内容は保存されないことに留意してください。[Cancel] をクリックすると、ページで行った変更はすべてキャンセルされ、ページの移動は行われません。変更は、[Apply] をクリックした場合にだけ適用されます。
- 

図 2-1 は、Web ブラウザ インターフェイスのホーム ページを示しています。

図 2-1 Web ブラウザ インターフェイスのホーム ページ

Interface	MAC Address	Transmission Rate
GigabitEthernet0	442b.039a.888f	1Gbps
Radio0-802.11n	3cce.731a.0800	Mcs Index 23
Radio1-802.11n	3cce.7318.0800	Mcs Index 23

Time	Severity	Description
Apr 2 07:42:51.003	Warning	Full power - NEGOTIATED inline power source
Apr 2 07:42:47.103	Information	Interface BV1 assigned DHCP address 172.31.255.104, mask 255.255.255.0, hostname ap
Apr 2 07:42:38.999	Notification	Line protocol on interface GigabitEthernet0, changed state to up
Apr 2 07:42:38.675	Error	Process DPAAINIT top-level routine exited
Apr 2 07:42:38.675	Critical	HW crypto FIPS self test passed
Apr 2 07:42:37.023	Notification	Line protocol on interface Dot11Radio1, changed state to down
Apr 2 07:42:37.023	Notification	Line protocol on interface Dot11Radio0, changed state to down
Apr 2 07:42:37.015	Notification	Line protocol on interface BV1, changed state to up
Apr 2 07:42:36.619	Notification	Line protocol on interface GigabitEthernet0, changed state to down

## アクション ボタンの使用方法

表 2-1 は、管理ページに表示されるページ リンクとボタンの一覧を示しています。

表 2-1 管理ページのボタンとリンク

ボタン/リンク	説明
<b>ナビゲーション リンク</b>	
Home	ワイヤレス デバイスにアソシエートされた無線デバイスの数、イーサネットおよび無線インターフェイスのステータス、最近のワイヤレスデバイスの活動リストを示す、ワイヤレス デバイスのステータス ページを表示します。
Easy Setup	システム名、IP アドレス、無線ネットワークでの役割などの基本的な設定を行う [Express Setup] ページを表示します。
Network	無線 LAN のインフラストラクチャ デバイスのリストを表示します。アクセス ポイント インターフェイス（無線とイーサネット）の設定サブメニューがあります。
Association	無線 LAN 上のすべてのデバイスのシステム名、ネットワークでの役割、および親とクライアントの関連性を示すリストを表示します。
Wireless	無線ドメイン サービスの設定とデバイスの要約を表示し、WDS の設定 ページへのリンクを示します。

表 2-1 管理ページのボタンとリンク (続き)

ボタン / リンク	説明
Security	セキュリティ設定の要約を表示し、セキュリティ設定ページへのリンクを提示します。
Services	いくつかの無線デバイス機能のステータスを表示し、Telnet/SSH、CDP、ドメイン ネーム サーバ、フィルタ、QoS、SNMP、SNTP、および VLAN の設定ページへのリンクを示します。
Management	現在のゲスト ユーザのリストを表示し、ゲスト ユーザの設定ページおよび Web 認証ページへのリンクを示します。
Software	無線デバイスで実行されているファームウェアのバージョン番号を表示し、ファームウェアをアップグレードおよび管理するための設定ページへのリンクを示します。
Event Log	無線デバイスのイベント ログを表示し、トラップに含めるイベントの選択、イベントの重大レベルの設定、通知方法の設定を行う設定ページへのリンクを示します。
<b>設定アクション ボタン</b>	
Apply	そのページに加えた変更を保存し、ページをそのまま表示します。
Refresh	ページに表示されるステータス情報または統計を更新します。
Cancel	そのページに加えた変更を廃棄し、ページをそのまま表示します。
Back	そのページに加えた変更を廃棄し、直前のページに戻ります。
Logout	AP 設定を保存せずに AP 設定 Web インターフェイスを終了します。
ping	IPv4 または IPv6 アドレスへの ping を実行します。
Save Configuration	AP の現在の設定を NVRAM に保存します。

## 入力フィールドの文字制限

Web ブラウザ インターフェイスの入力フィールドで、次の文字を使用することはできません。この制限は、Cisco IOS ソフトウェアを使用するアクセス ポイントのすべてに適用されます。

[  
]  
+  
/

タブ

末尾のスペース

# 安全なブラウザ利用のための HTTPS の有効化

HTTPS を有効にすることで、アクセス ポイントの Web ブラウザ インターフェイスとの通信を保護できます。HTTPS は、Secure Socket Layer (SSL) プロトコルを使用して HTTP ブラウザ セッションを保護します。



(注) HTTPS を有効にすると、ブラウザとアクセス ポイントの接続が解除される可能性があります。接続が解除された場合は、ブラウザのアドレス入力用ボックスの URL を「`http://ip_address`」から「`https://ip_address`」に変更し、アクセス ポイントに再びログインします。



(注) HTTPS を有効にした場合、大部分のブラウザでは、Fully Qualified Domain Name (FQDN; 完全修飾ドメイン名) を持たないデバイスを参照するたびに、承認を求めるプロンプトが表示されます。承認を求めるプロンプトが表示されないようにするには、次の手順の説明に従って、アクセス ポイントの FQDN を作成します。

FQDN を作成し、HTTPS を有効にする手順は、次のとおりです。

- ステップ 1 ブラウザでポップアップ ブロッキング ソフトウェアを使用している場合は、ポップアップ ブロッキング機能を無効にします。
- ステップ 2 [Easy Setup] > [Network Configuration] を選択します。  
[Network Configuration] ページが表示されます。
- ステップ 3 [Host Name] フィールドにアクセス ポイントの名前を入力し、[Apply] をクリックします。
- ステップ 4 [Services] > [DNS] ページを選択します。  
[Services: DNS - Domain Name Service] ページが表示されます。
- ステップ 5 [Domain Name System (DNS)] フィールドで、[Enable] オプション ボタンをクリックします。
- ステップ 6 [Domain Name] フィールドに、会社のドメイン名を入力します。
- ステップ 7 [Name Server IPv4/IPv6 Addresses] フィールドに、DNS サーバの IP アドレスを 1 つ以上入力します。
- ステップ 8 [Apply] をクリックします。  
アクセス ポイントの FQDN は、システム名とドメイン名を組み合わせたものです。たとえば、システム名が `ap3600`、ドメイン名が `company.com` の場合、FQDN は `ap3600.company.com` です。
- ステップ 9 DNS サーバの FQDN を入力します。



## ヒント

DNS サーバがない場合は、ダイナミック DNS サービスを使用してアクセス ポイントの FQDN を登録できます。インターネットでダイナミック DNS を検索し、有料の DNS サービスを見つけてください。

- ステップ 10 [Services] > [HTTP] を選択します。  
[Services: HTTP - Web Server] ページが表示されます。
- ステップ 11 [Web-based Configuration Management] フィールドで、[Enable Secure (HTTPS) Browsing] チェックボックスをオンにします。
- ステップ 12 [Domain Name] フィールドにドメイン名を入力し、[Apply] をクリックします。



(注) HTTPS を有効にすると、自動的に HTTP が無効になります。HTTPS が有効にされた状態で HTTP アクセスを維持するには、[Enable Secure (HTTPS) Browsing] チェックボックスをオンにしてから、[Enable Standard (HTTP) Browsing] チェックボックスをオンにします。標準 HTTP と HTTPS の両方を有効にできますが、いずれか一方のみを有効にすることを推奨します。

警告メッセージが表示され、以降はアクセス ポイントの参照にセキュア HTTP が使用されることが伝えられます。警告メッセージには、*https* を含む新しい URL も表示されます。アクセス ポイントを参照するには、この URL を使用する必要があります。

**ステップ 13** 警告メッセージ ボックスで [OK] をクリックします。

ブラウザのアドレス入力用ボックスのアドレスが、*http://<ip-address>* から *https://<ip-address>* に変更されます。

**ステップ 14** 別の警告メッセージが表示され、アクセス ポイントのセキュリティ証明書が、信頼できる認証局によって発行されたものではないことが伝えられます。ただし、この警告メッセージは無視できます。[Continue to this Website (not recommended)] をクリックします。



(注) 次の手順では、Microsoft Internet Explorer を使用していることを前提としています。そうでない場合は、自己署名証明書を使用した Web サイトへのアクセス方法の詳細について、ご使用のブラウザのマニュアルを参照してください。

**ステップ 15** アクセス ポイントのログイン ウィンドウが表示されます。アクセス ポイントに再びログインします。デフォルト ユーザ名とデフォルト パスワードは、いずれも Cisco (大文字/小文字を区別) です。

**ステップ 16** アクセス ポイントのセキュリティ証明書を表示するには、アドレス バーの [Certificate error] アイコンをクリックします。

**ステップ 17** [View Certificate] をクリックします。

**ステップ 18** [Certificate] ウィンドウで、[Install Certificate] をクリックします。Microsoft Windows の証明書のインポート ウィザードが表示されます。

**ステップ 19** [Next] をクリックします。次に表示される画面では、証明書を保管する場所を確認されます。システムのデフォルトの保管領域を使用することを推奨します。

**ステップ 20** [Next] をクリックし、デフォルトの保管領域を承認します。これで、正常に証明書がインポートされます。

**ステップ 21** [Finish] をクリックします。セキュリティ警告が表示されます。

**ステップ 22** [Yes] をクリックします。インストールが成功したことを示すメッセージ ボックスが表示されます。

**ステップ 23** [OK] をクリックします。

## CLI の設定例

次の例は、「安全なブラウザ利用のための HTTPS の有効化」(P.2-5) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# hostname ap3600
AP(config)# ip domain name company.com
AP(config)# ip name-server 10.91.107.18
AP(config)# ip http secure-server
AP(config)# end
```

この例では、アクセスポイントのシステム名は *ap3600*、ドメイン名は *company.com*、DNS サーバの IP アドレスは 10.91.107.18 です。

この例で使用されているコマンドの詳細については、リリース 12.4 の『Cisco IOS Commands Master List』を参照してください。次のリンクをクリックすると、コマンドのマスター リストを参照できます。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124html.htm>

## HTTPS 証明書の削除

HTTPS を有効にすると、アクセスポイントは証明書を自動的に生成します。ただし、HTTPS を有効にした後でアクセスポイントの完全修飾ドメイン名 (FQDN) を変更したり、FQDN を追加したりする必要が生じた場合、証明書の削除が必要になることがあります。手順は次のとおりです。

- 
- ステップ 1** [Services: HTTP Web Server] ページを表示します。
  - ステップ 2** [Enable Secure (HTTPS) Browsing] チェックボックスをオフにし、HTTPS を無効にします。
  - ステップ 3** [Delete Partial SSL certificate] をクリックして証明書を削除します。
  - ステップ 4** [Apply] をクリックします。アクセスポイントは、新しい FQDN を使用して新しい証明書を生成します。
- 

### HTTPS 証明書を削除する CLI コマンド

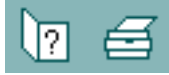
グローバル コンフィギュレーション モードでは、次のコマンドを使用して HTTPS 証明書を削除します。

	コマンド	目的
ステップ 1	no ip http secure-server	HTTPS を無効にします。
ステップ 2	crypto key zeroize rsa <i>name-of-rsa-key</i>	HTTP サーバ用の RSA キーを削除します。さらに、削除されるキーを使用して発行されたルータ証明書 (HTTPS 証明書) もすべて削除されます。

## オンライン ヘルプの使用法

オンライン ヘルプを表示するには、Web ブラウザ インターフェイスのホーム ページ上部にあるヘルプ アイコンをクリックします。図 2-2 は、ヘルプ アイコンと印刷アイコンを示しています。

図 2-2 ヘルプ アイコンと印刷アイコン



新しいブラウザ ウィンドウにヘルプ ページが表示された後、[Select a topic] ドロップダウン リストを使用して、VLAN の設定などの共通の設定作業のヘルプ索引または手順を表示します。

## ヘルプ ファイルの場所の変更

シスコでは、アクセス ポイントの最新の HTML ヘルプ ファイルをシスコの Web サイトで管理しています。デフォルトでは、アクセス ポイントの Web ブラウザ インターフェイスでヘルプ ボタンをクリックされると、アクセス ポイントは Cisco.com にあるヘルプ ファイルを開きます。しかし、ヘルプ ファイルを各自のネットワークにインストールして、アクセス ポイントでそこにアクセスすることもできます。ヘルプ ファイルをローカルにインストールする手順は、次のとおりです。

- 
- ステップ 1** ヘルプ ファイルを Cisco.com の Software Center からダウンロードします。次のリンクをクリックして、Software Center の [Wireless Software] ページを表示します。
- <http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>
- アクセス ポイント上のソフトウェア バージョンに対応するヘルプ ファイルを選択します。
- ステップ 2** アクセス ポイントがアクセスできるネットワーク上のディレクトリに、ヘルプ ファイルを解凍します。ヘルプ ファイルを解凍すると、ヘルプのバージョン番号とアクセス ポイントのモデル番号に従って名前が付けられたフォルダに、HTML ヘルプ ページが保存されます。
- ステップ 3** アクセス ポイントの Web ブラウザ インターフェイスの [Services: HTTP Web Server] ページを表示します。
- ステップ 4** [Default Help Root URL] 入力フィールドに、ヘルプ ファイルを解凍した場所への完全なパスを入力します。アクセス ポイントのヘルプ ボタンをクリックすると、アクセス ポイントでは入力したパスにヘルプのバージョン番号とモデル番号が自動的に追加されます。



(注) ヘルプのバージョン番号とデバイスのモデル番号を [Default Help Root URL] 入力フィールドに追加しないでください。アクセス ポイントによってヘルプのバージョンとモデル番号がヘルプのルート URL に自動的に追加されます。

ネットワーク ファイル サーバ上の `//myserver/myhelp` にヘルプ ファイルを解凍した場合、Default Help Root URL は次のようになります。

**http://myserver/myhelp**

表 2-2 は、1100 シリーズ アクセス ポイントのヘルプの場所と Help Root URL の例を示しています。



表 2-2 Help Root URL とヘルプの場所の例

ファイルの解凍先	Default Help Root URL	ヘルプ ファイルの実際の場所
//myserver/myhelp	http://myserver/myhelp	//myserver/myhelp/123-02.JA/1100

ステップ 5 [Apply] をクリックします。

## Web ブラウザ インターフェイスの無効化

Web ブラウザ インターフェイスの使用をすべて中止するには、[Services: HTTP-Web Server] ページで [Disable Web-Based Management] チェックボックスをオンにし、[Apply] をクリックします。

Web ブラウザ インターフェイスを再び有効にするには、アクセス ポイントの CLI で次のグローバル コンフィギュレーション コマンドを入力します。

```
ap(config)# ip http server
```





## コマンドライン インターフェイスの使用

この章では、ワイヤレス デバイスの設定に使用できる Cisco IOS コマンドライン インターフェイス (CLI) について説明します。ここで説明する内容は、次のとおりです。

- 「Cisco IOS コマンド モード」 (P.3-2)
- 「ヘルプの表示」 (P.3-3)
- 「コマンドの短縮形」 (P.3-4)
- 「コマンドの no 形式および default 形式の使用」 (P.3-4)
- 「CLI メッセージの概要」 (P.3-4)
- 「コマンド履歴の使用方法」 (P.3-5)
- 「編集機能の使用方法」 (P.3-6)
- 「show および more コマンド出力の検索およびフィルタリング」 (P.3-9)
- 「CLI のアクセス」 (P.3-9)

# Cisco IOS コマンド モード

Cisco IOS ユーザ インターフェイスには多くのモードがあります。使用できるコマンドの種類は、現在のモードによって異なります。システム プロンプトに疑問符 (?) を入力すると、各コマンド モードで使用できるコマンドの一覧が表示されます。

ワイヤレス デバイスでセッションを開始すると、ユーザ モードになります。このモードは、通常、ユーザ EXEC モードと呼ばれます。ユーザ EXEC モードでは、Cisco IOS コマンドのサブセットを利用することができます。たとえば、現在の設定ステータスを示す **show** コマンドや、カウンタまたはインターフェイスを消去する **clear** コマンドなど、ほとんどのユーザ EXEC コマンドは 1 回限りのコマンドです。ユーザ EXEC コマンドは、ワイヤレス デバイスをリブートするときには保存されません。

すべてのコマンドにアクセスする場合は、特権 EXEC モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。グローバル コンフィギュレーション モードを開始するには、特権 EXEC モードを開始していなければなりません。

コンフィギュレーション モード（グローバル、インターフェイス、およびライン）を使用して、実行コンフィギュレーションを変更できます。設定を保存した場合はこれらのコマンドが保存され、ワイヤレス デバイスをリブートするときに使用されます。各種のコンフィギュレーション モードにアクセスするには、まずグローバル コンフィギュレーション モードを開始する必要があります。グローバル コンフィギュレーション モードから、インターフェイス コンフィギュレーション モードおよびライン コンフィギュレーション モードに移行できます。

表 3-1 は主なコマンド モードと、それぞれのモードへのアクセス方法、各モードで表示されるプロンプト、およびモードの終了方法をまとめたものです。表内の例では、ホスト名に *ap* を使用しています。

表 3-1 コマンド モードの概要

モード	アクセス方法	プロンプト	終了方法	モードの用途
ユーザ EXEC	ワイヤレス デバイスでセッションを開始します。	ap>	<b>logout</b> または <b>quit</b> を入力します。	このモードは次の場合に使用します。 <ul style="list-style-type: none"> <li>ターミナルの設定変更</li> <li>基本テストの実行</li> <li>システム情報の表示</li> </ul>
特権 EXEC	ユーザ EXEC モードで、 <b>enable</b> コマンドを入力します。	ap#	<b>disable</b> を入力して終了します。	このモードは、コマンドの確認に使用します。パスワードを使用して、このモードへのアクセスを保護します。
グローバル コンフィギュレーション	特権 EXEC モードで、 <b>configure</b> コマンドを入力します。	ap(config)#	終了して特権 EXEC モードに戻るには、 <b>exit</b> または <b>end</b> コマンドを入力するか、Ctrl+Z を押します。	このモードは、ワイヤレス デバイス全体に適用するパラメータを設定する場合に使用します。

表 3-1 コマンド モードの概要 (続き)

モード	アクセス方法	プロンプト	終了方法	モードの用途
インターフェイス コンフィギュレーション	グローバル コンフィギュレーション モードで、 <b>interface</b> コマンド を入力し、イン ターフェイスを指 定します。	ap(config-if) #	終了してグローバル コンフィギュレーション モードに戻るには、 <b>exit</b> を入力します。特権 EXEC モードに戻るに は、Ctrl+Z を押すか、 <b>end</b> を入力します。	このモードは、イーサネット および無線インターフェ イスのパラメータを設定す る場合に使用します。  2.4GHz 無線および 802.11n 2.4GHz 無線は無線 0 です。  5GHz 無線および 802.11n 5GHz 無線は無線 1 です。

## ヘルプの表示

システムプロンプトで疑問符 (?) を入力すると、各コマンドモードに使用できるコマンドのリストが表示されます。また、任意のコマンドについて、関連するキーワードおよび引数の一覧を表示することもできます。表 3-2 を参照してください。

表 3-2 ヘルプの概要

コマンド	目的
<b>help</b>	コマンドモードのヘルプシステムの簡単な説明を表示します。
コマンドの先頭部分?	特定のストリングで始まるコマンドのリストを表示します。 次に例を示します。 ap# <b>di?</b> dir disable disconnect
コマンドの先頭部分<Tab>	特定のコマンド名を補完します。 次に例を示します。 ap# <b>sh conf&lt;tab&gt;</b> ap# show configuration
?	特定のコマンドモードで使用可能なすべてのコマンドをリストします。 次に例を示します。 ap> ?
コマンド?	コマンドに関連するキーワードを一覧表示します。 次に例を示します。 ap> <b>show ?</b>
コマンド キーワード?	キーワードに関連する引数を一覧表示します。 次に例を示します。 ap(config)# <b>cdp holdtime ?</b> <10-255> Length of time (in sec) that receiver must keep this packet

## コマンドの短縮形

ワイヤレス デバイスでコマンドが一意に認識される長さまでコマンドを入力します。次の例は、**show configuration** 特権 EXEC コマンドの入力方法を示しています。

```
ap# show conf
```

## コマンドの no 形式および default 形式の使用

ほとんどのコンフィギュレーション コマンドに **no** 形式があります。**no** 形式は一般に、特定の機能または動作をディセーブルにする場合、あるいはコマンドの動作を取り消す場合に使用します。たとえば、インターフェイス コンフィギュレーション コマンド **no shutdown** を使用すると、インターフェイスのシャットダウンが取り消されます。キーワード **no** を指定せずにコマンドを使用すると、ディセーブルにした機能が再びイネーブルになり、また、デフォルトでディセーブルに設定されている機能がイネーブルになります。

コンフィギュレーション コマンドには、**default** 形式もあります。コマンドの **default** 形式は、コマンドの設定値をデフォルトに戻します。ほとんどのコマンドはデフォルトで無効に設定されているため、**default** 形式を使用しても **no** 形式と同じ結果になります。ただし、デフォルトでイネーブルに設定されていて、なおかつ変数が特定のデフォルト値に設定されているコマンドもあります。これらのコマンドについては、**default** コマンドを使用すると、コマンドがイネーブルになり、変数がデフォルト値に設定されます。

## CLI メッセージの概要

表 3-3 は、CLI を使用してワイヤレス デバイスを設定しているときに表示されるエラー メッセージの一部を示しています。

表 3-3 CLI の代表的なエラー メッセージ

エラー メッセージ	意味	ヘルプの表示方法
% Ambiguous command: "show con"	ワイヤレス デバイスがコマンドとして認識できるだけの長さの文字が入力されていません。	コマンドの後ろに 1 スペース空けて疑問符 (?) を入力します。 コマンドとともに入力できる利用可能なキーワードが表示されます。
% Incomplete command.	コマンドに必須のキーワードまたは値が、一部入力されていません。	コマンドの後ろに 1 スペース空けて疑問符 (?) を入力します。 コマンドとともに入力できる利用可能なキーワードが表示されます。
% Invalid input detected at '^' marker.	コマンドの入力ミスです。間違っている箇所をキャレット (^) 記号で示しています。	疑問符 (?) を入力すると、そのコマンド モードで利用できるすべてのコマンドが表示されます。 コマンドとともに入力できる利用可能なキーワードが表示されます。

## コマンド履歴の使用法

CLI は、入力されたコマンドの履歴を保存します。この機能は、アクセス リストなど、長いまたは複雑なコマンドやエントリを呼び出す場合、特に便利です。コマンド履歴機能は、次の項で説明するように要件に合わせてカスタマイズできます。

- 「コマンド履歴バッファ サイズの変更」(P.3-5)
- 「コマンドの呼び出し」(P.3-5)
- 「コマンド履歴機能のディセーブル化」(P.3-6)

## コマンド履歴バッファ サイズの変更

デフォルトでは、ワイヤレス デバイスは履歴バッファにコマンド ライン 10 行を記録します。特権 EXEC モードで次のコマンドを入力して、現在のターミナルセッションでワイヤレス デバイスが記録するコマンド ライン数を変更します。

```
ap# terminal history [size number-of-lines]
```

指定できる範囲は 0 ~ 256 です。

特定のライン上のすべてのセッションでワイヤレス デバイスが記録するコマンド ライン数を設定するには、ライン コンフィギュレーション モードから次のコマンドを入力します。

```
ap(config-line)# history [size number-of-lines]
```

指定できる範囲は 0 ~ 256 です。

## コマンドの呼び出し

履歴バッファにあるコマンドを呼び出すには、表 3-4 にリストされているいずれかの操作を行います。

表 3-4 コマンドの呼び出し

操作 <sup>1</sup>	結果
Ctrl+P キーまたは↑キーを押します。	履歴バッファに保存されているコマンドを、最新のコマンドから順に呼び出します。キーを押すたびに、より古いコマンドが順次表示されます。
Ctrl+N キーまたは↓キーを押します。	Ctrl+P キーまたは↑キーを使用してコマンドを呼び出した後、履歴バッファ内のより新しいコマンドに戻ります。キーを押すたびに、より新しいコマンドが順次表示されます。
show history	特権 EXEC モードで、直前に入力したいくつかのコマンドを表示します。表示されるコマンドの数は、グローバル コンフィギュレーション コマンド <b>terminal history</b> および回線コンフィギュレーション コマンド <b>history</b> の設定によって決まります。

1. 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

## コマンド履歴機能のディセーブル化

コマンド履歴機能は、自動的にイネーブルになっています。

現在の端末セッションでこの機能をディセーブルにするには、**terminal no history** 特権 EXEC コマンドを使用します。

回線に関するセッションでコマンド履歴をディセーブルにするには、**no history** ライン コンフィギュレーション コマンドを使用します。

## 編集機能の使用法

ここでは、コマンドラインの操作に役立つ編集機能について説明します。この章の内容は、次のとおりです。

- 「編集機能のイネーブル化およびディセーブル化」(P.3-6)
- 「キー入力によるコマンドの編集」(P.3-7)
- 「画面幅よりも長いコマンドラインの編集」(P.3-8)

## 編集機能のイネーブル化およびディセーブル化

拡張編集モードは自動的に有効に設定されますが、ディセーブルにできます。

現在の端末セッションで拡張編集モードを再びイネーブルにするには、特権 EXEC モードで次のコマンドを入力します。

```
ap# terminal editing
```

特定の回線について拡張編集モードを再び設定するには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
ap(config-line)# editing
```

拡張編集モードをグローバルにディセーブルにするには、ライン コンフィギュレーション モードで次のコマンドを入力します。

```
ap(config-line)# no editing
```



## キー入力によるコマンドの編集

表 3-5 は、コマンド ラインの編集に必要なキー入力を示しています。

表 3-5 キー入力によるコマンドの編集

機能	キーストローク <sup>1</sup>	目的
コマンドライン上を移動して、変更または訂正を行います。	<b>Ctrl+B</b> キーまたは←キー	カーソルを 1 文字分だけ後ろに戻します。
	<b>Ctrl+F</b> キーまたは→キー	カーソルを 1 文字分だけ前に進めます。
	<b>Ctrl+A</b>	カーソルをコマンドラインの先頭に移動させます。
	<b>Ctrl+E</b>	カーソルをコマンドラインの末尾に移動させます。
	<b>Esc B</b>	カーソルを 1 ワード分だけ後ろに戻します。
	<b>Esc F</b>	カーソルを 1 ワード分だけ前に進めます。
	<b>Ctrl+T</b>	カーソルの左にある文字を、カーソル位置の文字と置き換えます。
バッファからコマンドを呼び出し、コマンドラインにペーストします。ワイヤレス デバイスは、直前に削除された 10 項目をバッファに入れます。	<b>Ctrl+Y</b>	バッファから最新のエントリを呼び出します。
	<b>Esc Y</b>	バッファから次のエントリを呼び出します。 バッファには、最後に削除またはカットした 10 項目しか保存されません。 <b>Esc+Y</b> を 11 回以上押すと、最初のバッファ エントリに戻って表示されます。
不要なエントリを削除します。	<b>Delete</b> または <b>Backspace</b>	カーソルの左にある文字を消去します。
	<b>Ctrl+D</b>	カーソル位置にある文字を削除します。
	<b>Ctrl+K</b>	カーソル位置からコマンドラインの末尾までの全文字を削除します。
	<b>Ctrl+U</b> または <b>Ctrl+X</b>	カーソル位置からコマンドラインの先頭までの全文字を削除します。
	<b>Ctrl+W</b>	カーソルの左にあるワードを消去します。
	<b>Esc D</b>	カーソル位置からワードの末尾までを削除します。
ワードを大文字または小文字にします。または、一連の文字をすべて大文字にします。	<b>Esc C</b>	カーソル位置のワードを大文字にします。
	<b>Esc L</b>	カーソル位置のワードを小文字に変更します。
	<b>Esc U</b>	カーソル位置からワードの末尾までの文字を大文字にします。
特定のキーストロークを実行可能なコマンド（通常はショートカット）として指定します。	<b>Ctrl+V</b> または <b>Esc Q</b>	

表 3-5 キー入力によるコマンドの編集 (続き)

機能	キーストローク <sup>1</sup>	目的
1 行または 1 画面下へスクロールして、端末画面に収まりきらない表示内容を表示させます。  (注) <b>show</b> コマンドの出力など、ターミナル画面で表示しきれない行のある出力には、More プロンプトが表示されます。More プロンプトが表示されている場合は、いつでも <b>Return</b> および <b>Space</b> バーを使用できます。	<b>Return</b>	1 行下へスクロールします。
	<b>Space</b>	1 画面下へスクロールします。
ワイヤレス デバイスから画面に突然メッセージが出力された場合に、現在のコマンドラインを再表示する。	<b>Ctrl+L</b> または <b>Ctrl+R</b>	現在のコマンドラインを再表示します。

1. 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

## 画面幅よりも長いコマンドラインの編集

画面上で複数行にわたるコマンドに対して折り返し機能を使用できます。カーソルが右マージンに達すると、そのコマンドラインは 10 文字分だけ左へシフトされます。コマンドラインの先頭から 10 文字までは見えなくなりますが、左へスクロールして、コマンドの先頭部分の構文をチェックできます。

コマンドの先頭にスクロールして入力内容をチェックするには、**Ctrl+B** キーまたは←キーを繰り返し押します。コマンドラインの先頭に直接移動するには、**Ctrl+A** を押します。



(注) 矢印キーが使用できるのは、VT100 などの ANSI 互換端末に限られます。

次の例では、**access-list** グローバル コンフィギュレーション コマンド エントリが 1 行分よりも長くなっています。最初にカーソルが行末に達すると、その行は 10 文字分だけ左へシフトされ、再表示されます。ドル記号 (\$) は、その行が左へスクロールされたことを表します。カーソルが行末に達するたびに、その行は再び 10 文字分だけ左へシフトされます。

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
ap(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
ap(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
ap(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

コマンドの入力が終わった後、**Ctrl+A** を押して全体の構文をチェックし、その後 **Return** キーを押してコマンドを実行してください。行末に表示されるドル記号 (\$) は、その行が右へスクロールされたことを表します。

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

ソフトウェアでは、端末画面は 80 カラム幅であると想定されています。それ以外の幅の場合は、特権 EXEC コマンド **terminal width** を使用してターミナルの幅を設定します。

ラップアラウンド機能とコマンド履歴機能を併用すると、前に入力した複雑なコマンド エントリを呼び出して変更できます。前に入力したコマンド エントリの呼び出し方法については、「[キー入力によるコマンドの編集](#)」(P.3-7) を参照してください。

# show および more コマンド出力の検索およびフィルタリング

**show** コマンドおよび **more** コマンドの出力を検索してフィルタリングできます。この機能は、大量の出力をソートしたり、表示する必要のない出力を除外したりする場合に便利です。

この機能を使用するには、**show** または **more** コマンドを入力した後、パイプ記号 (|)、**begin**、**include**、または **exclude** のいずれかのキーワード、および文字列（検索またはフィルタの条件）を指定します。

```
command | {begin | include | exclude} regular-expression
```

文字列では、大文字と小文字が区別されます。たとえば、**| exclude output** と入力した場合、*output* を含む行は表示されませんが、*Output* を含む行は表示されます。

次に、*protocol* が使用されている行だけを出力するように指定する例を示します。

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

## CLI のアクセス

ワイヤレス デバイスの CLI は、Telnet またはセキュア シェル (SSH) を使用して開くことができます。

## Telnet を使用して CLI を開く

Telnet を使用して CLI を開く手順は、次のとおりです。これらの手順は、Microsoft Windows を実行する PC で Telnet 端末アプリケーションを使用する場合を想定しています。オペレーティング システムの詳細な操作方法については、ご使用の PC の操作マニュアルを確認してください。

- 
- ステップ 1** [Start] > [Programs] > [Accessories] > [Telnet] の順に選択します。  
[Accessories] メニューに Telnet がない場合は、[Start] > [Run] の順に選択し、入力フィールドに **Telnet** と入力して Enter を押します。
  - ステップ 2** [Telnet] ウィンドウで、**open** の後にワイヤレス デバイスの IP アドレスを入力し、**Enter** キーを押します。
  - ステップ 3** ユーザ名とパスワードが要求されたら、管理者のユーザ名とパスワードを入力します。デフォルトのユーザ名は **Cisco**、デフォルトのパスワードは **Cisco** です。デフォルトのイネーブルパスワードも **Cisco** です。ユーザ名とパスワードでは、大文字と小文字が区別されます。
-

## セキュア シェルを使用して CLI を開く

セキュア シェル プロトコルは、ネットワーク デバイスとの安全なリモート接続を可能にするプロトコルです。セキュア シェル (SSH) は、セッション全体を暗号化することによって、安全なログイン セッションを実現するソフトウェア パッケージです。SSH は、強力な暗号の認証、強力な暗号化、および完全性保護を特長としています。SSH の詳細は、SSH Communications Security, Ltd. のホームページ (<http://www.ssh.com/>) を参照してください。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりもリモート接続の安全性が高くなります。このリリースでは SSH バージョン 1 および 2 がサポートされています。ワイヤレス デバイスの SSH アクセスに関する設定手順の詳細は、「[アクセス ポイントのセキュア シェルの設定](#)」(P.5-28) を参照してください。



## 第 4 章

# アクセスポイントの最初の設定

この章では、最初にワイヤレスデバイスの基本設定を行うときの手順について説明します。この章の内容は、ワイヤレスデバイスに付属するクイックスタートガイドの説明と共通する箇所があります。この章で説明する設定はすべて CLI を使用して実行できますが、ワイヤレスデバイスの Web ブラウザ インターフェイスで初期設定を完了してから、CLI を使用して詳細設定を追加入力する方が簡単な場合があります。

この章の内容は、次のとおりです。

- 「はじめる前に」 (P.4-2)
- 「アクセスポイントへのログイン」 (P.4-4)
- 「IP アドレスの取得と割り当て」 (P.4-4)
- 「1130 シリーズのアクセスポイントへのローカル接続」 (P.4-5)
- 「1130 シリーズのアクセスポイントへのローカル接続」 (P.4-5)
- 「1040、1140、1240、1250、1260、および 2600 シリーズのアクセスポイントへのローカル接続」 (P.4-6)
- 「1300 シリーズのアクセスポイント/ブリッジへのローカル接続」 (P.4-7)
- 「デフォルトの無線設定」 (P.4-8)
- 「基本設定の割り当て」 (P.4-8)
- 「CLI の設定例」 (P.4-16)
- 「アクセスポイントでのシステム電力の設定」 (P.4-23)
- 「CLI を使用した IP アドレスの割り当て」 (P.4-27)
- 「CLI を使用した IP アドレスの割り当て」 (P.4-27)
- 「Telnet セッションを使用した CLI へのアクセス」 (P.4-27)
- 「802.1X サプリカントの設定」 (P.4-28)
- 「IPv6 の設定」 (P.4-31)



(注)

このリリースでは、アクセスポイントの無線インターフェイスがデフォルトで無効に設定されています。

## はじめる前に

ワイヤレス デバイスを設置する前に、使用しているコンピュータがこのワイヤレス デバイスと同じネットワークに接続されていることを確認し、ネットワーク管理者から次の情報を取得してください。

- ワイヤレス デバイスのシステム名
- 大文字と小文字を区別する、無線ネットワークの無線 Service Set Identifier (SSID; サービスセット ID)
- DHCP サーバに接続されていない場合は、ワイヤレス デバイスの一意の IP アドレス (172.17.255.115 など)
- ワイヤレス デバイスが PC と同じサブネット上にない場合、デフォルト ゲートウェイ アドレスとサブネット マスク
- 簡易ネットワーク管理プロトコル (SNMP) コミュニティ名と SNMP ファイル属性 (SNMP を使用している場合)
- Cisco IP Setup Utility (IPSU) を使用して、ワイヤレス デバイスの IP アドレスを検索する場合、アクセス ポイントの MAC アドレス。MAC アドレスは、アクセス ポイントの底面ラベルに記載されています (00164625854c など)。

## デバイスのデフォルト設定へのリセット

初期設定時に最初からやり直す必要がある場合は、アクセス ポイントをデフォルト設定にリセットすることができます。

### MODE ボタンを使用したデフォルト設定へのリセット



(注) MODE ボタンを使用したデフォルト設定へのリセットは、自律モードのアクセス ポイントにのみ適用されます。Lightweight モードのアクセス ポイントには適用されません。

アクセス ポイントの MODE ボタンを使用して、アクセス ポイントをデフォルト設定にリセットする手順は、次のとおりです。

- ステップ 1** アクセス ポイントの電源 (外部電源用の電源ジャックまたはインライン パワー用のイーサネット ケーブル) を切ります。
- ステップ 2** MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。
- ステップ 3** MODE ボタンを押し続けて、ステータス LED がオレンジに変わったら (約 1 ~ 2 秒かかります) ボタンを放します。アクセス ポイントのすべての設定が、デフォルトに戻ります。

## GUI を使用したデフォルト設定へのリセット

アクセスポイントの GUI を使用してデフォルトの設定に戻す手順は、次のとおりです。

- 
- ステップ 1** インターネットブラウザを開きます。  
無線デバイスの Web ブラウザ インターフェイスは、Microsoft Internet Explorer バージョン 9.0 と Mozilla Firefox バージョン 17 と完全に互換性があります。
  - ステップ 2** ブラウザのアドレス入力用ボックスにワイヤレスデバイスの IP アドレスを入力して、**Enter** キーを押します。[Enter Network Password] ウィンドウが表示されます。
  - ステップ 3** [User Name] フィールドにユーザ名を入力します。デフォルトのユーザ名は **Cisco** です。
  - ステップ 4** [Password] フィールドにワイヤレスデバイスのパスワードを入力し、**Enter** を押します。デフォルトのパスワードは **Cisco** です。[Summary Status] ページが表示されます。
  - ステップ 5** [Software] をクリックして [System Software] 画面を表示します。
  - ステップ 6** [System Configuration] をクリックして、[System Configuration] 画面を表示します。
  - ステップ 7** [Reset to Defaults] ボタンをクリックすると、IP アドレスを含むすべての設定がデフォルト値にリセットされます。IP アドレスを除いたすべての設定をデフォルト値にリセットするには、[Reset to Defaults (Except IP)] ボタンをクリックします。
- 

## CLI を使用したデフォルト設定へのリセット




### 注意

デフォルトにリセットまたはソフトウェアをリロードする前に、システム ファイルを削除しないでください。

アクセスポイントをデフォルト設定および静的 IP アドレスにリセットする場合、*write erase* または *erase /all nvram* コマンドを使用します。静的 IP アドレスなどすべてを消去する場合、上記のコマンドの他に、*erase* および *erase boot static-ipaddr static-ipmask* コマンドを使用します。

特権 EXEC モードからは、CLI を使用して次の手順でアクセスポイント/ブリッジの設定をデフォルト値にリセットできます。

- 
- ステップ 1** **erase nvram** を入力して、スタートアップ コンフィギュレーションを含むすべての NVRAM ファイルを消去します。
- 

(注) **erase nvram** コマンドでは、静的 IP アドレスは消去されません。
- 
- ステップ 2** 静的 IP アドレスおよびサブネット マスクを消去するには、次の手順を実行します。それ以外の場合は、ステップ 3 に進みます。
    - a. **write default-config** と入力します。
  - ステップ 3** 「Erasing the nvram filesystem will remove all configuration files!Continue? [confirm].」という CLI メッセージが表示されたら、**Y** と入力します。
  - ステップ 4** 「Erase of nvram: complete.」という CLI メッセージが表示されたら、**reload** と入力します。このコマンドにより、オペレーティングシステムがリロードされます。
  - ステップ 5** 「Proceed with reload? [confirm].」という CLI メッセージが表示されたら、**Y** と入力します。



注意

コンフィギュレーションファイルの損傷を防ぐため、ブートプロセスは中断しないでください。CLI コンフィギュレーションの変更を続ける前に、アクセスポイント/ブリッジ Install Mode LED が緑色に点滅するまで待ちます。ロードプロセスが完了すると、「*Line protocol on Interface Dot11Radio0, changed state to up.*」という CLI メッセージが表示されます。

**ステップ 6** アクセスポイント/ブリッジがリブートしたら、静的 IP アドレスを割り当てている場合は WEB ブラウザ インターフェイスを使用して、割り当てていない場合は CLI を使用して、アクセスポイントを再設定できます。

アクセスポイントは、特権 EXEC モードから、IP アドレスも含めてデフォルト値に設定されています (DHCP を使用して IP アドレスを受信するように設定されます)。アクセスポイント/ブリッジの新しい IP アドレスを取得するには、*show interface bvi1* CLI コマンドを使用します。

## アクセスポイントへのログイン

ユーザは、次のいずれかの方法を使用してアクセスポイントにログインできます。

- グラフィカル ユーザ インターフェイス (GUI)
- Telnet (IP アドレスを使用して AP が設定されている場合)
- コンソール ポート



(注)

Cisco Aironet アクセスポイントのすべてのモデルにコンソールポートが用意されているわけではありません。アクセスポイントにコンソールポートが用意されていない場合は、GUI または Telnet を使用してアクセスしてください。

GUI を使用して AP にログインする方法については、「初めて Web ブラウザ インターフェイスを使用する場合」(P.2-2) を参照してください。

CLI を使用して AP にログインする方法については、「CLI のアクセス」(P.3-9) を参照してください。

コンソールポートを使用して AP にログインする方法については、「1040、1140、1240、1250、1260、および 2600 シリーズのアクセスポイントへのローカル接続」(P.4-6) を参照してください。

## IP アドレスの取得と割り当て

ワイヤレスデバイスの [Express Setup] ページにアクセスするには、次のいずれかの方法でワイヤレスデバイスの IP アドレスを取得するか、割り当てる必要があります。

- 1040、1130AG、1240、1250、1260 シリーズのアクセスポイント、または 1300 シリーズのアクセスポイント/ブリッジの場合は、アクセスポイントのコンソールポートに接続し、静的 IP アドレスを割り当てます。デバイスのコンソールポートに接続するには、次の項の手順を実行します。
  - 「1130 シリーズのアクセスポイントへのローカル接続」(P.4-5)
  - 「1130 シリーズのアクセスポイントへのローカル接続」(P.4-5)



- 「1040、1140、1240、1250、1260、および 2600 シリーズのアクセスポイントへのローカル接続」 (P.4-6)
- 「1300 シリーズのアクセスポイント/ブリッジへのローカル接続」 (P.4-7)



(注) ターミナルエミュレータアプリケーションによっては、フロー制御パラメータを Xon/Xoff に設定する必要があります。フロー制御値が none に設定されているためにデバイスのコンソールポートに接続できない場合は、フロー制御値を Xon/Xoff に変更してみてください。

- IP アドレスを自動的に割り当てるには、DHSP サーバを使用します (使用可能な場合)。次のいずれかの方法により、DHCP によって割り当てられた IP アドレスを検索できます。
  - まず、ワイヤレスデバイスのコンソールポートに接続し、**show ip interface brief** コマンドを使用して IP アドレスを表示します。コンソールポートに接続するには、「1130 シリーズのアクセスポイントへのローカル接続」 (P.4-5) または「1040、1140、1240、1250、1260、および 2600 シリーズのアクセスポイントへのローカル接続」 (P.4-6) の手順を実行します。
  - 組織のネットワーク管理者に、ワイヤレスデバイスのメディアアクセスコントロール (MAC) アドレスを知らせます。ネットワーク管理者は、MAC アドレスを使用して DHCP サーバに照会し、IP アドレスを確認します。アクセスポイントの MAC アドレスは、アクセスポイントの底面ラベルに記載されています。

## デフォルトの IP アドレスの動作

1040、1130AG、1140、1240、1250、1260、2600 シリーズのアクセスポイント、または 1300 シリーズのアクセスポイント/ブリッジをデフォルトの設定で LAN に接続している場合、アクセスポイントは DHCP サーバに IP アドレスを要求し、アドレスを受信できない場合、要求を無期限に送信し続けます。

1300 シリーズ アクセスポイント/ブリッジは、ルート アクセスポイントの無線ネットワークとして機能していると判断します。ブリッジとして設定するには、手動でインストールモードを指定して、アンテナの位置を合わせて無線リンクを確立します。リンクを確立するには、2 台のアクセスポイント/ブリッジをインストールモードに設定しておく必要があります。インストールモードでは、1 台のアクセスポイント/ブリッジをルートブリッジに、もう 1 台の方を非ルートブリッジとして設定してください。設定しやすいよう、アクセスポイント/ブリッジをインストールモードにすると自動オプションが使用できます。無線リンクを確立してブリッジアンテナの位置を合わせたら、アクセスポイント/ブリッジ両方のインストールモードを解除して、ルートブリッジと非ルートブリッジとして LAN に配置してください。

## 1130 シリーズのアクセスポイントへのローカル接続

アクセスポイントを (有線 LAN に接続せずに) ローカルに設定する必要がある場合、DB-9 to RJ-45 のシリアルケーブルを使用して PC をアクセスポイントのコンソールポートに接続できます。次の手順に従ってアクセスポイントのコンソールポートに接続し、CLI を開きます。

- ステップ 1** アクセスポイントのカバーを開きます。
- ステップ 2** 9 ピンのメスの DB-9 to RJ-45 シリアルケーブルを、アクセスポイントの RJ-45 シリアルポートと、コンピュータの COM ポートに接続します。DB-9 to RJ-45 シリアルケーブルのシスコ製品番号は AIR-CONCAB1200 です。シリアルケーブルは、<http://www.cisco.com/go/marketplace> で注文できます。

- ステップ 3** アクセスポイントと通信できるようにターミナルエミュレータを設定します。ターミナルエミュレータの接続では、9600 ボー、データビット 8、パリティなし、ストップビット 1 の設定を使用します。フロー制御はなしです。



(注) xon/xoff フロー制御で正常に機能しない場合は、フロー制御なしを使用してください。

- ステップ 4** 接続したら、**enter** を押すか、**en** と入力して、コマンドプロンプトを表示します。**enter** を押すと、ユーザ EXEC モードになります。**en** と入力すると、パスワードを入力するよう求められ、パスワードを入力すると特権 EXEC モードになります。デフォルトのパスワードは *Cisco* です。大文字と小文字は区別されます。

## 1040、1140、1240、1250、1260、および2600シリーズのアクセスポイントへのローカル接続

アクセスポイントを（有線 LAN に接続せずに）ローカルに設定する必要がある場合、DB-9 to RJ-45 のシリアルケーブルを使用して PC をアクセスポイントのコンソールポートに接続できます。次の手順に従ってアクセスポイントのコンソールポートに接続し、CLI を開きます。

- ステップ 1** 9 ピンのメスの DB-9 to RJ-45 シリアルケーブルを、アクセスポイントの RJ-45 シリアルポートと、コンピュータの COM ポートに接続します。DB-9 to RJ-45 シリアルケーブルのシスコ製品番号は AIR-CONCAB1200 です。シリアルケーブルは、<http://www.cisco.com/go/marketplace> で注文できます。
- ステップ 2** アクセスポイントと通信できるようにターミナルエミュレータを設定します。ターミナルエミュレータの接続では、9600 ボー、データビット 8、パリティなし、ストップビット 1 の設定を使用します。フロー制御はなしです。



(注) xon/xoff フロー制御で正常に機能しない場合は、フロー制御なしを使用してください。

- ステップ 3** 接続したら、**enter** を押すか、**en** と入力して、コマンドプロンプトを表示します。**enter** を押すと、ユーザ EXEC モードになります。**en** と入力すると、パスワードを入力するよう求められ、パスワードを入力すると特権 EXEC モードになります。デフォルトのパスワードは *Cisco* です。大文字と小文字は区別されます。



(注) 設定の変更が完了したら、アクセスポイントからシリアルケーブルを取り外してください。

# 1300 シリーズのアクセスポイント/ブリッジへのローカル接続

アクセスポイント/ブリッジをローカルに設定する（アクセスポイント/ブリッジを有線 LAN に接続しない）必要がある場合、カテゴリ 5 のイーサネット ケーブルを使用して PC を長距離用パワー インジェクタのイーサネット ポートに接続できます。シリアルポート接続を使用するのと同じように、パワー インジェクタのイーサネット ポートへのローカル接続を使用できます。



(注) 特別なクロス ケーブルを使用しなくても、PC をパワー インジェクタに接続できます。また、ストレートケーブルまたはクロス ケーブルのいずれも使用できます。

ブリッジをローカルで接続する手順は、次のとおりです。

- ステップ 1** 使用する PC が IP アドレスを自動的に取得するように設定します。または、アクセスポイント/ブリッジの IP アドレスと同じサブネット内の IP アドレスを手動で割り当てます。たとえば、アクセスポイント/ブリッジに IP アドレス 10.0.0.1 を割り当てた場合、PC に IP アドレス 10.0.0.20 を割り当てます。
- ステップ 2** パワー インジェクタから電源ケーブルを抜いた状態で、カテゴリ 5 のイーサネット ケーブルを使用して PC をパワー インジェクタに接続します。クロス ケーブルまたはストレート ケーブルのいずれかを使用できます。



(注) イーサネット ポート 0 を使用して、パワー インジェクタとアクセスポイント/ブリッジ間で通信が実行されます。イーサネット ポート 0 の設定は何も変更しないようにしてください。

- ステップ 3** 二重同軸ケーブルで、パワー インジェクタをアクセスポイント/ブリッジに接続します。
- ステップ 4** パワー インジェクタの電源ケーブルを接続して、アクセスポイント/ブリッジの電源を入れます。
- ステップ 5** 「基本設定の割り当て」(P.4-8) の手順を実行します。操作を間違えたため、最初からやり直す必要がある場合は、「デバイスのデフォルト設定へのリセット」(P.4-2) の手順の手順に従ってください。
- ステップ 6** アクセスポイント/ブリッジの設定後、PC からイーサネット ケーブルを抜いて、アクセスポイントを有線 LAN に接続します。



(注) PC をアクセスポイント/ブリッジに接続するか、PC を有線 LAN に再接続する場合は、PC の IP アドレスを解放または更新しなければならない場合があります。ほとんどの PC では、PC をリブートするか、コマンドプロンプト画面で `ipconfig /release` および `ipconfig /renew` コマンドを入力することによって、IP アドレスを解放および更新できます。手順の詳細は、ご使用の PC の操作マニュアルを参照してください。



## デフォルトの無線設定

Cisco IOS Release 12.3(8)JA から、アクセスポイントの無線は無効に設定され、デフォルトの SSID は何も割り当てられていません。これは、権限のないユーザが、デフォルトの SSID を使用してセキュリティを設定していないこのアクセスポイントからお客様の無線ネットワークにアクセスするのを防ぐための措置です。アクセスポイントの無線インターフェイスを有効にする前に、SSID を作成する必要があります。

詳細については、第 6 章「無線の設定」を参照してください。

## 基本設定の割り当て

ワイヤレスデバイスの IP アドレスを決定または割り当てた後、次の手順に従って、このワイヤレスデバイスの [Express Setup] ページにアクセスし、初期設定を行います。

- 
- ステップ 1** インターネット ブラウザを開きます。
- ステップ 2** ブラウザのアドレス入力用ボックスにワイヤレスデバイスの IP アドレスを入力して、**Enter** キーを押します。  
[Enter Network Password] 画面が表示されます。
- ステップ 3** Tab を押して、[Username] フィールドの次の [Password] フィールドに進みます。
- ステップ 4** 大文字/小文字を区別して *Cisco* というパスワードを入力し、**Enter** を押します。  
[Summary Status] ページが表示されます。
- ステップ 5** [Easy Setup] をクリックします。  
[Express Setup] 画面が表示されます。
- ステップ 6** [Network Configuration] をクリックします。
- ステップ 7** システム管理者から入手した設定を [Network Configuration] に入力します。  
設定可能な項目は、次のとおりです。
- [Host Name] : ホスト名は必須設定ではありませんが、ネットワーク上のワイヤレスデバイスを識別するのに役立ちます。ホスト名は、管理システム ページのタイトルに表示されます。
- 
-  (注) システム名には、32 文字まで入力することができます。しかし、ワイヤレスデバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。異なるワイヤレス デバイスを区別することがクライアント ユーザにとって重要な場合、最初の 15 文字に、システム名の固有の部分を含めてください。
- 
-  (注) システム名を変更すると、ワイヤレスデバイスにより無線がリセットされます。この結果、アソシエートされたクライアント デバイスのアソシエーションが解除され、ただちに再アソシエートされます。
- 
- [Server Protocol] : ネットワークの IP アドレスの割り当て方法に対応するオプション ボタンをクリックします。
    - [DHCP] : IP アドレスは、ネットワークの DHCP サーバによって自動的に割り当てられます。

- [Static IP] : ワイヤレス デバイスでは、[IP Address] フィールドに入力された静的 IP アドレスが使用されます。
- [IP Address] : ワイヤレス デバイスの IP アドレスを割り当てたり、変更したりします。DHCP がネットワークで有効な場合、このフィールドは空白のままにします。



(注) 有線 LAN 上で Web ブラウザ インターフェイスや Telnet セッションを使用してワイヤレス デバイスの設定をしている間にワイヤレス デバイスの IP アドレスが変更されると、そのワイヤレス デバイスへの接続は解除されます。接続が解除された場合は、新しい IP アドレスを使用してワイヤレス デバイスに再接続してください。もう一度、最初からやり直す必要がある場合は、「デバイスのデフォルト設定へのリセット」(P.4-2) の手順に従ってください。

- [IP Subnet Mask] : IP アドレスが LAN 上で認識されるように、ネットワーク管理者から提供された IP サブネット マスクを入力します。DHCP が有効な場合、このフィールドは空白のままにします。
- [Default Gateway] : ネットワーク管理者から提供されたデフォルト ゲートウェイ IP アドレスを入力します。DHCP が有効な場合、このフィールドは空白のままにします。
- [IPv6 ProtocolIP] : 適用するプロトコルに対応する対応するチェックボックスをオンにして、そのプロトコルを指定します。次のオプションを選択できます。
  - DHCP
  - Autoconfig
  - Static IP
- [IPv6 Address] : IPv6 アドレスを入力します。
- [Username] : ネットワークへのアクセスに必要なユーザ名を入力します。
- [Password] : ネットワークへのアクセスに必要なユーザ名に対応するパスワードを入力します。
- [SNMP Community] : ネットワークで SNMP が使用されている場合、ネットワーク管理者により用意された SNMP コミュニティ名を入力して、(同じくネットワーク管理者により用意された) SNMP データの属性を選択します。
- [Current SSID List] (読み取り専用)

**ステップ 8** アクセス ポイントでサポートされる無線帯域について、次の [Network Configuration] 設定を入力します。2.4 GHz 無線と 5 GHz の無線には共通して次のオプションがあります。

- [SSID] : [SSID] 入力フィールドに SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
  - [Broadcast SSID in Beacon] : SSID を指定していないデバイスをアクセス ポイントにアソシエートできるようにするには、このチェックボックスをオンにします。このチェックボックスがオンになっている場合、アクセス ポイントは Broadcast SSID プローブ要求に応答すると共に、ビーコンと併せて自身の SSID をブロードキャストします。SSID をブロードキャストすると、SSID を指定していないデバイスがこの無線デバイスとアソシエートできます。このオプションは、パブリック スペースでゲストやクライアント デバイスが SSID を使用する場合に便利です。SSID をブロードキャストしない場合、クライアント デバイスの SSID がこの SSID と一致しない限り、そのクライアント デバイスは無線デバイスとアソシエートできません。無線デバイス ビーコンに組み込める SSID は 1 つだけです。



- [VLAN] : 無線のVLANを有効にするには、[Enable VLAN ID] オプション ボタンをクリックし、VLAN ID を 1 ~ 4095 の範囲で入力します。この VLAN をネイティブ VLAN として指定する場合は、[Native VLAN] チェックボックスをオンにします。VLAN を無効にするには、[No VLAN] オプション ボタンをクリックします。
- [Security] : SSID のセキュリティ設定を選択します。この設定は、[No Security] から [WPA] まで堅牢性の順に並んでいます。[WPA] が最も強力なセキュリティ設定です。[EAP Authentication] または [WPA] を選択する場合は、ネットワーク上の認証サーバの IP アドレス (RADIUS サーバの IP アドレス) と共有秘密 (RADIUS サーバ シークレット) を入力します。



(注) 無線 LAN で VLAN を使用しない場合、複数の SSID に割り当てることができるセキュリティ オプションが制限されます。詳細については、「[VLAN の使用](#)」(P.4-14) を参照してください。

- [No Security] : このセキュリティ設定では、暗号キーやキー管理は使用されず、Open 認証が使用されます。
- [WEP Key] : このセキュリティ設定では、WEP 暗号化が必須となり、キー管理や Open 認証は使用されません。最大 4 つの WEP キー (つまり、キー 1、2、3、および 4) を指定できます。キーごとに値を入力し、128 ビットまたは 40 ビットのどちらであるかを指定します。
- [EAP Authentication] : 拡張認証プロトコル (EAP) 認証では、認証サーバのサービスを通じてデータベースに対して認証されたユーザに無線アクセスを許可します。その上で、認証済みユーザに許可されているトラフィックを暗号化します。LEAP、PEAP、EAP-TLS、EAP-TTLS、EAP-GTC、EAP-SIM、およびその他の 802.1x/EAP ベースのプロトコルには、この設定を使用します。この設定では、暗号化必須 WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 が使用されます。RADIUS サーバおよび RADIUS サーバ シークレットを指定します。
- [WPA] : Wi-Fi Protected Access (WPA) は、認証サーバのサービスを通じてデータベースに対して認証されたユーザへの無線アクセスを許可します。その上で、WEP で使用されるアルゴリズムよりも強力なアルゴリズムを使用して、認証済みユーザに許可されている IP トラフィックを暗号化します。このオプションを選択する前に、クライアントが WPA 認定済みであることを確認してください。この設定では、暗号スイート tkip、Open 認証 + EAP、ネットワーク EAP 認証、キー管理 WPA 必須、RADIUS サーバ認証ポート 1645 が使用されます。RADIUS サーバおよび RADIUS サーバ シークレットを指定します。



(注) ここで使用されるセキュリティ設定の詳細については、「[セキュリティ設定の概要](#)」(P.4-13) を参照してください。

- [Role in Radio Network] : ネットワークでのワイヤレス デバイスの役割を示すボタンをクリックします。ワイヤレス デバイスが有線 LAN に接続されている場合は、[Access Point (Root)] を選択します。有線 LAN に接続されていない場合は、[Repeater (Non-Root)] を選択します。
  - [Access Point] : ルート デバイス。クライアントからのアソシエーションを受け入れ、クライアントから無線 LAN までの無線トラフィックを仲介します。この設定は、どのアクセスポイントにも適用できます。
  - [Repeater] : 非ルート デバイス。クライアントからのアソシエーションを受け入れ、クライアントから、無線 LAN に接続中のルート アクセスポイントまでの無線トラフィックを仲介します。この設定は、どのアクセスポイントにも適用できます。

- [Root Bridge] : 非ルートブリッジとのリンクを確立します。このモードでは、クライアントからのアソシエーションも受け入れます。この設定は、1240 シリーズのアクセスポイントにのみ使用できます。
- [Non-Root Bridge] : このモードでは、ルートブリッジとのリンクを確立します。この設定は、1240 シリーズのアクセスポイントにのみ使用できます。
- [Install Mode] : 1300 シリーズ アクセスポイント /ブリッジを自動インストールモードに指定することで、最適な効率が得られるようにブリッジのリンクを位置合わせして調整できます。
- [Workgroup Bridge] : ワークグループブリッジモードの場合、アクセスポイントは、Cisco Aironet アクセスポイントまたはブリッジにアソシエートするクライアントデバイスとして機能します。他の無線クライアントがルートブリッジまたはアクセスポイントにアソシエートされていないと仮定すると、ワークグループブリッジは最大 254 のクライアントを持つことができます。この設定は、1040 および 1300 シリーズのアクセスポイントにのみ使用できます。
- [Universal Workgroup Bridge] : アクセスポイントを、シスコ以外のアクセスポイントとアソシエートできるワークグループブリッジとして設定します。この設定は、1130、1240 シリーズ アクセスポイント、および 1300 シリーズ アクセスポイント /ブリッジで可能です。
- [Client MAC] : ユニバーサルワークグループブリッジに接続されているクライアントのイーサネット MAC アドレス。このフィールドが表示されるのは、ユニバーサルワークグループブリッジモードの場合のみです。
- [Scanner] : ネットワーク モニタリング デバイスとして機能します。スキャナモードでは、アクセスポイントはクライアントからのアソシエーションを受け入れません。継続的にスキャンを行い、無線 LAN に接続中の他の無線デバイスから検出した無線トラフィックをレポートします。すべてのアクセスポイントは、スキャナとして設定できます。
- [Optimize Radio Network for] : ワイヤレス デバイスの無線の設定済みの設定か、ワイヤレス デバイスの無線のカスタマイズされた設定のいずれかを選択します。
  - [Throughput] : ワイヤレス デバイスで処理されるデータ量が最大限に増えます。ただし、その範囲は縮小される可能性があります。
  - [Range] : ワイヤレス デバイスの範囲が最大限に拡張されます。ただし、スループットは減少する可能性があります。
  - [Default] : アクセスポイントに使用するデフォルト値のセット。
  - [Custom] : [Network Interfaces] で入力した設定がワイヤレス デバイスに使用されます。[Custom] をクリックすると、次のネットワーク インターフェイスのページに移動します。
    - [Radio-802.11b Settings] ページ
    - [Radio-802.11b Settings] ページ
    - [Radio-802.11n Settings] ページ (1250 および 1260)
    - [Radio-802.11n Settings] ページ (1250 および 1260)
- [Aironet Extensions] : 無線 LAN 上に Cisco Aironet デバイスだけがある場合には、この設定を有効にします。
- [Channel] : 無線デバイスの無線のデフォルト チャネル設定は Least Congested です。この場合、無線デバイスは、起動時に最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後にも一貫したパフォーマンスが維持されるように、各アクセスポイントにスタティック チャネル設定を指定することを推奨します。

## ■ 基本設定の割り当て

- 2.4 GHz 無線に対応するオプションは、Least Congested を設定したチャンネル 1-2412、チャンネル 2-2417、チャンネル 3-2422、チャンネル 4-2427、チャンネル 5-2432、チャンネル 6-2437、チャンネル 7-2442、チャンネル 8-2447、チャンネル 9-2452、チャンネル 10-2457、チャンネル 11-2462 です。
- 5 GHz 無線に対応するオプションは、動的周波数選択を設定したチャンネル 36-5180、チャンネル 40-5200、チャンネル 44-5220、チャンネル 48-5240、チャンネル 149-5745、チャンネル 153-5765、チャンネル 157-5785、チャンネル 161-5805、チャンネル 165-5825 です。
- [Power] : [Power] ドロップダウン リストから電力レベルを選択します。
  - 2.4 GHz 無線に対応するオプションは、Maximum、22、19、16、13、10、7、および 4 です。
  - 5 GHz 無線に対応するオプションは、Maximum、14、11、8、5、および 2 です。

**ステップ 9** [Apply] をクリックして設定値を保存します。

**ステップ 10** [Network Interfaces] をクリックして [Network Interfaces Summary] ページを表示します。

**ステップ 11** [Radio Interface] をクリックして [Network Interfaces: Radio Status] ページを表示します。

**ステップ 12** [Settings] タブをクリックして無線インターフェイスの [Settings] ページを表示します。

**ステップ 13** [Enable] をクリックして、無線を有効に設定します。

**ステップ 14** [Apply] をクリックします。

これでワイヤレス デバイスは稼働しますが、ネットワークの運用およびセキュリティに関する要件を満たすための追加の設定が必要になる場合があります。設定の完了に必要な情報については、このマニュアルの該当する章を参照してください。



**(注)** 1040、1140、1240、1250、および 1260 シリーズのアクセス ポイントは、デフォルト設定に戻すことができます。それには、ステータス LED がオレンジになるまで、MODE ボタンを数秒間押しながら、電源ジャックを抜いて再び差し込みます。

## [Easy Setup] ページのデフォルト設定

表 4-1 は、[Express Setup] ページのデフォルト設定一覧です。

**表 4-1** [Express Setup] ページのデフォルト設定

設定	デフォルト
Host Name	ap
Configuration Server Protocol	DHCP
IP Address	デフォルトで DHCP により割り当てられます。アクセス ポイントにおけるデフォルトの IP アドレスの動作については、「デフォルトの IP アドレスの動作」(P.4-5) を参照してください。
IP Subnet Mask	デフォルトで DHCP により割り当てられます。DHCP が無効の場合、デフォルト設定は 255.255.255.224 です。
Default Gateway	デフォルトで DHCP により割り当てられます。DHCP が無効の場合、デフォルト設定は 0.0.0.0 です。



表 4-1 [Express Setup] ページのデフォルト設定 (続き)

設定	デフォルト
IPv6 Protocol	DHCP および Autoconfig
SNMP Community	defaultCommunity (Read-only)
VLAN	No VLAN
Security	No Security
Role in Radio Network (インストール済みの無線ごとに設定)	Access Point
Optimize Radio Network for	Default
Aironet Extensions	Enable
Channel	Least-Congested (2.4GHz の場合) および Dynamic Frequency Selection (5GHz の場合)
Power	Maximum

## セキュリティ設定の概要

基本的なセキュリティ設定は、[Easy Setup] > [Radio Configuration] セクションで設定できます。このセクションに提供されているオプションを使用して、固有の SSID を作成し、4 つのセキュリティ タイプのいずれかを割り当てることができます。

ワイヤレス デバイスには最大 16 の SSID を作成できます。作成した SSID は、[Current SSID List] に表示されます。デュアル無線のワイヤレス デバイスでは、デフォルトで、作成した SSID が両方の無線インターフェイスで有効になります。



**(注)** Cisco IOS Release 12.4(23c)JA および 12.xxx には、デフォルトの SSID は存在しません。クライアント デバイスからアクセスポイントにアソシエートする前に、SSID を設定しておく必要があります。

SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。

最初の文字として次の文字は使用できません。

- 感嘆符 (!)
- ポンド記号 (#)
- セミコロン (;)

次の文字は無効とされ、SSID には使用できません。

- プラス記号 (+)
- 閉じ大カッコ (])
- スラッシュ (/)
- 引用符 (")
- タブ
- 末尾のスペース

## VLAN の使用

無線 LAN で VLAN を使用し、VLAN に SSID を割り当てる場合、[Express Security] ページの 4 つのセキュリティ設定のうちいずれかを使用して複数の SSID を作成できます。ただし、無線 LAN で VLAN を使用しない場合、SSID に割り当てることのできるセキュリティオプションは制限されます。[Express Security] ページでは暗号化設定と認証タイプがリンクしているためです。VLAN を使用しない場合、暗号化設定 (WEP と暗号) が 2.4GHz 無線などのインターフェイスに適用されるため、1 つのインターフェイスで複数の暗号化設定を使用することはできません。たとえば、VLAN をディセーブルにして静的 WEP で SSID を作成すると、WPA 認証を使用する追加の SSID は作成できません。これは、異なる暗号化設定を使用しているからです。SSID のセキュリティ設定が別の SSID と競合していることがわかった場合、1 つ以上の SSID を削除して競合を解消することができます。

## SSID のセキュリティ タイプ

表 4-2 は、SSID に割り当てられる 4 つのセキュリティ タイプについて説明しています。

表 4-2 [Express Security Setup] ページのセキュリティ タイプ

セキュリティ タイプ	説明	有効になるセキュリティ機能
No Security	これは安全性が最も低いオプションです。このオプションは、パブリックスペースで使用されている SSID だけに使用し、ネットワークへのアクセスを制限している VLAN に割り当てる必要があります。	なし。
Static WEP Key	このオプションは、[No Security] よりは安全です。ただし、静的 WEP キーは攻撃に対して脆弱です。この設定を行う場合、MAC アドレスに基づいてワイヤレスデバイスへのアソシエーションを制限することを考慮してください ( <a href="#">「MAC アドレス ACL を使用したアクセスポイントへのクライアントアソシエーションの許可と禁止」(P.16-7)</a> を参照)。または、ネットワークに RADIUS サーバが存在しない場合、アクセスポイントをローカルの認証サーバとして使用することを考慮してください ( <a href="#">第 9 章「ローカル認証サーバとしてのアクセスポイントの設定」</a> を参照)。	WEP が必須。ワイヤレスデバイスキーに合う WEP キーがないと、この SSID を使用してもクライアントデバイスをアソシエートできません。

表 4-2 [Express Security Setup] ページのセキュリティタイプ (続き)

セキュリティタイプ	説明	有効になるセキュリティ機能
EAP Authentication	<p>このオプションでは、802.1X 認証 (LEAP、PEAP、EAP-TLS、EAP-FAST、EAP-TTLS、EAP-GTC、EAP-SIM、その他 802.1X/EAP ベースの製品) が有効になります。</p> <p>この設定では、暗号化必須、WEP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理なし、RADIUS サーバ認証ポート 1645 を選択します。</p> <p>ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります (サーバ認証ポート 1645)。802.1X 認証によって動的暗号キーが提供されるため、WEP キーを入力する必要はありません。</p>	<p>必須の 802.1X 認証。この SSID を使用してアソシエートするクライアント デバイスは、802.1X 認証を実行する必要があります。</p> <p>ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。</p> <p>「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」</p> <p>CLI を使用している場合は、次の警告メッセージが表示されます。</p> <p>「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」</p>
WPA	<p>Wi-Fi Protected Access (WPA) は、認証サーバのサービスを通じてデータベースに対して認証されたユーザへの無線アクセスを許可し、WEP で使用されるアルゴリズムよりも強力なアルゴリズムを使用して IP トラフィックを暗号化します。</p> <p>この設定では、暗号スイート、TKIP、Open 認証 + EAP、ネットワーク EAP 認証、キー管理 WPA 必須、RADIUS サーバ認証ポート 1645 を選択します。</p> <p>拡張認証プロトコル (EAP) 認証の場合と同じように、ネットワーク上の認証サーバの IP アドレスと共有秘密キーを入力する必要があります (サーバ認証ポート 1645)。</p>	<p>WPA 認証が必須。この SSID を使用してアソシエートするクライアント デバイスは、WPA 対応でなければなりません。</p> <p>ワイヤレス クライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。</p> <p>「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」</p> <p>CLI を使用している場合は、次の警告メッセージが表示されます。</p> <p>「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」</p>

## セキュリティ設定の制限事項

[Easy Setup] の [Radio Configuration] セクションでのセキュリティ設定は、基本セキュリティの簡易設定として設計されています。使用可能なオプションは、ワイヤレス デバイスのセキュリティ機能のサブセットです。[Express Security] ページの使用にあたっては、次の制限事項に留意してください。

- [No VLAN] オプションを選択している場合、静的 WEP キーを一度設定することができます。[Enable VLAN] を選択した場合は、静的 WEP キーを無効にする必要があります。
- SSID を編集することはできません。ただし、SSID を削除して再作成することはできます。
- 複数の認証サーバは設定できません。複数の認証サーバを設定する場合は、[Security Server Manager] ページを使用します。
- 複数の WEP キーは設定できません。複数の WEP キーを設定する場合は、[Security Encryption Manager] ページを使用します。
- ワイヤレス デバイス上にすでに設定されている VLAN に SSID を割り当てることはできません。既存の VLAN に SSID を割り当てる場合は、[Security SSID Manager] ページを使用します。
- 同一の SSID 上で認証タイプを組み合わせることはできません (MAC アドレス認証と EAP 認証など)。認証タイプを組み合わせる場合は、[Security SSID Manager] ページを使用します。

## CLI の設定例

ここでは、各セキュリティタイプを使用して SSID を作成するのと同じ働きをする CLI コマンドの例を示します。この項で取り上げる設定例は次のとおりです。

- 「例：2.4GHz 無線の [No Security]」 (P.4-16)
- 「例：2.4 GHz 無線の静的 WEP」 (P.4-17)
- 「例：[EAP Authentication]」 (P.4-19)
- 「例：2.4GHz 無線の [WPA]」 (P.4-20)

### 例：2.4GHz 無線の [No Security]

次の例は、`no_security_ssid` という名前の SSID を作成し、その SSID をビーコンに組み込んで VLAN 10 に割り当ててから、VLAN 10 をネイティブ VLAN として選択した場合の設定の一部を示しています。

```
!
dot11 ssid no_security_ssid
    vlan 10
    authentication open
    guest-mode
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
!
ssid no_security_ssid
!
antenna gain 0
station-role root
!
```

```
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

#### 例 : 2.4 GHz 無線の静的 WEP

次の例は、*static\_wep\_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して VLAN 20 に割り当て、キー スロットとして 3 を選択し、128 ビット キーを入力した場合の設定の一部を示しています。

```
!
dot11 ssid static_wep_ssid
  vlan 20
  authentication open
!
!
!
encryption vlan 20 key 3 size 128bit 7 76031220D71D63394A6BD63DE57F transmit-key
encryption vlan 20 mode wep mandatory
!
ssid static_wep_ssid
!
!
interface Dot11Radio0.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 spanning-disabled
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
!
interface Dot11Radio0.31
 encapsulation dot1Q 31 native
 no ip route-cache
 bridge-group 1
```

```
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radiol
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 E55F05382FE2064B7C377B164B73 transmit-key
encryption vlan 20 mode wep mandatory
!
ssid static_wep_ssid
!
!
interface Dot11Radiol.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radiol.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface GigabitEthernet0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 spanning-disabled
no bridge-group 20 source-learning
!
interface GigabitEthernet0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
```

**例 : [EAP Authentication]**

次の例は、*eap\_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して、SSID を VLAN 30 に割り当てた場合の設定の一部を示しています。

**(注)**

無線クライアントで EAP-FAST を使用していて、設定の中に Open 認証 + EAP を含めていないと、次の警告メッセージが表示されます。

「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

```
dot11 ssid eap_ssid
  vlan 30
  authentication open eap eap_methods
  authentication network-eap eap_methods
!
dot11 guest
!
username apuser password 7 096F471A1A0A
!
bridge irb
!
interface Dot11Radio0
  no ip address
  no ip route-cache
  shutdown
  !
  encryption vlan 30 mode wep mandatory
  !
  ssid eap_ssid
  !
  antenna gain 0
  station-role root
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.30
  encapsulation dot1Q 30
  no ip route-cache
  bridge-group 30
  bridge-group 30 subscriber-loop-control
  bridge-group 30 spanning-disabled
  bridge-group 30 block-unknown-source
  no bridge-group 30 source-learning
  no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
  no ip address
  no ip route-cache
  shutdown
  antenna gain 0
  peakdetect
  dfs band 3 block
  channel dfs
  station-role root
  bridge-group 1
  bridge-group 1 subscriber-loop-control
```

```

bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radiol.30
encapsulation dot1Q 30
no ip route-cache
bridge-group 30
bridge-group 30 subscriber-loop-control
bridge-group 30 spanning-disabled
bridge-group 30 block-unknown-source
no bridge-group 30 source-learning
no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface GigabitEthernet0.30
encapsulation dot1Q 30
no ip route-cache
bridge-group 30
bridge-group 30 spanning-disabled
no bridge-group 30 source-learning
!
interface BVI1
ip address dhcp client-id GigabitEthernet0
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
key 7 00271A150754
!
bridge 1 route ip

```

**例 : 2.4GHz 無線の [WPA]**

次の例は、*wpa\_ssid* という名前の SSID を作成し、その SSID をビーコンから除外して、SSID を VLAN 40 に割り当てた場合の設定の一部を示しています。

```

aaa new-model
!
aaa group server radius rad_eap
server name 10.10.11.100

```



```
!  
aaa group server radius rad_mac  
!  
aaa group server radius rad_acct  
!  
aaa group server radius rad_admin  
!  
aaa group server tacacs+ tac_admin  
!  
aaa group server radius rad_pmip  
!  
aaa group server radius dummy  
!  
aaa authentication login eap_methods group rad_eap  
aaa authentication login mac_methods local  
aaa authorization exec default local  
aaa accounting network acct_methods start-stop group rad_acct  
!  
aaa session-id common  
!  
dot11 ssid wpa_ssid  
    vlan 40  
        authentication open eap eap_methods  
        authentication network-eap eap_methods  
        authentication key-management wpa  
!  
interface Dot11Radio0  
    no ip address  
    no ip route-cache  
    shutdown  
    !  
    encryption vlan 40 mode ciphers tkip  
    !  
    ssid wpa_ssid  
    !  
    antenna gain 0  
    station-role root  
    bridge-group 1  
    bridge-group 1 subscriber-loop-control  
    bridge-group 1 block-unknown-source  
    no bridge-group 1 source-learning  
    no bridge-group 1 unicast-flooding  
    !  
interface Dot11Radio0.40  
    encapsulation dot1Q 40  
    no ip route-cache  
    bridge-group 40  
    bridge-group 40 subscriber-loop-control  
    bridge-group 40 spanning-disabled  
    bridge-group 40 block-unknown-source  
    no bridge-group 40 source-learning  
    no bridge-group 40 unicast-flooding  
    !  
interface Dot11Radio1  
    no ip address  
    no ip route-cache  
    shutdown  
    antenna gain 0  
    peakdetect  
    dfs band 3 block  
    channel dfs  
    station-role root  
    bridge-group 1  
    bridge-group 1 subscriber-loop-control
```

```
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radiol.40
encapsulation dot1Q 40
no ip route-cache
bridge-group 40
bridge-group 40 subscriber-loop-control
bridge-group 40 spanning-disabled
bridge-group 40 block-unknown-source
no bridge-group 40 source-learning
no bridge-group 40 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
interface GigabitEthernet0.40
encapsulation dot1Q 40
no ip route-cache
bridge-group 40
bridge-group 40 spanning-disabled
no bridge-group 40 source-learning
!
interface BVI1
ip address dhcp client-id GigabitEthernet0
no ip route-cache
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
key 7 01300F175804
!
```

## アクセスポイントでのシステム電力の設定

AP 1040、AP 802、AP 1140、AP 1550、AP 1600、AP 2600、AP 3500、AP 3600、および AP 1260 は、ユニットの接続先電源が十分に電力を供給していないことを感知すると、無線インターフェイスをディセーブルにします。使用している電源によっては、アクセスポイントの設定で電源のタイプを入力する必要がある場合があります。Web ブラウザ インターフェイスで [Software] > [System Configuration] ページを選択し、電力オプションを選択します。図 4-1 は、[System Configuration] ページの [System Power Settings] セクションを示しています。

図 4-1 [System Software: System Configuration] ページの電力オプション

System Power Settings	
Power State:	FULL POWER
Power Source:	AC_ADAPTOR
Power Settings:	<input checked="" type="radio"/> Power Negotiation <input type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	
Locate Access Point	
Blink the Access Point LEDs:	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<input type="button" value="Apply"/>	

### AC 電源アダプタの使用

AC 電源アダプタを使用してアクセスポイントに電力を供給する場合は、アクセスポイントの設定を調整する必要はありません。

### IEEE 802.3af 電力ネゴシエーションのスイッチ機能の使用

Power over Ethernet (PoE) を 1040、1130、1140、1240、1250、および 1260 アクセスポイントに供給するスイッチを使用し、そのスイッチが IEEE 802.3af 電力ネゴシエーション標準に対応している場合、[System Software: System Configuration] ページで [Power Negotiation] を選択します。

### IEEE 802.3af 電力ネゴシエーションに対応していないスイッチの使用

Power over Ethernet (PoE) を 1040、1130、または 1140 アクセスポイントに供給するスイッチを使用し、そのスイッチが IEEE 802.3af 電力ネゴシエーション標準に対応していない場合、[System Software: System Configuration] ページで [Pre-Standard Compatibility] を選択します。

### 電力インジェクタの使用

電力インジェクタを使用して 1040、1130、1140、1240、1250、または 1260 アクセスポイントに電力を供給している場合、[System Software: System Configuration] ページで [Power Injector] を選択し、アクセスポイントを接続しているスイッチポートの MAC アドレスを入力します。

## dot11 extension power native コマンド

有効になっている場合、**dot11 extension power native** によって、無線で使用中のパワー テーブルが IEEE 802.11 テーブルからネイティブ パワー テーブルへシフトされます。無線装置は、このテーブル値を CISCO-DOT11-1F-MIB の NativePowerTable および NativePowerSupportedTable から取り出します。[Native Power] テーブルは、-1dBm レベルをサポートする Cisco Aironet の無線機器で使用できるように、電源を -1dBm 近辺に低く設定するよう厳密に設計されています。

## 802.3af 標準 PoE を備える 1250 シリーズ アクセスポイントでの 802.11n パフォーマンスのサポート

2.4 GHz 帯域と 5 GHz 帯域の両方で 802.11n の最適なパフォーマンスを発揮するため、Cisco Aironet 1250 シリーズ アクセスポイントには 20 W の電力が必要です。これにより、一方の無線が 802.3af を使用して稼働するように設定できます。このように設定することで、もう一方の無線を無効にしなが、802.3af で全機能を使用できます。アクセスポイントに 20 W の電力を供給する電力ソリューションにアップグレードすると、両方の無線が 2x3 Multiple Input/Multiple Output (MIMO) テクノロジーを使用して完全に機能するように、もう一方の無線を設定できます。

## 1250 シリーズの電力モード

1250 シリーズ アクセスポイントには、インライン電源またはオプションの AC/DC アダプタ電源を使用して電力を供給できます。無線設定によっては、インライン電源で供給できる電力を超える電力が必要になる場合があります。インライン電源の電力が不足している場合は、表 4-3 に示すように、アクセスポイントの無線設定に基づいて複数のオプションを選択できます。

表 4-3 アクセスポイントの無線設定に基づくインライン電源オプション

無線帯域	データ レート	トランスミッタ数	サイクリックシフトダイバーシティ (CSD)	最大伝送パワー (dBm) <sup>1</sup>		
				802.3af モード (15.4W)	拡張 PoE 電力最適化モード (16.8 W)	拡張 PoE モード (20 W)
2.4 GHz	802.11b	1	該当なし	20	20	20
	802.11g	1	該当なし	17	17	17
	802.11n (MCS 0-7)	1	ディセーブル	17	17	17
		2	有効 (デフォルト)	ディセーブル	14 (Tx あたり 17) <sup>2</sup>	20 (トランスミッタあたり 17)
802.11n (MCS 8-15)	2	該当なし	ディセーブル	14 (トランスミッタあたり 17)	20 (トランスミッタあたり 17)	

表 4-3 アクセスポイントの無線設定に基づくインライン電源オプション (続き)

無線帯域	データ レート	トランスミッタ数	サイクリックシフトダイバーシティ (CSD)	最大伝送パワー (dBm) <sup>1</sup>		
				802.3af モード (15.4W)	拡張 PoE 電力最適化モード (16.8 W)	拡張 PoE モード (20 W)
5 GHz	802.11a	1	該当なし	17	17	17
	802.11n (MCS 0-7)	1	ディセーブル	17	17	17
		2	有効 (デフォルト)	ディセーブル	20 (トランスミッタあたり 17)	20 (トランスミッタあたり 17)
802.11n (MCS 8-15)	2	該当なし	ディセーブル	20 (トランスミッタあたり 17)	20 (トランスミッタあたり 17)	

1. 最大伝送パワーは、チャンネルおよび国別の規制により異なります。詳細については製品のドキュメンテーションを参照してください。
2. Tx-トランスミッタ

## 3600 シリーズ アクセスポイントでの 802.11ac のサポート

3600 シリーズのアクセスポイントでは、3 番目の無線スロットとして 802.11ac を使用できます。Cisco IOS Release 15.2(4)JA でサポートされる動作モードは、次のとおりです。

- Local Mode
- Flex Mode
  - Connected Mode
  - Standalone Mode

次のモードはサポートされていません。

- Mesh
- Spectrum
- Monitor mode
- Autonomous mode



(注) サポートされていないモードのいずれかで AP を設定する場合は、802.11ac 無線をディセーブルにする必要があります。



(注) 802.11ac 無線では、TKIP を使用する SSID と TKIP+AES を使用する SSID は有効にされません。したがって、5 GHz のクライアントは、いずれも 802.11n 無線に参加する必要があります。

802.11ac 無線を設定する際には、以下の点に留意してください。

- 802.11ac 無線が完全に機能するには、802.11n 無線が必要です。802.11n 無線をシャットダウンすると、802.11ac の機能に影響します。

- 802.11n 無線と 802.11ac 無線は、同じ帯域で動作します。ただし、802.11n のチャンネル帯域幅のほうを低く設定した場合に限り、それぞれのチャンネル帯域幅を個別に設定できます。サポートされるチャンネル帯域幅の組み合わせの詳細については、表 4-4 を参照してください。

表 4-4 サポートされるチャンネル帯域幅の組み合わせ

802.11n のチャンネル帯域幅	802.11ac のチャンネル帯域幅
20	20
20	40
20	80
40	40
40	80

- オフ チャンネル スキャンまたは伝送はサポートされません。802.11ac 無線でオフ チャンネル スキャン機能を利用するには、802.11n 無線が必要です。

## 802.11ac の電源管理

屋外メッシュ製品を除くすべてのアクセスポイントは、Power over Ethernet 対応です。Power over Ethernet を使用する無線を 2 台使用するアクセスポイントは、完全に機能し、すべての機能をサポートします。ただし、3600 シリーズ AP で接続された 802.11ac の場合、802.3af は、3 台すべての無線をサポートするには十分な電源ではありません。使用可能なさまざまな電源管理オプションについては、表 4-5 を参照してください。

表 4-5 電源に基づくインライン パワー オプション

電源	有効にされる無線			注
	2.4G	5G 802.11n	5G 802.11ac	
AC アダプタ	Yes	Yes	Yes	これはデフォルトの動作です。1250 の実装方法と同じように、2.4G が無効にされると 5G 11ac を有効にする方式を追加することが検討されています。
802.3af	Yes	Yes	No	
802.3at	Yes	Yes	Yes	

802.11n と 802.11ac は、802.11n に設定された電力レベルを使用します。802.11ac に個別に電力レベルを設定することはできません。

## CLI を使用した IP アドレスの割り当て

ワイヤレス デバイスを有線 LAN に接続すると、ワイヤレス デバイスは、自動的に生成される Bridge Virtual Interface (BVI; ブリッジ仮想インターフェイス) を使用してネットワークにリンクします。ネットワークは、ワイヤレス デバイスのイーサネットと無線ポートの IP アドレスを個別に記録せずに、BVI を使用します。

CLI を使用してワイヤレス デバイ스에 IP アドレスを割り当てる場合、そのアドレスを BVI に割り当てる必要があります。ワイヤレス デバイスの BVI に IP アドレスを割り当てるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface bvi1</code>	BVI 対応のインターフェイス コンフィギュレーション モードに入ります。
ステップ 3	<code>ip address address mask</code>	BVI に IP アドレスとアドレス マスクを割り当てます。 <b>(注)</b> Telnet セッションを使用してワイヤレス デバイスに接続している場合は、BVI に新しい IP アドレスを割り当てると、このワイヤレス デバイスへの接続が失われます。Telnet を使用してワイヤレス デバイスの設定を続ける必要がある場合は、新しい IP アドレスで、そのワイヤレス デバイスへの別の Telnet セッションを開始します。

## Telnet セッションを使用した CLI へのアクセス

Telnet セッションを使用して CLI にアクセスする手順は、次のとおりです。これらの手順は、Microsoft Windows を実行する PC で Telnet 端末アプリケーションを使用する場合を想定しています。オペレーティング システムの詳細な操作方法については、ご使用の PC の操作マニュアルを確認してください。

- ステップ 1** [Start] > [Programs] > [Accessories] > [Telnet] の順に選択します。  
[Accessories] メニューに Telnet がない場合は、[Start] > [Run] の順に選択し、入力フィールドに **Telnet** と入力して Enter を押します。
- ステップ 2** [Telnet] ウィンドウが表示されたら、[Connect] をクリックして、[Remote System] を選択します。
-  **(注)** Windows 2000 では、[Telnet] ウィンドウにドロップダウン リストが表示されません。Windows 2000 で Telnet セッションを起動するには、**open** と入力してから、ワイヤレス デバイスの IP アドレスを入力します。
- ステップ 3** [Host Name] フィールドにワイヤレス デバイスの IP アドレスを入力して、[Connect] をクリックします。

## 802.1X サブリカントの設定

dot1x 認証サーバ/クライアントの関係には、従来、ネットワーク デバイスと PC クライアントがそれぞれ使用されていました。これは、ネットワークへのアクセスに認証が必要なのは PC ユーザであるためです。しかし、無線ネットワークになってから、今までの認証サーバ/クライアントの関係とは違う手法が取り入れられました。まず、プラグが抜かれる可能性や、ネットワーク接続が部外者から使用される可能性がある公衆の場にアクセス ポイントを設置できるようになりました。次に、リピータ アクセス ポイントを無線ネットワークに組み込む場合、そのリピータ アクセス ポイントをクライアントと同様にルート アクセス ポイントで認証させる必要があります。



(注)

802.1X サブリカントは、1040、1130AG、1140、1240AG、1250、1260、および 1300 シリーズのアクセス ポイントで使用できます。1100 シリーズおよび 1200 シリーズのアクセス ポイントでは利用できません。

サブリカントの設定には、次の 2 段階があります。

- クレデンシャル プロファイルを作成して設定する
- このクレデンシャルをインターフェイスまたは SSID に適用する

どちらの手順を先に完了してもかまいませんが、サブリカントを使用する前に完了しておく必要があります。

## クレデンシャル プロファイルの作成

特権 EXEC モードから、次の手順に従って 802.1X クレデンシャル プロファイルを作成します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot1x credentials profile</code>	dot1x クレデンシャル プロファイルを作成し、dot1x クレデンシャルのコンフィギュレーション サブモードに入ります。
ステップ 3	<code>anonymous-id description</code>	(任意)：使用する匿名 ID を入力します。
ステップ 4	<code>description description</code>	(任意)：クレデンシャル プロファイルの名称を入力します。
ステップ 5	<code>username username</code>	認証ユーザ ID を入力します。
ステップ 6	<code>password {0   7   LINE}</code>	<p>クレデンシャルに、暗号化されていないパスワードを入力します。</p> <p><b>0</b>：続けて、暗号化されていないパスワードを入力します。</p> <p><b>7</b>：続けて、非表示のパスワードを入力します。非表示のパスワードは、すでに保存済みの設定を適用する場合に使用します。</p> <p><b>LINE</b>：暗号化されていない (クリア テキストの) パスワード。</p> <p>(注) 暗号化されていないテキストとクリア テキストは同じものです。クリア テキストのパスワードの後に <b>0</b> を入力してください。または、<b>0</b> を省略してクリア テキストのパスワードを入力してください。</p>



	コマンド	目的
ステップ 7	<code>pki-trustpoint pki-trustpoint</code>	(オプション。EAP-TLS だけに使用) : デフォルトの PKI トラストポイントを入力します。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>copy running config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

パラメータを無効にするには、`dot1x credentials` コマンドの `no` 形式を使用します。

次に、クレデンシャルプロファイルの作成例を示します。名称を `test`、ユーザ名を `Cisco`、暗号化されていないパスワードを `Cisco` とします。

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line.CTRL-Z を押して終了します。
ap1240AG(config)# dot1x credentials test
ap1240AG(config-dot1x-creden)#username Cisco
ap1240AG(config-dot1x-creden)#password Cisco
ap1240AG(config-dot1x-creden)#exit
ap1240AG(config)#
```

## インターフェイスまたは SSID にクレデンシャルを適用する方法

クレデンシャルプロファイルの適用方法は、インターフェイスに対しても SSID に対しても同じです。

### クレデンシャルプロファイルを有線ポートに適用する方法

特権 EXEC モードから、次の手順に従ってクレデンシャルをアクセスポイントの有線ポートに適用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface gigabitethernet 0</code>	アクセスポイントのギガビットイーサネットポートのインターフェイス コンフィギュレーション モードを開始します。  (注) <code>interface fa0</code> を使用してギガビットイーサネット コンフィギュレーション モードを開始することもできます。
ステップ 3	<code>dot1x credentials profile name</code>	すでに作成しておいたクレデンシャルプロファイル名を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、アクセスポイントのファストイーサネットポートまで、クレデンシャルプロファイル `test` を適用しています。

```
ap1240AG>enable
```

```

Password:xxxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line.CTRL-Z を押して終了します。
ap1240AG(config)#interface Gig0
ap1240AG(config-if)#dot1x credentials test
ap1240AG(config-if)#end
ap1240AG#

```

## アップリンクに使用する SSID にクレデンシャル プロファイルを適用する方法

無線ネットワーク内にリピータ アクセス ポイントがあり、ルート アクセス ポイントで 802.1X サブリカントを使用している場合、リピータがルート アクセス ポイントとアソシエートして認証に使用する SSID に、802.1X サブリカントのクレデンシャルを適用する必要があります。

特権 EXEC モードから、次の手順に従って、アップリンクに使用する SSID にクレデンシャルを適用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 ssid ssid</code>	802.11 SSID と入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。  (注) 先頭の文字に !、#、; は使用できません。  +、]、/、"、TAB、末尾のスペースは、SSID で無効な文字です。
ステップ 3	<code>dot1x credentials profile</code>	設定済みのクレデンシャル プロファイル名を入力します。
ステップ 4	<code>end</code>	dot1x クレデンシャルの設定サブモードを終了します。
ステップ 5	<code>copy running config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、`test` という名前のクレデンシャル プロファイルを適用しています。リピータ アクセス ポイント上の適用先 SSID を `testap1` としています。

```

repeater-ap>enable
Password:xxxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line.End with CTRL-Z.
repeater-ap(config-if)#dot11 ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)

```

## EAP 方式プロファイルの作成と適用

EAP 方式リストを設定して、サブリカントを有効にし、特定の EAP 方式を認識するオプションも用意されています。「[802.1X サブリカントの EAP 方式プロファイルの作成と適用 \(P.11-18\)](#)」を参照してください。

## IPv6 の設定

IPv6 は、膨大な数のアドレスを提供するために開発された、最新のインターネット プロトコルです。IPv4 では 32 ビットのアドレスが使用されますが、このプロトコルは 128 ビットのアドレスを使用します。

無線ネットワークでの展開では多数の IP 無線デバイスやスマートフォンを使用することから、128 ビットのアドレス形式を使用する IPv6 のアドレス空間では、 $3.4 \times 10^{38}$  個のアドレスをサポートできます。

IPv6 アドレスは、 $x:x:x:x:x:x:x$  のようにコロン (:) で区切られた一連の 16 ビットの 16 進フィールドで表されます。

IPv6 アドレス タイプには、次の 3 つのタイプがあります。

- ユニキャスト

Cisco IOS ソフトウェアでは、次の IPv6 ユニキャスト アドレス タイプがサポートされます。

- 集約可能グローバル アドレス

集約可能グローバル ユニキャスト アドレスは、インターネットの IPv6 部分でグローバルにルーティングおよび到達することができます。これらのグローバル アドレスは、アドレス形式のプレフィックス 001 で識別されます。

- リンクローカル アドレス

リンクローカル アドレスは、リンクローカル プレフィックス FE80::/10 (1111 1110 10) を使用して自動的にインターフェイスに設定されます。インターフェイス ID は、Modified EUI-64 形式になります。

- エニーキャストを使用できるのは、ルータだけです。ホストでは使用できません。エニーキャスト アドレスは、IPv6 パケットの送信元アドレスには使用しないでください。
  - マルチキャスト アドレスは、指定のネットワーク サービスにマルチキャストされるように意図されたフレームを処理するホスト グループの論理 ID です。IPv6 のマルチキャスト アドレスは、プレフィックス FF00::/8 (1111 1111) を使用します。

IPv6 設定では、次のマルチキャスト グループを使用します。

- 送信要求ノード マルチキャスト グループ FF02:0:0:0:1:FF00::/104
    - 全ノード リンクローカル マルチキャスト グループ FF02::1
    - 全ルータ リンクローカル マルチキャスト グループ FF02::2

表 4-6 に、IPv6 アドレスのタイプと形式を示します。

表 4-6 IPv6 アドレス形式

IPv6 アドレス タイプ	優先形式	圧縮形式
ユニキャスト	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

サポートされるモード

- Root
- Root bridge
- Non Root bridge
- Repeater
- WGB

サポートされないモード

- Spectrum mode
- Monitor mode

IPv6 アドレスを有効にするには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **int bv1**
- ap(config-if)# **ipv6 address**

ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカルアドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

ステートレス自動設定をイネーブルにするには、特権 EXEC モードから、次のコマンドを使用します。

```
ap(config-if)# ipv6 address autoconfig
```

他の IPv6 アドレスをインターフェイスに割り当てることなくリンクローカルアドレスを設定するには、特権 EXEC モードから、次のコマンドを使用します。

```
ap(config-if)# ipv6 address ipv6-address link-local
```

サイトローカルアドレスまたはグローバルアドレスをインターフェイスに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

```
ap(config-if)# ipv6 address ipv6-address [eui-64]
```



(注)

オプションの eui-64 キーワードは、アドレスの下位 64 ビットに Modified EUI-64 インターフェイス ID を使用する場合に使用します。

## DHCPv6 アドレスの設定

DHCPv6 は、IPv6 ネットワークで動作するために必要な IP アドレス、IP プレフィックス、およびその他のコンフィギュレーションを使用して IPv6 ホストを設定するために使用するネットワークプロトコルです。DHCPv6 クライアントは、迅速な 2 つのメッセージ交換（送信要求、応答）または通常の 4 つのメッセージ交換（送信要求、アドバタイズ、要求、応答）によって、サーバから設定パラメータを取得します。デフォルトでは、4 つのメッセージ交換が使用されます。rapid-commit オプションをクライアントとサーバの両方でイネーブルにすると、2 つのメッセージ交換が使用されます。

アクセスポイントの DHCPv6 クライアントをイネーブルにするには、特権 EXEC モードから、次のコマンドを使用します。

- ap# **conf t**
- ap(config)# **int bv1**
- ap(config)# **ipv6 address dhcp rapid-commit(optional)**

自律 AP は、ステートフルおよびステートレス DHCPv6 アドレッシングの両方をサポートします。

### ステートフルアドレッシング

ステートフルアドレッシングでは、DHCP サーバが使用されます。DHCP クライアントはステートフル DHCPv6 アドレッシングを使用して IP アドレスを取得します。

ステートフルアドレッシングを設定するには、特権 EXEC モードから、次のコマンドを使用します。

```
ap(config)# ipv6 address dhcp
```

### ステートレスアドレッシング

ステートレスアドレッシングでは、DHCP サーバを使用せずに IP アドレスを取得します。DHCP クライアントは、ルータ アドバタイズメントに基づいて、自身の IP アドレスを自動的に設定します。

ステートレスアドレッシングを設定するには、特権 EXEC モードから、次のコマンドを使用します。

```
ap(config)# ipv6 address autoconfig
```

## IPv6 ネイバー探索

IPv6 ネイバー探索プロセスでは、同じネットワーク上のネイバーのリンク層アドレスを決定するために、ICMP メッセージと送信要求ノード マルチキャスト アドレスを使用します。

IPv6 ネイバー探索を設定するには、特権 EXEC モードから、次のコマンドを使用します。

コマンド	目的
<code>ipv6 nd?</code>	ネイバー探索プロトコルを設定します。
<code>ipv6 nd ns-interval value</code>	このコマンドは、ブリッジグループ仮想インターフェイス (BVI) に対してのみ有効です。 インターフェイスに IPv6 ネイバー送信要求の再送信する間隔を設定します。
<code>ipv6 nd reachable-time value</code>	リモートの IPv6 ノードに到達可能な時間を設定します。
<code>ipv6 nd dad attempts value</code>	このコマンドは、ブリッジグループ仮想インターフェイス (BVI) に対してのみ有効です。 ユニキャスト IPv6 アドレスで、重複アドレス検出を行う際に連続して送信するネイバー送信要求メッセージの数を設定します。
<code>ipv6 nd dad time value</code>	重複アドレス検出の際の IPv6 ネイバー送信要求の送信間隔を設定します。
<code>ipv6 nd autoconfig default-router</code>	このコマンドは、ブリッジグループ仮想インターフェイス (BVI) に対してのみ有効です。 ネイバー検出によって導出されるデフォルト ルータへのデフォルト ルートを設定します。

コマンド	目的
<code>ipv6 nd autoconfig prefix</code>	このコマンドは、ブリッジグループ仮想インターフェイス (BVI) に対してのみ有効です。 次の定期ルータ アドバタイズメントの待機中に遅延を発生させないようにルータ アドバタイズメントの送信要求を行うルータ送信要求メッセージを設定します。
<code>ipv6 nd cache expire <i>expire-time-in-seconds</i></code>	IPv6 ネイバー探索キャッシュ エントリの期限が切れるまでの時間を設定します。
<code>ipv6 nd cache interface-limit size [log rate]</code>	指定したインターフェイスにネイバー探索キャッシュ制限を設定します。
<code>ipv6 nd na glean</code>	このコマンドは、ブリッジグループ仮想インターフェイス (BVI) に対してのみ有効です。 非送信要求ネイバー アドバタイズメントからエントリを収集するネイバー探索を設定します。
<code>ipv6 nd nsf {convergence <i>time-in-seconds</i>   dad [suppress]   throttle <i>resolutions</i>}</code>	IPv6 ネイバー探索ノンストップ フォワーディングを設定します。コンバージェンス時間を秒単位で設定したり (10 ~ 600 秒)、重複アドレス検出 (DAD) を抑止したり、ノンストップ フォワーディング (NSF) で使用する解決の数を設定したりすることもできます。
<code>ipv6 nd nud limit <i>limit</i></code>	ネイバー到達不能検出 (NUD) の再送信回数を設定し、未解決の再送信回数の制限を設定します。
<code>ipv6 nd resolution data limit <i>limit-in-packets</i></code>	キュー内でネイバー探索 (ND) 解決を待機するデータ パケット数の制限を設定します。
<code>ipv6 nd route-owner</code>	ネイバー探索で学習したルートを「ND」ステータスのルーティング テーブルに挿入し、ND 自動構成動作を有効にします。

## IPv6 アクセス リストの設定

IPv6 アクセス リスト (ACL) は、トラフィックをフィルタリングしてルータへのアクセスを制限するために使用します。IPv6 プレフィックスのリストを使用して、ルーティング プロトコル アップデートをフィルタリングします。

アクセス リストをグローバルに設定してインターフェイスに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

```
– ap(config)# ipv6 access-list acl-name
```

IPv6 アクセス リストの設定には、特権 EXEC モードから、表 4-7 に記載されているコマンドを使用できます。

表 4-7 IPv6 アクセス リストの設定コマンド

コマンド	目的
<code>default</code>	コマンドをデフォルト値に設定します。
<code>deny</code>	拒否するパケットを指定します。
<code>evaluate</code>	アクセス リストを評価します。

表 4-7 IPv6 アクセス リストの設定コマンド (続き)

コマンド	目的
<b>exit</b>	アクセス リスト コンフィギュレーション モードを終了します。
<b>no</b>	コマンドを無効にするか、そのデフォルトに設定します。
<b>permit</b>	転送するパケットを指定します。
<b>remark</b>	アクセス リスト エントリのコメントを設定します。
<b>sequence</b>	このエントリのシーケンス番号を設定します。

グローバルに設定された ACL をレイヤ 3 インターフェイスの発信トラフィックと着信トラフィックに割り当てるには、特権 EXEC モードから、次のコマンドを使用します。

- ap(config)# **interface interface**
- ap(config)# **ipv6 traffic-filter acl-name in/out**

## RADIUS の設定

RADIUS サーバは、次の 3 つの機能を提供するバックグラウンド プロセスです。

- ネットワークへのアクセスを許可する前に、ユーザを認証する
- 特定のネットワーク サービスに対してユーザを許可する
- 特定のネットワーク サービスの使用状況を把握する

XXX (「RADIUS の設定」セクションの相互参照) を参照してください。

## IPv6 WDS のサポート

WDS およびインフラストラクチャ アクセス ポイントは、WLAN Context Control Protocol (WLCCP) と呼ばれるマルチキャスト プロトコルで通信します。

Cisco IOS Release 15.2(4)JA は、IPv6 アドレスを使用して、WDS とアクセス ポイント間の通信をサポートします。WDS はデュアル スタックで動作します。つまり、IPv4 と IPv6 の両方の登録を受け入れます。

### IPv6 WDS AP 登録

最初のアクティブな IPv6 アドレスが WDS の登録に使用されます。表 4-8 に、IPv6 WDS AP 登録プロセスでのさまざまなシナリオを示します。

表 4-8 IPv6 WDS-AP 登録

シナリオ	WDS			AP			通信モード
	デュアル	IPv6	IPv4	デュアル	IPv6	IPv4	
1	Yes			yes			IPv6
2	Yes				yes		IPv6

表 4-8 IPv6 WDS-AP 登録 (続き)

シナリオ	WDS			AP			通信モード
	デュアル	IPv6	IPv4	デュアル	IPv6	IPv4	
3	Yes					yes	IPv4
4		yes		yes			IPv6
5		yes			yes		IPv6
6		yes				yes	失敗
7			yes	yes			IPv4
8			yes		yes		失敗
9			yes			yes	IPv4



(注) IPv4 および IPv6 のアクセスポイント間の 11r ローミングは、MDIE が異なるため、サポートされません。AP および WDS は両方とも、BV1 の最初のアクティブな IPv6 アドレスを使用して登録し、アドバタイズします。リンクローカルは登録に使用されません。

## CDPv6 サポート

CDP は、隣接するネイバーのデバイス ID、機能、MAC アドレス、IP アドレスまたはデュプレックスに関する情報を取得するために使用されるレイヤ 2 プロトコルです。各 CDP 対応デバイスは、隣接するネイバーに自身の情報を送信します。ネイティブ IPv6 の一部として、アクセスポイントはアドレス TLV の一部と併せて自身の IPv6 アドレスを cdp メッセージで送信すると共に、隣接スイッチから取得した IPv6 アドレス情報を解析します。

次のコマンドは、接続されている IPv6 ネイバーを表示します。

```
ap# show cdp neighbors detail
```

## RA フィルタリング

RA フィルタリングにより、無線クライアントから送信された RA をドロップすることで、IPv6 ネットワークのセキュリティが強化されます。RA フィルタリングは、設定に誤りがあるか、悪意のある IPv6 クライアント（正規の IPv6 ルータよりも優先される高い優先順位が設定されている場合がよくあります）が、ネットワークに接続できないようにします。いずれの場合も、IPv6 RA はある時点でドロップされ、悪意または設定の誤りがある IPv6 デバイスから、他の無線デバイスやアップストリームにある有線ネットワークが保護されます。

ただし、RA フィルタリングはアップリンクの方向ではサポートされません。





## アクセスポイントの管理

この章では、ワイヤレス デバイスの管理方法について説明します。この章の内容は、次のとおりです。

- 「MODE ボタンの無効化」 (P.5-2)
- 「アクセス ポイントへの不正アクセスの防止」 (P.5-3)
- 「特権 EXEC コマンドへのアクセスの保護」 (P.5-3)
- 「[Easy Setup] の設定」 (P.5-10)
- 「Spectrum Expert モードの設定」 (P.5-11)
- 「RADIUS によるアクセス ポイントへのアクセスの制御」 (P.5-12)
- 「TACACS+ によるアクセス ポイントへのアクセスの制御」 (P.5-17)
- 「イーサネットの速度およびデュプレックスの設定」 (P.5-21)
- 「アクセス ポイントの無線ネットワーク管理の設定」 (P.5-21)
- 「アクセス ポイントのローカル認証および許可の設定」 (P.5-22)
- 「認証キャッシュとプロファイルの設定」 (P.5-23)
- 「DHCP サービスを提供するためのアクセス ポイントの設定」 (P.5-25)
- 「アクセス ポイントのセキュア シェルの設定」 (P.5-28)
- 「クライアント ARP キャッシングの設定」 (P.5-29)
- 「システム日時の管理」 (P.5-31)
- 「HTTP アクセスの定義」 (P.5-36)
- 「HTTP アクセスの定義」 (P.5-36)
- 「バナーの作成」 (P.5-39)
- 「自律 Cisco Aironet アクセス ポイントを Lightweight モードにアップグレードする方法」 (P.5-41)
- 「日本の W52 ドメインへの移行方法」 (P.5-42)
- 「ポイントツーマルチポイントブリッジングにおける複数の VLAN とレート制限の設定」 (P.5-43)

## MODE ボタンの無効化

コンソールポートを搭載したアクセスポイントのMODEボタンは、**[no] boot mode-button** コマンドで無効にできます。このコマンドを使用するとパスワードによるリカバリを防ぎ、権限のないユーザがアクセスポイントのCLIにアクセスできないようにします。



### 注意

このコマンドは、パスワードによるリカバリを無効にします。このコマンドを入力した後、アクセスポイントの特権EXECモードのパスワードを紛失してしまうと、アクセスポイントのCLIにアクセスし直すには、シスコの Technical Assistance Center (TAC) に連絡する必要があります。

MODEボタンはデフォルトで有効に設定されています。特権EXECモードから、次の手順に従ってアクセスポイントのMODEボタンを無効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>no boot mode-button</b>	アクセスポイントのMODEボタンを無効にします。
ステップ 3	<b>end</b>	(注) この設定は保存する必要はありません。

MODEボタンのステータスをチェックするには、特権EXECモードから **show boot** または **show boot mode-button** コマンドを実行します。設定の実行時には、ステータスが表示されません。**show boot** と **show boot mode-button** コマンドを実行すると、通常次のような応答が表示されます。

```
ap#show boot
BOOT path-list: flash:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

ap#show boot mode-button
on
ap#
```



### (注)

特権EXECのパスワードがわかっている場合は、**boot mode-button** コマンドを使用して、MODEボタンを通常動作に復旧できます。

## アクセスポイントへの不正アクセスの防止

権限のないユーザがワイヤレス デバイスの設定を変更したり、設定情報を表示したりするのを防ぐことができます。通常は、ネットワーク管理者からワイヤレス デバイスへのアクセスを許可し、ローカル ネットワーク内の端末またはワークステーションから接続するユーザのアクセスは制限します。

ワイヤレス デバイスへの不正なアクセスを防ぐには、次のいずれかのセキュリティ機能を設定してください。

- ワイヤレス デバイスでローカルに保存されるユーザ名とパスワードの組み合わせ。この組み合わせによって、各ユーザはワイヤレス デバイスにアクセスする前に認証されます。また、特定の特権レベル（読み取り専用または読み取り/書き込み）をユーザ名とパスワードのそれぞれの組み合わせに指定できます。詳細については、「[ユーザ名とパスワードのペアの設定](#)」(P.5-7) を参照してください。デフォルトのユーザ名は *Cisco*、デフォルトのパスワードは *Cisco* です。ユーザ名とパスワードでは、大文字と小文字が区別されます。



(注) TAB、?、\$、+、および [ は、パスワードには無効な文字です。

- セキュリティ サーバのデータベースに集中的に保存されたユーザ名とパスワードの組み合わせ。詳細については、「[RADIUS によるアクセスポイントへのアクセスの制御](#)」(P.5-12) を参照してください。

## 特権 EXEC コマンドへのアクセスの保護

ネットワークで端末のアクセス コントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワーク デバイスへのアクセスが制限されます。特権レベルは、ユーザがネットワーク デバイスにログインした後に発行できるコマンドを定義します。



(注) この項で使用されるコマンドの構文と使用方法の詳細については、リリース 12.3 の『*Cisco IOS Security Command Reference*』を参照してください。

この項では、コンフィギュレーション ファイルと特権 EXEC コマンドへのアクセスを制御する方法について説明します。内容は次のとおりです。

- 「[デフォルトのパスワードおよび権限レベル設定](#)」(P.5-4)
- 「[スタティック イネーブルパスワードの設定または変更](#)」(P.5-4)
- 「[暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護](#)」(P.5-5)
- 「[ユーザ名とパスワードのペアの設定](#)」(P.5-7)
- 「[複数の特権レベルの設定](#)」(P.5-8)

## デフォルトのパスワードおよび権限レベル設定

表 5-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 5-1 デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
ユーザ名とパスワード	デフォルトのユーザ名は <i>Cisco</i> 、デフォルトのパスワードは <i>Cisco</i> です。
イネーブル パスワードおよび権限レベル	デフォルトのパスワードは <i>Cisco</i> です。デフォルトはレベル 15 です (特権 EXEC レベル)。パスワードはコンフィギュレーション ファイルで暗号化されます。
イネーブル シークレット パスワードおよび権限レベル	デフォルトのイネーブル パスワードは <i>Cisco</i> です。デフォルトはレベル 15 です (特権 EXEC レベル)。パスワードは、暗号化されてからコンフィギュレーション ファイルに書き込まれます。
回線パスワード	デフォルトのパスワードは <i>Cisco</i> です。パスワードはコンフィギュレーション ファイルで暗号化されます。

## スタティック イネーブルパスワードの設定または変更

イネーブル パスワードは、特権 EXEC モードへのアクセスを制御します。



(注)

グローバル コンフィギュレーション コマンド **no enable password** は、イネーブル パスワードを削除しますが、このコマンドを使用する場合は十分な注意が必要です。イネーブル パスワードを削除すると、EXEC モードからロックアウトされます。

スタティック イネーブル パスワードを設定または変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>enable password password</code>	<p>特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>デフォルトのパスワードは <i>Cisco</i> です。</p> <p><i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。パスワードに疑問符 (?) を含めることができます。その場合はパスワードを作成するとき、疑問符を入力する前に <b>Ctrl</b> キーを押した状態で <b>V</b> キーを押してください。たとえば、パスワード <code>abc?123</code> を作成する場合は、次のように入力します。</p> <ol style="list-style-type: none"> <li><b>abc</b> を入力します。</li> <li><b>Ctrl+V</b> を入力します。</li> <li><b>?123</b> を入力します。</li> </ol> <p><code>enable</code> パスワードの入力を求められたら、疑問符の前で <b>Ctrl+V</b> キーを押す必要はありません。パスワード プロンプトで <code>abc?123</code> と入力するだけで済みます。</p> <p>(注) <b>TAB</b>、<b>?</b>、<b>\$</b>、<b>+</b>、および <b>[</b> は、パスワードには無効な文字です。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p> <p>イネーブル パスワードは暗号化されず、ワイヤレス デバイスのコンフィギュレーション ファイルで読み取ることができます。</p>

次に、イネーブル パスワードを `11u2c3k4y5` に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます (従来の特権 EXEC モード アクセス)。

```
AP(config)# enable password 11u2c3k4y5
```

## 暗号化によるイネーブルおよびイネーブルシークレット パスワードの保護

セキュリティ レベルを強化するために、特にネットワークを超えるパスワードや Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバに保存されたパスワードについて、グローバル コンフィギュレーション コマンド `enable password` または `enable secret` を使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード (デフォルト設定) または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、`enable secret` コマンドを使用することを推奨します。

## ■ 特権 EXEC コマンドへのアクセスの保護

**enable secret** コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

イネーブルおよびイネーブル シークレット パスワードに暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>enable password [level level] {password   encryption-type encrypted-password}</b> または <b>enable secret [level level] {password   encryption-type encrypted-password}</b>	特権 EXEC モードへのアクセス用に、新しいパスワードを定義するか、既存のパスワードを変更します。 または シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。  <ul style="list-style-type: none"> <li>• (任意) <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です (特権 EXEC モード権限)。</li> <li>• <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。</li> <li>• (任意) <i>encryption-type</i> には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、別のアクセス ポイントの設定からコピーした暗号化パスワードを指定する必要があります。</li> </ul> <p>(注) 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。</p>
ステップ 3	<b>service password-encryption</b>	(任意) パスワードを定義するとき、または設定を保存するときに、パスワードを暗号化します。  暗号化を行うと、コンフィギュレーション ファイル内でパスワードが読み取り可能な形式になるのを防止できます。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

イネーブルおよびイネーブル シークレット パスワードの両方が定義されている場合、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルのパスワードを定義する場合は、**level** キーワードを使用します。レベルを指定してパスワードを設定したあと、特権レベルにアクセスする必要のあるユーザだけに、パスワードを通知してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**privilege level** グローバル コンフィギュレーション コマンドを使用します。詳細については、「複数の特権レベルの設定」(P.5-8) を参照してください。

パスワードの暗号化をイネーブルにすると、ユーザ名パスワード、認証キー パスワード、イネーブル コマンド パスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

パスワードとレベルを削除するには、**no enable password [level level]** または **no enable secret [level level]** グローバル コンフィギュレーション コマンドを使用します。パスワードの暗号化をディセーブルにするには、**no service password-encryption** グローバル コンフィギュレーション コマンドを使用します。

次に、権限レベル 2 に対して暗号化パスワード `$1$FaD0$Xyti5Rkls3LoyxzS8` を設定する例を示します。

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

## ユーザ名とパスワードのペアの設定

ユーザ名とパスワードの組み合わせを設定できます。これは、ワイヤレス デバイスでローカルに保存されます。ユーザ名とパスワードの組み合わせは、回線またはインターフェイスに割り当てられ、各ユーザがワイヤレス デバイスにアクセスする際の認証に使用されます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

ユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。この認証システムでは、ログイン ユーザ名とパスワードが要求されます。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>username name [privilege level]</b> <b>{password encryption-type password}</b>	各ユーザのユーザ名、権限レベル、パスワードを入力します。 <ul style="list-style-type: none"> <li><b>name</b> には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。</li> <li>(任意) <b>level</b> には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。</li> <li><b>encryption-type</b> には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。</li> <li><b>password</b> には、ワイヤレス デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<b>username</b> コマンドの最後のオプションとして指定します。</li> </ul>
ステップ 3	<b>login local</b>	ログイン時のローカルパスワードチェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。

	コマンド	目的
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定ユーザのユーザ名認証をディセーブルにするには、**no username name** グローバル コンフィギュレーション コマンドを使用します。

パスワード チェックをディセーブルにし、パスワードなしでの接続を可能にするには、**no login** ライン コンフィギュレーション コマンドを使用します。



(注) ユーザ名は少なくとも 1 つ設定する必要があります。また、**login local** をワイヤレス デバイスとの Telnet セッションを開くように設定する必要があります。ユーザ名が 1 つだけの場合にそのユーザ名を入力しないと、ワイヤレス デバイスからロックアウトされることがあります。

## 複数の特権レベルの設定

デフォルトでは、Cisco IOS ソフトウェアにはユーザ EXEC モードと特権 EXEC モードという 2 つのパスワード セキュリティのモードがあります。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザ グループ別に特定のコマンドへのアクセスを許可することができます。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

この項では設定情報を扱います。

- 「コマンドの特権レベルの設定」(P.5-9)
- 「特権レベルへのログインと終了」(P.5-10)



## コマンドの特権レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>privilege mode level level command</code>	コマンドの権限レベルを設定します。 <ul style="list-style-type: none"> <li><code>mode</code> には、グローバル コンフィギュレーション モードの場合は <b>configure</b> を、EXEC モードの場合は <b>exec</b> を、インターフェイス コンフィギュレーション モードの場合は <b>interface</b> を、ライン コンフィギュレーション モードの場合は <b>line</b> をそれぞれ入力します。</li> <li><code>level</code> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。レベル 15 は、<b>enable</b> パスワードによって許可されるアクセス レベルです。</li> <li><code>command</code> には、アクセスを制限したいコマンドを指定します。</li> </ul>
ステップ 3	<code>enable password level level password</code>	権限レベルに対応するイネーブル パスワードを指定します。 <ul style="list-style-type: none"> <li><code>level</code> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。</li> <li><code>password</code> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。</li> </ul> <p>(注) TAB、?、\$、+、および[は、パスワードには無効な文字です。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code> または <code>show privilege</code>	入力内容を確認します。 最初のコマンドは、パスワードとアクセス レベルの設定を表示します。2 番目のコマンドは、特権レベルの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip route** コマンドをレベル 15 に設定すると、個別に異なるレベルに設定しない限り、**show** コマンドと **show ip** コマンドも自動的に特権レベル 15 に設定されます。

特定のコマンドについて、デフォルトの権限に戻すには、**no privilege mode level level command** グローバル コンフィギュレーション コマンドを使用します。

**configure** コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用する場合にユーザが入力するパスワードとして *SecretPswd14* を定義する例を示します。

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

## 特権レベルへのログインと終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>enable level</code>	指定した権限レベルにログインします。 <i>level</i> に指定できる範囲は 0 ~ 15 です。
ステップ 2	<code>disable level</code>	指定した権限レベルを終了します。 <i>level</i> に指定できる範囲は 0 ~ 15 です。

## [Easy Setup] の設定

[Easy Setup] を使用すると、一つの画面でネットワークと無線を設定できます。

### ネットワーク設定

ネットワーク設定を使用してアクセス ポイントを設定するには、次のフィールドに値を入力します。

- Hostname
- IP Address
- Server protocol
- IP Subnet
- Default Gateway
- Admin Login
- Admin Password
- SNMP Community

### 無線設定

無線設定を使用してアクセス ポイントを設定するには、次のフィールドを設定します。

- [SSID] : 32 バイト文字列。
- [Security]。
- 無線ネットワークでの役割
  - [Access point] : ルート デバイス。この設定は、どのアクセス ポイントにも適用できます。
  - [Repeater] : 非ルート デバイス。この設定も、どのアクセス ポイントにも適用できます。
  - [Root Bridge] : この設定は、どのアクセス ポイントにも適用できます。
  - [Non-Root Bridge] : この設定は、どのアクセス ポイントにも適用できます。
  - [Workgroup Bridge] : この設定は、どのアクセス ポイントにも適用できます。
  - [Scanner] : アクセス ポイントはネットワーク モニタリング デバイスとして機能します。継続的にスキャンを行い、このモードで無線 LAN に接続中の他の無線デバイスから検出した無線トラフィックをレポートします。すべてのアクセス ポイントは、スキャナとして設定できます。

- [Optimize Radio] : 無線デバイスの無線に対する事前設定を選択するか、設定をカスタマイズできます。
- [Aironet Extensions] : 無線 LAN 上に Cisco Aironet 無線デバイスがある場合にのみ、この設定を有効にできます。
- 画面上の [Current SSID list] に、アクセスポイントに設定された SSID リストが表示されます。これは読み取り専用リストです。

工場出荷時設定にアクセスポイントのリセットするには、[Factory Reset] をクリックします。アクセスポイントのイメージをリロードするには、[Reboot AP] をクリックします。

## Spectrum Expert モードの設定

Spectrum Expert モードは、AP3500、AP3600、AP2600、AP1550 シリーズなどのすべての CleanAir 対応のアクセスポイントでサポートされます。専用スペクトルセンサーとして設定すると、Spectrum Expert Connect 自律アクセスポイントは Cisco Spectrum Expert に接続できます。Spectrum Expert モードは、独立したモードであり、モニタモードのサブセットではありません。

Spectrum Expert モードを有効にするには、次の手順を実行します。

- 
- ステップ 1 [Home] > [Easy Setup] > [Network Configuration] を選択します。
  - ステップ 2 [Role in Radio Network] ドロップダウンリストから [Spectrum] を選択します。
  - ステップ 3 [Apply] をクリックします。
  - ステップ 4 [Spectrum Expert] アイコンをクリックして Spectrum Expert を起動します。
- 

または、次の手順を実行して、Spectrum Expert モードを有効にすることもできます。

- 
- ステップ 1 [Network] > [Network Interface] を選択します。
  - ステップ 2 [Radio0-802.11n 2G.Hz] または [Radio0-802.11n 5G.Hz] をクリックします。
  - ステップ 3 [Settings] をクリックします。
  - ステップ 4 [Spectrum] オプション ボタンをクリックします。
  - ステップ 5 [Apply] をクリックします。
  - ステップ 6 [Spectrum Expert] アイコンをクリックして Spectrum Expert を起動します。
- 

Spectrum Expert モードは、AP3500、AP3600、AP2600、AP1550 シリーズなどのすべての CleanAir 対応のアクセスポイントでサポートされます。

### Spectrum Expert の接続の設定

アクセスポイントを Spectrum Expert として設定するには、次のコマンドを使用します。

- AP(config)#**interface dot11Radio 0**
- AP(config-if)#**station-role spectrum**
- AP# **show spectrum status**

Spectrum Expert は、Internet Explorer でのみサポートされます。Spectrum Expert を起動にする前に、次の設定を変更します。

**ステップ 1** [Tools] > [Internet options] > [Security] > [custom level] > [ActiveX Controls & plug-ins] > [Initialize and script ActiveX controls not marked as safe for scripting] を選択します。

**ステップ 2** [Enable] オプション ボタンをクリックします。  
次のポップアップ メッセージは無視できます。

Your current security settings put computer at risk.

## RADIUS によるアクセスポイントへのアクセスの制御

この項では、Remote Authentication Dial-In User Service (RADIUS) を使用して、ワイヤレスデバイスの管理者アクセス権を制御する手順について説明します。RADIUS をサポートするようにワイヤレス デバイスを設定する手順の詳細は、[第 13 章「RADIUS サーバと TACACS+ サーバの設定」](#)を参照してください。

RADIUS は詳細なアカウント情報を提供し、認証と許可のプロセスを柔軟に管理します。RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。



**(注)** この項で使用されるコマンドの構文と使用方法の詳細については、リリース 12.3 の『*Cisco IOS Security Command Reference*』を参照してください。

次の各項で RADIUS の設定について説明します。

- 「[RADIUS のデフォルト設定](#)」(P.5-12)
- 「[RADIUS ログイン認証の設定](#)」(P.5-12) (必須)
- 「[AAA サーバグループの定義](#)」(P.5-14) (任意)
- 「[ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定](#)」(P.5-16) (任意)
- 「[RADIUS の設定の表示](#)」(P.5-17)

## RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI 経由でワイヤレス デバイスにアクセスするユーザを認証できます。

## RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを

特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login {default   list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li>• <b>login authentication</b> コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。</li> <li>• <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。</li> <li>• <i>method1...</i> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li>• <b>local</b> : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。<b>username password</b> グローバル コンフィギュレーション コマンドを使用します。</li> <li>• <b>radius</b> : RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細については、「<a href="#">RADIUS サーバホストの識別</a>」(P.13-4)を参照してください。</li> </ul>
ステップ 4	<code>line [console   tty   vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。

	コマンド	目的
ステップ 5	<code>login authentication {default   list-name}</code>	回線または回線セットに対して、認証リストを適用します。 <ul style="list-style-type: none"> <li>• <b>default</b> を指定する場合は、<b>aaa authentication login</b> コマンドで作成したデフォルトのリストを使用します。</li> <li>• <b>list-name</b> には、<b>aaa authentication login</b> コマンドで作成したリストを指定します。</li> </ul>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login {default | list-name} method1 [method2...]** グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication {default | list-name}** ライン コンフィギュレーション コマンドを使用します。

## AAA サーバグループの定義

認証時に AAA サーバグループを使用して既存のサーバホストをグループ化するようにワイヤレス デバイスを設定できます。設定済みのサーバホストのサブセットを選択して、それを特定のサービスに使用します。サーバグループは、選択されたサーバホストの IP アドレスのリストを含むグローバルなサーバホスト リストとともに使用されます。

サーバグループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID (IP アドレスと UDP ポート番号の組み合わせ) を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同一の RADIUS サーバにアカウントリングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリのフェールオーバー時のバックアップとして機能します。

定義したグループサーバに特定のサーバを対応付けるには、**server** グループサーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバグループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
<b>ステップ 3</b> <code>radius-server host {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> <li>• (任意) <code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>timeout seconds</code> には、ワイヤレス デバイスが RADIUS サーバの返答を待ち、再送信するまでの時間を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドによる設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。</li> <li>• (任意) <code>retransmit retries</code> には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信回数を指定しない場合、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。</li> <li>• (任意) <code>key string</code> には、ワイヤレス デバイスと RADIUS サーバで動作する RADIUS デーモン間で使用される認証と暗号キーを指定します。</li> </ul> <p>(注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に <code>radius-server host</code> コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。</p> <p>ワイヤレス デバイスが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な回数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。ワイヤレス デバイス ソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。</p>
<b>ステップ 4</b> <code>aaa group server radius group-name</code>	<p>AAA サーバ グループを、特定のグループ名で定義します。</p> <p>このコマンドを実行すると、ワイヤレス デバイスはサーバ グループ コンフィギュレーション モードへ移行します。</p>
<b>ステップ 5</b> <code>server ip-address</code>	<p>特定の RADIUS サーバを定義済みのサーバグループに対応付けます。AAA サーバグループの RADIUS サーバごとに、このステップを繰り返します。</p> <p>グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。</p>
<b>ステップ 6</b> <code>end</code>	<p>特権 EXEC モードに戻ります。</p>

	コマンド	目的
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「 <a href="#">RADIUS ログイン認証の設定</a> 」(P.5-12) を参照してください。

特定の RADIUS サーバを削除するには、`no radius-server host {hostname | ip-address}` グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、`no aaa group server radius group-name` グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、`no server ip-address` サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、ワイヤレス デバイスは異なる 2 つの RADIUS グループ サーバ (*group1* と *group2*) を認識するように設定されます。group1 では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

## ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルの場合、ワイヤレス デバイスはローカル ユーザ データベースまたはセキュリティ サーバ上にあるユーザ プロファイルから取得した情報を使用して、ユーザ セッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

グローバル コンフィギュレーション コマンド `aaa authorization` と `radius` キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

`aaa authorization exec radius local` コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。



特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network radius</code>	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにワイヤレス デバイスを設定します。
ステップ 3	<code>aaa authorization exec radius</code>	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、ワイヤレス デバイスを設定します。  <code>exec</code> キーワードを指定すると、ユーザ プロファイル情報 ( <code>autocommand</code> 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

## RADIUS の設定の表示

RADIUS の設定を表示するには、`show running-config` 特権 EXEC コマンドを使用します。

## TACACS+ によるアクセスポイントへのアクセスの制御

この項では、Terminal Access Controller Access Control System Plus (TACACS+) を使用してワイヤレス デバイスの管理者アクセス権を制御する手順について説明します。TACACS+ をサポートするようにワイヤレス デバイスを設定する手順の詳細は、第 9 章「ローカル認証サーバとしてのアクセスポイントの設定」を参照してください。

TACACS+ は詳細なアカウント情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は、AAA を介して実装され、AAA コマンドを使用するのみインーブルにできません。



(注) この項で使用されるコマンドの構文と使用方法の詳細については、リリース 12.3 の『Cisco IOS Security Command Reference』を参照してください。

次の項で TACACS+ の設定について説明します。

- 「TACACS+ のデフォルト設定」(P.5-18)
- 「TACACS+ ログイン認証の設定」(P.5-18)
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」(P.5-20)
- 「TACACS+ 設定の表示」(P.5-20)

## TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティ上の危険を回避するため、ネットワーク管理アプリケーションから TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI 経由でワイヤレスデバイスにアクセスする管理者を認証できます。

## TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、まずリストの最初の方式を使用してユーザを認証します。その方式が失敗すれば、方式リストの次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	<code>aaa authentication login {default   list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li>• <b>login authentication</b> コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。</li> <li>• <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。</li> <li>• <i>method1...</i> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li>• <b>local</b> : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。 <b>username password</b> グローバル コンフィギュレーション コマンドを使用します。</li> <li>• <b>tacacs+</b> : TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。</li> </ul>
ステップ 4	<code>line [console   tty   vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5	<code>login authentication {default   list-name}</code>	<p>回線または回線セットに対して、認証リストを適用します。</p> <ul style="list-style-type: none"> <li>• <b>default</b> を指定する場合は、<b>aaa authentication login</b> コマンドで作成したデフォルトのリストを使用します。</li> <li>• <i>list-name</i> には、<b>aaa authentication login</b> コマンドで作成したリストを指定します。</li> </ul>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、**no aaa new-model** グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、**no aaa authentication login {default | list-name} method1 [method2...]** グローバル コンフィギュレーション コマンドを使用します。ログインに関する TACACS+ 認証をディセーブルにする、あるいはデフォルト値に戻すには、**no login authentication {default | list-name}** ライン コンフィギュレーション コマンドを使用します。

## 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルの場合、ワイヤレス デバイスはローカル ユーザ データベースまたはセキュリティ サーバ上にある ユーザ プロファイルから取得した情報を使用して、ユーザ セッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

グローバル コンフィギュレーション コマンド `aaa authorization` と `tacacs+` キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

`aaa authorization exec tacacs+ local` コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network tacacs+</code>	ネットワーク関連のすべてのサービス要求に対して、ユーザが TACACS+ 許可を受けるようにワイヤレス デバイスを設定します。
ステップ 3	<code>aaa authorization exec tacacs+</code>	ユーザの TACACS+ 許可でユーザの特権 EXEC アクセス権の有無を判断するように、ワイヤレス デバイスを設定します。 <code>exec</code> キーワードを指定すると、ユーザ プロファイル情報 ( <code>autocommand</code> 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

## TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、`show tacacs` 特権 EXEC コマンドを使用します。

## イーサネットの速度およびデュプレックスの設定

ワイヤレス デバイスのイーサネット ポートに速度およびデュプレックスの設定を割り当てる  
ことができます。ワイヤレス デバイスのイーサネット ポート上の速度設定とデュプレックス  
設定のどちらについても、デフォルト設定の **auto** を使用することを推奨します。ワイヤレス  
デバイスがスイッチからインライン電源を受け取ったときに、速度設定またはデュプレックス  
設定が変更されるとイーサネット リンクがリセットされ、ワイヤレス デバイスがリブートし  
ます。ワイヤレス デバイスの接続先のスイッチのポートが **auto** に設定されていない場合、ワ  
イヤレス デバイスのポートを **half** または **full** に変更してデュプレックスの不一致を修正するこ  
とができます。これによってイーサネット リンクはリセットされなくなります。ただし、**half**  
または **full** から **auto** に戻すと、リンクがリセットされ、ワイヤレス デバイスがスイッチから  
インライン電源を受け取ると、そのワイヤレス デバイスはリブートします。



(注) ワイヤレス デバイスのイーサネット ポート上の速度およびデュプレックスの設定は、  
ワイヤレス デバイスの接続先のポート上のイーサネット設定と一致させる必要があります。  
ワイヤレス デバイスの接続先のポート上の設定を変更する場合は、これと一致  
するようにワイヤレス デバイスのイーサネット ポート上の設定も変更します。

イーサネットの速度とデュプレックスは、デフォルトでは **auto** に設定されています。特権  
EXEC モードから、次の手順に従ってイーサネットの速度とデュプレックスを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface fastethernet0</code>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>speed { 10   100   auto }</code>	イーサネット速度を設定します。デフォルト設定の <b>auto</b> を使用 することをお勧めします。
ステップ 4	<code>duplex { auto   full   half }</code>	デュプレックス設定を行います。デフォルト設定の <b>auto</b> を使用 することをお勧めします。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## アクセスポイントの無線ネットワーク管理の設定

ワイヤレス デバイスを無線ネットワーク管理に対して有効にできます。無線ネットワーク マ  
ネージャ (WNM) は無線 LAN 上のデバイスを管理します。

ワイヤレス デバイスが WNM と対話するように設定するには、次のコマンドを入力します。

```
AP(config)# wlccp wnm ip address ip-address
```

WDS アクセスポイントと WNM の間の認証ステータスをチェックするには、次のコマンドを  
入力します。

```
AP# show wlccp wnm status
```

*not authenticated*、*authentication in progress*、*authentication fail*、*authenticated*、*security keys  
setup* のいずれかのステータスをとります。

# アクセスポイントのローカル認証および許可の設定

サーバを介さずに AAA を操作できるように設定するには、ローカル モードで AAA を実装するようにワイヤレス デバイスを設定します。ワイヤレス デバイスは、認証と許可を処理します。この設定ではアカウント機能は使用できません。



(注) ワイヤレス デバイスを 802.1x 対応のクライアント デバイス用のローカル認証サーバとして設定し、メイン サーバのバックアップを提供したり、RADIUS サーバのないネットワーク上で認証サービスを提供したりできます。ワイヤレス デバイスをローカル認証サーバとして設定する方法の詳細は、第9章「ローカル認証サーバとしてのアクセスポイントの設定」を参照してください。

特権 EXEC モードから、次の手順に従ってローカル AAA にワイヤレス デバイスを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login default local</code>	ローカルのユーザ名データベースを使用するようにログイン認証を設定します。 <b>default</b> キーワードにより、ローカル ユーザ データベース認証がすべてのインターフェイスに適用されます。
ステップ 4	<code>aaa authorization exec local</code>	ローカル データベースをチェックして、ユーザが EXEC シェルの実行を許可されているかどうかを判断するようにユーザ AAA 許可を設定します。
ステップ 5	<code>aaa authorization network local</code>	ネットワーク関連のすべてのサービス要求に対するユーザ AAA 認証を設定します。
ステップ 6	<code>username name [privilege level] {password encryption-type password}</code>	ローカル データベースを使用し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 <ul style="list-style-type: none"> <li><b>name</b> には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。</li> <li>(任意) <b>level</b> には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。</li> <li><b>encryption-type</b> には、後ろに暗号化されていないパスワードが続くことを指定する場合は <b>0</b> を入力します。非表示のパスワードが続くことを指定するには <b>7</b> を入力します。</li> <li><b>password</b> には、ワイヤレス デバイスへアクセスするためにユーザが入力しなければならないパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<b>username</b> コマンドの最後のオプションとして指定します。</li> </ul> (注) TAB、?、\$、+、および [ は、パスワードには無効な文字です。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	<code>show running-config</code>	入力内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

## 認証キャッシュとプロファイルの設定

認証キャッシュとプロファイル機能を使用すると、アクセス ポイントがユーザのために認証/許可応答をキャッシュできるようになります。このため、次の認証/許可要求を AAA サーバに送信しなくて済むようになります。



(注) この機能は、アクセス ポイントの Admin 認証だけにサポートされています。

この機能をサポートする次のコマンドが、Cisco IOS Release 12.3(7) に用意されています。

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```



(注) これらのコマンドについては、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.3(7)JA』を参照してください。

次の例は、Admin 認証用に設定したアクセス ポイントの設定例です。認証キャッシュを有効に設定した状態の TACACS+ を使用しています。この例では TACACS サーバを使用していますが、アクセス ポイントは RADIUS を使用して Admin 認証用に設定できます。

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
```

```
!  
aaa group server radius rad_acct  
server 192.168.134.229 auth-port 1645 acct-port 1646  
!  
aaa group server radius rad_admin  
server 192.168.134.229 auth-port 1645 acct-port 1646  
cache expiry 1  
cache authorization profile admin_cache  
cache authentication profile admin_cache  
!  
aaa group server tacacs+ tac_admin  
server 192.168.133.231  
cache expiry 1  
cache authorization profile admin_cache  
cache authentication profile admin_cache  
!  
aaa group server radius rad_pmip  
!  
aaa group server radius dummy  
!  
aaa authentication login default local cache tac_admin group tac_admin  
aaa authentication login eap_methods group rad_eap  
aaa authentication login mac_methods local  
aaa authorization exec default local cache tac_admin group tac_admin  
aaa accounting network acct_methods start-stop group rad_acct  
aaa cache profile admin_cache  
all  
!  
aaa session-id common  
!  
!  
!  
bridge irb  
!  
!  
interface Dot11Radio0  
no ip address  
no ip route-cache  
shutdown  
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0  
station-role root  
bridge-group 1  
bridge-group 1 subscriber-loop-control  
bridge-group 1 block-unknown-source  
no bridge-group 1 source-learning  
no bridge-group 1 unicast-flooding  
bridge-group 1 spanning-disabled  
!  
interface Dot11Radio1  
no ip address  
no ip route-cache  
shutdown  
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0  
station-role root  
bridge-group 1  
bridge-group 1 subscriber-loop-control  
bridge-group 1 block-unknown-source  
no bridge-group 1 source-learning  
no bridge-group 1 unicast-flooding  
bridge-group 1 spanning-disabled  
!  
interface FastEthernet0  
no ip address  
no ip route-cache
```



```
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

## DHCP サービスを提供するためのアクセスポイントの設定

次の項では、ワイヤレス デバイスを DHCP サーバとして機能させる方法について説明します。

- 「[DHCP サーバの設定](#)」(P.5-25)
- 「[DHCP サーバ アクセスポイントのモニタリングと維持](#)」(P.5-27)

### DHCP サーバの設定

デフォルトでは、アクセスポイントは、ネットワーク上の DHCP サーバから IP 設定を受信するように設定されています。アクセスポイントを DHCP サーバとして機能するように設定し、IP 設定を、有線 LAN と無線 LAN 両方のデバイスに割り当てることもできます。



(注) アクセスポイントを DHCP サーバとして設定すると、IP アドレスがそのサブネット上のデバイスに割り当てられます。このデバイスは、サブネット上の他のデバイスと通信しますが、それ以上先とは通信しません。サブネットより先にデータを送信する必要がある場合は、デフォルトのルータを割り当てる必要があります。デフォルトルータの IP アドレスには、DHCP サーバとして設定したアクセスポイントと同じサブネット上のものを設定してください。

DHCP 関連のコマンドとオプションの詳細は、リリース 12.3 の『Cisco IOS IP Configuration Guide』の「Configuring DHCP」の章を参照してください。「Configuring DHCP」の章を参照するには、次の URL をクリックしてください。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr\\_c/ipcprt1/1cfdhcp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm)

特権 EXEC モードから、次の手順に従って、アクセスポイントが DHCP サービスを提供するように設定し、デフォルトルータを指定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>ip dhcp excluded-address</b> <i>low_address</i> [ <i>high_address</i> ]	ワイヤレス デバイスが割り当てるアドレス範囲から、ワイヤレス デバイスの IP アドレスを除外します。IP アドレスを、10.91.6.158 のように 4 つのグループに区切って入力します。  ワイヤレス デバイスでは、DHCP アドレス プール サブネット中のすべての IP アドレスを DHCP クライアントへの割り当てに使用できると仮定されます。DHCP サーバがクライアントに割り当てるべきでない IP アドレスを指定する必要があります。  (任意) 除外するアドレスの範囲を指定するには、範囲の下限のアドレスの後に、範囲の上限のアドレスを入力します。
ステップ 3	<b>ip dhcp pool</b> <i>pool_name</i>	DHCP 要求に応じてワイヤレス デバイスが割り当てる IP アドレスのプールの名前を生成し、DHCP コンフィギュレーション モードを開始します。
ステップ 4	<b>network</b> <i>subnet_number</i> [ <i>mask</i>   <i>prefix-length</i> ]	アドレス プールにサブネット番号を割り当てます。ワイヤレス デバイスは、このサブネット内の IP アドレスを割り当てます。  (任意) アドレス プールにサブネット マスクを割り当てるか、アドレス接頭辞を構成するビット数を指定します。接頭辞はネットワーク マスクを割り当てる代替法です。プレフィックス長は、スラッシュ (/) で開始する必要があります。
ステップ 5	<b>lease</b> { <i>days</i> [ <i>hours</i> ] [ <i>minutes</i> ]   <b>infinite</b> }	ワイヤレス デバイスによって割り当てられた IP アドレスのリース期間を設定します。  <ul style="list-style-type: none"> <li>days : 日数でリース期間を設定します。</li> <li>(任意) hours : 時間数でリース期間を設定します。</li> <li>(任意) minutes : 分数でリース期間を設定します。</li> <li>infinite : リース期間を無限に設定します。</li> </ul>
ステップ 6	<b>default-router</b> <i>address</i> [ <i>address2</i> ... <i>address</i> 8]	サブネット上の DHCP クライアントに対し、デフォルトルータの IP アドレスを指定します。求められるのは 1 つの IP アドレスですが、コマンド行 1 行につき最大 8 つまでのアドレスを指定できます。
ステップ 7	<b>end</b>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 8	<code>show running-config</code>	入力内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルト設定に戻すには、これらのコマンドの **no** 形式を使用します。

この例では、ワイヤレス デバイスを DHCP サーバとして設定する方法を示しています。IP アドレスの範囲は省略し、デフォルト ルータを割り当てています。

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

## DHCP サーバアクセスポイントのモニタリングと維持

次の項では、DHCP サーバアクセスポイントのモニタと維持に使用できるコマンドについて説明します。

- 「[show コマンド](#)」 (P.5-27)
- 「[clear コマンド](#)」 (P.5-28)
- 「[debug コマンド](#)」 (P.5-28)

### show コマンド

DHCP サーバとしてのワイヤレス デバイスに関する情報を表示するには、EXEC モードで [表 5-2](#) 中のコマンドを入力します。

**表 5-2** DHCP サーバ用の show コマンド

コマンド	目的
<code>show ip dhcp conflict [ address ]</code>	特定の DHCP サーバによって記録されているすべてのアドレス競合のリストを表示します。ワイヤレス デバイスの IP アドレスを入力すると、ワイヤレス デバイスによって記録されている競合が表示されます。
<code>show ip dhcp database [ url ]</code>	DHCP データベースでの最近のアクティビティを表示します。 <b>(注)</b> このコマンドは特権 EXEC モードで使用してください。
<code>show ip dhcp server statistics</code>	送受信されたサーバの統計情報やメッセージに関するカウント情報を表示します。

## clear コマンド

DHCP サーバ変数を消去するには、特権 EXEC モードで表 5-3 中のコマンドを使用します。

表 5-3 DHCP サーバ用の clear コマンド

コマンド	目的
<b>clear ip dhcp binding</b> { address   * }	DHCP データベースから自動アドレス バインディングを削除します。address 引数を指定すると、特定の（クライアント）IP アドレスの自動バインディングが消去されます。アスタリスク（*）を指定すると、すべての自動バインディングが消去されます。
<b>clear ip dhcp conflict</b> { address   * }	DHCP データベースのアドレス競合をクリアします。address 引数を指定すると、特定の IP アドレスの競合が消去されます。アスタリスク（*）を指定すると、すべてのアドレスの競合が消去されます。
<b>clear ip dhcp server statistics</b>	すべての DHCP サーバのカウンタを 0 にリセットします。

## debug コマンド

DHCP サーバのデバッグを有効にするには、特権 EXEC モードで次のコマンドを使用します。

**debug ip dhcp server** { events | packets | linkage }

ワイヤレス デバイス DHCP サーバのデバッグを無効にするには、このコマンドの **no** 形式を使用します。

# アクセスポイントのセキュアシェルの設定

この項では、セキュアシェル（SSH）機能の設定方法について説明します。



(注)

この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Security Command Reference for Release 12.3』の「Secure Shell Commands」の項を参照してください。

## SSH について

SSH は、レイヤ 2 デバイスまたはレイヤ 3 デバイスに安全なリモート接続を提供するプロトコルです。SSH には、SSH バージョン 1 と SSH バージョン 2 の 2 種類のバージョンがあります。このソフトウェア リリースでは、どちらの SSH バージョンもサポートします。バージョン番号を指定しないと、アクセスポイントがデフォルトのバージョン 2 になります。

SSH はデバイスの認証時に強力な暗号化を行うため、Telnet よりもリモート接続の安全性が高くなります。SSH 機能では SSH サーバと SSH 統合クライアントを使用します。クライアントは次のユーザ認証方式をサポートしています。

- RADIUS（詳細については、「RADIUS によるアクセスポイントへのアクセスの制御」(P.5-12) を参照してください)

- ローカル認証および許可（詳細については、「[アクセスポイントのローカル認証および許可の設定](#)」(P.5-22)を参照)

SSHの詳細については、『*Cisco IOS Security Configuration Guide for Release 12.3*』の「Other Security Features」のパート5を参照してください。



(注)

このソフトウェアリリースのSSH機能はIP Security (IPsec)をサポートしていません。

## SSHの設定

SSHを設定する前に、Cisco.comから暗号ソフトウェアイメージをダウンロードします。詳細は、このリリースのリリースノートを参照してください。

SSHの設定方法とSSH設定の表示方法については、『*Cisco IOS Security Configuration Guide for Release 12.3*』の「Other Security Features」のパート5を参照してください。次のCisco.comから入手できます。

[http://cisco.com/en/US/products/sw/iosswrel/ps5187/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://cisco.com/en/US/products/sw/iosswrel/ps5187/products_installation_and_configuration_guides_list.html)

## セキュアコピープロトコルのサポート

セキュアコピープロトコル (SCP) は、セキュリティのためにセキュアシェル (SSH) を使用してネットワーク上のホスト間のファイル転送をサポートします。Cisco IOS リリース 15.2(2)JB は、アクセスポイント自体へのログイン中に、アクセスポイントとの間の SCP ファイル転送をサポートします。

AAA 認証を使用してデータ転送が制限されます。SCP では、AAA 認証を使用してユーザ名とパスワードを確認して、転送中のデータの完全性と機密性を確保できます。

SSHを設定するには、次のコマンドを使用します。

- ip hostname**
- ip domain-name**
- crypto key generate rsa (512, 1024, 2048)**
- ip SSH version**
- aaa new-model**
- aaa authentication login default local**
- aaa authorization exec default local**
- username cisco privilege 15 password 0 cisco**

SCPを実行するには、**copy run scp://url** コマンドを使用します。

## クライアント ARP キャッシングの設定

アソシエートされたクライアントデバイスの Address Resolution Protocol (ARP; アドレスレゾリューションプロトコル) キャッシュを保持するように、ワイヤレスデバイスを設定できます。ワイヤレスデバイスでARPキャッシュを保持すると、無線LANのトラフィック負荷が軽減されます。ARPキャッシングはデフォルトで無効に設定されています。

## ■ クライアント ARP キャッシングの設定

ここでは、次の情報について説明します。

- 「クライアント ARP キャッシングの概要」 (P.5-30)
- 「ARP キャッシングの設定」 (P.5-30)

## クライアント ARP キャッシングの概要

ワイヤレス デバイスでの ARP キャッシングは、クライアント デバイスへの ARP 要求をワイヤレス デバイスで止めることによって、無線 LAN 上のトラフィックを軽減します。ワイヤレス デバイスは、ARP 要求をクライアント デバイスへ転送する代わりに、アソシエートされたクライアント デバイスに代わって ARP 要求に応答します。

ARP キャッシングを無効にすると、ワイヤレス デバイスはすべての ARP 要求をアソシエートされたクライアントに無線ポート経由で転送し、ARP 要求を受け取ったクライアントが応答します。一方、ARP キャッシングを有効にすると、ワイヤレス デバイスはアソシエートされたクライアントに代わって ARP 要求に応答し、クライアントへは要求を転送しません。ワイヤレス デバイスがキャッシュにない IP アドレスに向けた ARP 要求を受け取ると、ワイヤレス デバイスはその要求をドロップして転送しません。ワイヤレス デバイスは、ビーコンに情報エレメントを追加して、バッテリーの寿命を延ばすためのブロードキャスト メッセージを安全に無視できることをクライアント デバイスに通知します。

## オプションの ARP キャッシング

アクセス ポイントにシスコ製以外のクライアント デバイスがアソシエートされ、そのデバイスがデータを通さない場合、ワイヤレス デバイスがそのクライアントの IP アドレスを認識していない可能性があります。無線 LAN でこの状況が頻発する場合は、オプションの ARP キャッシングを有効にできます。ARP キャッシングがオプションの場合、ワイヤレス デバイスはワイヤレス デバイスに既知の IP アドレスのクライアントについては、その代理として応答しますが、不明なクライアント宛ての ARP 要求はすべて無線ポートから転送します。アソシエートされた全クライアントの IP アドレスを記憶すると、ワイヤレス デバイスはそれらのアソシエートされたクライアント以外に対する ARP 要求をドロップします。

## ARP キャッシングの設定

特権 EXEC モードから、次の手順に従って、アソシエートされたクライアントの ARP キャッシングを保持するようにワイヤレス デバイスを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 arp-cache [ optional ]</code>	ワイヤレス デバイスでの ARP キャッシングを有効にします。 <ul style="list-style-type: none"> <li>• (任意) ワイヤレス デバイスが認識している IP アドレスのクライアント デバイスに限って ARP キャッシングを有効にするには、<b>optional</b> キーワードを使用します。</li> </ul>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例に、アクセスポイントで ARP キャッシングを設定する方法の例を示します。

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

## システム日時の管理

ワイヤレス デバイスのシステムの時刻と日付は、Simple Network Time Protocol (SNTP; 簡易ネットワーク タイム プロトコル) を使用して自動的に管理することも、ワイヤレス デバイスに時刻と日付を設定して手動で管理することもできます。



(注) この項で使用されるコマンドの構文と使用方法の詳細は、リリース 12.3 の『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

ここでは、次の設定情報について説明します。

- 「簡易ネットワーク タイム プロトコルの概要」(P.5-31)
- 「SNTP の設定」(P.5-32)
- 「手動での日時の設定」(P.5-32)

## 簡易ネットワーク タイム プロトコルの概要

簡易ネットワーク タイム プロトコル (SNTP) とは、クライアント専用バージョンの簡易版 NTP です。SNTP は、NTP サーバから時間を受信するだけで、他のシステムに時刻サービスを提供することはできません。通常、SNTP は 100 ミリ秒以内の精度で時刻を提供しますが、NTP のような複雑なフィルタリングや統計メカニズムは提供しません。

SNTP は、設定済みのサーバからパケットを要求して受け入れるように設定するか、任意の送信元から NTP ブロードキャスト パケットを受け入れるように設定できます。複数の送信元が NTP パケットを送信している場合、最適な層にあるサーバが選択されます。NTP とストラタムの詳細は、次の URL をクリックしてください。

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_configuration\\_guide\\_chapter09186a00800ca66f.html#1001131](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66f.html#1001131)

複数のサーバのストラタムが同じだった場合は、ブロードキャスト サーバよりも設定済みサーバが優先されます。これらの両方を満たすサーバが複数ある場合は、時刻パケットを最初に送信したサーバが選択されます。現在選択中のサーバからパケット受信が途絶えたり、または上記の基準に基づいてより最適なサーバが検出されたりしない限り、SNTP が新たにサーバを選択することはありません。



## SNTP の設定

SNTP は、デフォルトでディセーブルになっています。アクセスポイントで SNTP をイネーブルにするには、表 5-4 に示すコマンドのいずれか、または両方をグローバル コンフィギュレーション モードで使用します。

表 5-4 SNTP コマンド

コマンド	目的
<code>sntp server {address   hostname} [version number]</code>	NTP サーバからの NTP パケットを要求するように SNTP を設定します。
<code>sntp broadcast client</code>	任意の NTP ブロードキャストからの NTP パケットを受け入れるように SNTP を設定します。

各 NTP サーバについて、`sntp server` コマンドを 1 回入力します。NTP サーバは、アクセスポイントからの SNTP メッセージに応答できるよう設定しておく必要があります。

`sntp server` コマンドと `sntp broadcast client` コマンドの両方を入力した場合、アクセスポイントはブロードキャストサーバからの時間を受け付けますが、同一のストラタムと判断して設定済みサーバからの時間の方を優先します。SNTP に関する情報を表示するには、`show sntp EXEC` コマンドを使用します。

## 手動での日時の設定

他のタイムソースが使用できない場合は、システムの再起動後、手動で日時を設定できます。時刻は、次にシステムを再起動するまで正確です。手動設定は最後の手段としてのみ使用することを推奨します。ワイヤレスデバイスが同期できる外部ソースがある場合は、システムクロックを手動で設定する必要はありません。

ここでは、次の設定情報について説明します。

- 「システムクロックの設定」(P.5-32)
- 「日時設定の表示」(P.5-33)
- 「タイムゾーンの設定」(P.5-33)
- 「夏時間の設定」(P.5-34)

## システムクロックの設定

ネットワーク上に、NTP サーバなどの時刻サービスを提供する外部ソースがある場合、手動でシステムクロックを設定する必要はありません。



システム クロックを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>clock set hh:mm:ss day month year</code> または <code>clock set hh:mm:ss month day year</code>	次のいずれかの書式を使ってシステム クロックを手動で設定します。 <ul style="list-style-type: none"><li><code>hh:mm:ss</code> には、時刻を時間 (24 時間形式)、分、秒で指定します。指定された時刻は、設定されたタイムゾーンに基づきます。</li><li><code>day</code> には、当月の日付で日を指定します。</li><li><code>month</code> には、月を名前で指定します。</li><li><code>year</code> には、年を指定します (常に 4 桁で指定)。</li></ul>
ステップ 2	<code>show running-config</code>	入力内容を確認します。
ステップ 3	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次に、システム クロックを手動で 2001 年の 7 月 23 日午後 1 時 32 分に設定する例を示します。

```
AP# clock set 13:32:00 23 July 2001
```

## 日時設定の表示

日時の設定を表示するには、`show clock [detail]` 特権 EXEC コマンドを使用します。

システム クロックは、信頼性がある (正確であると信じられる) かどうかを示す *authoritative* フラグを維持します。システム クロックがタイミグ ソースによって設定されている場合は、フラグを設定します。時刻が信頼性のないものである場合は、表示目的でのみ使用されます。クロックが信頼できず、*authoritative* フラグも設定されていないければ、ピアの時刻が無効でも、フラグはピアがクロックと同期しないようにします。

`show clock` の表示の前にある記号は、次の意味があります。

- \* : 時刻は信頼できません。
- (空白) : 時刻は信頼できます。
- . : 時刻は信頼できますが、NTP は同期していません。

## タイムゾーンの設定

手動でタイムゾーンを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>clock timezone zone hours-offset</b> [minutes-offset]	タイムゾーンを設定します。 ワイヤレス デバイスは内部時間を協定世界時 (UTC) で維持するため、このコマンドは表示専用で、時刻を手動で設定するときだけに使用されます。 <ul style="list-style-type: none"> <li>• <i>zone</i> には、標準時間が施行されているときに表示されるタイムゾーンの名前を入力します。デフォルトは UTC です。</li> <li>• <i>hours-offset</i> には、UTC からの時差を入力します。</li> <li>• (任意) <i>minutes-offset</i> には、UTC からの分差を入力します。</li> </ul>
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	入力内容を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

**clock timezone** グローバル コンフィギュレーション コマンドの **minutes-offset** 変数は、現地のタイムゾーンと UTC との時差が分単位である場合に使用できます。たとえば、カナダ大西洋沿岸のある区域のタイムゾーン (大西洋標準時 (AST)) は UTC-3.5 です。この場合、3 は 3 時間、.5 は 50% を意味します。この場合、必要なコマンドは **clock timezone AST -3 30** です。

時刻を UTC に設定するには、**no clock timezone** グローバル コンフィギュレーション コマンドを使用します。

## 夏時間の設定

毎年特定の曜日に夏時間が開始して終了する地域に夏時間を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>clock summer-time zone recurring</b> [week day month hh:mm week day month hh:mm [offset]]	毎年指定した日に開始および終了するように夏時間を設定します。 夏時間はデフォルトでディセーブルに設定されています。パラメータなしで <b>clock summer-time zone recurring</b> を指定すると、夏時間のルールは米国のルールをデフォルトにします。 <ul style="list-style-type: none"> <li>• <i>zone</i> には、夏時間が施行されているときに表示されるタイムゾーンの名前 (たとえば PDT) を入力します。</li> <li>• (任意) <i>week</i> には、月の何週目かを指定します (1 ~ 5、または last)。</li> <li>• (任意) <i>day</i> には、曜日を指定します (Sunday、Monday など)。</li> <li>• (任意) <i>month</i> には、月を指定します (January、February など)。</li> <li>• (任意) <i>hh:mm</i> には、時刻を時間 (24 時間形式) と分で指定します。</li> <li>• (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。</li> </ul>
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

**clock summer-time** グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイムゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

次に、夏時間が4月の第一日曜の2時に始まり、10月の最終日曜の2時に終わるように指定する例を示します。

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

ユーザの居住地の夏時間が定期的なパターンに従わない (次の夏時間のイベントの正確な日時を設定する) 場合は、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>clock summer-time zone date</code> [ <i>month date year hh:mm month date year hh:mm [offset]</i> ]  または <code>clock summer-time zone date</code> [ <i>date month year hh:mm date month year hh:mm [offset]</i> ]	最初の日付で夏時間開始の日付を、2 番目の日付で終了の日付を設定します。  夏時間はデフォルトでディセーブルに設定されています。 <ul style="list-style-type: none"> <li>• <i>zone</i> には、夏時間が施行されているときに表示されるタイムゾーンの名前 (たとえば PDT) を入力します。</li> <li>• (任意) <i>week</i> には、月の何週目かを指定します (1 ~ 5、または <b>last</b>)。</li> <li>• (任意) <i>day</i> には、曜日を指定します (Sunday、Monday など)。</li> <li>• (任意) <i>month</i> には、月を指定します (January、February など)。</li> <li>• (任意) <i>hh:mm</i> には、時刻を時間 (24 時間形式) と分で指定します。</li> <li>• (任意) <i>offset</i> には、夏時間の間、追加する分の数を指定します。デフォルト値は 60 です。</li> </ul>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

**clock summer-time** グローバル コンフィギュレーション コマンドの最初の部分では夏時間の開始時期を、2 番目の部分では終了時期を指定します。すべての時刻は、現地のタイムゾーンを基準にしています。開始時間は標準時を基準にしています。終了時間は夏時間を基準にしています。開始月が終了月より後の場合は、システムでは南半球にいると見なされます。

夏時間をディセーブルにするには、**no clock summer-time** グローバル コンフィギュレーション コマンドを使用します。

次に、夏時間が2000年10月12日の2時に始まり、2001年4月26日の2時に終わるように設定する例を示します。

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 2:00
```

## HTTP アクセスの定義

デフォルトでは、80 が HTTP アクセスに使用され、ポート 443 が HTTPS アクセスに使用されます。この値は、ユーザがカスタマイズできます。HTTP アクセスの定義方法は、次のとおりです。

- 
- ステップ 1 アクセスポイントの GUI から、[Services] > [HTTP] の順にクリックします。[Service: HTTP-Web server] 画面が表示されます。
  - ステップ 2 この画面に、目的の HTTP と HTTPS のポート番号を入力します。このポート番号フィールドに値を入力しないと、デフォルト値が使用されます。
  - ステップ 3 [Apply] をクリックします。
- 

## システム名およびプロンプトの設定

ワイヤレス デバイスを識別するシステム名を設定します。デフォルトでは、システム名とプロンプトは *ap* です。

システム プロンプトを設定していない場合は、システム名の最初の 20 文字をシステム プロンプトとして使用します。大なり記号 (>) が追加されます。プロンプトは、システム名が変更されると必ず更新されますが、グローバル コンフィギュレーション コマンド **prompt** を使用して手動でプロンプトを設定している場合は更新されません。



(注) この項で使用されるコマンドの構文と使用方法の詳細は、『Cisco IOS Configuration Fundamentals Command Reference』およびリリース 12.3 の『Cisco IOS IP and IP Routing Command Reference』を参照してください。

ここでは、次の設定情報について説明します。

- 「デフォルトのシステム名およびプロンプトの設定」(P.5-36)
- 「システム名の設定」(P.5-36)
- 「DNS の概要」(P.5-37)

## デフォルトのシステム名およびプロンプトの設定

アクセスポイントのデフォルトのシステム名とプロンプトは *ap* です。

## システム名の設定

手動でシステム名を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>hostname name</code>	<p>手動でシステム名を設定します。</p> <p>デフォルト設定は <code>ap</code> です。</p> <p>(注) システム名を変更する場合、ワイヤレス デバイスの無線はリセットされ、アソシエートしているクライアント デバイスはアソシエーションが解除され、ただちに再アソシエートされます。</p> <p>(注) システム名には、63 文字まで入力することができます。しかし、ワイヤレス デバイスでは、クライアント デバイスに自分自身を識別させる際に、システム名の最初の 15 文字だけを使用します。クライアント ユーザがアクセス ポイントを区別することが重要な場合、システム名の一意の部分を最初の 15 文字に含めてください。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

システム名を設定すると、システム プロンプトとしても使用されます。

デフォルトのホスト名に戻すには、グローバル コンフィギュレーション コマンド `no hostname` を使用します。

## DNS の概要

ドメイン ネーム システム (DNS) プロトコルは、DNS 分散型データベースを制御し、これによりホスト名を IP アドレスに対応付けできます。ワイヤレス デバイスに DNS を設定すると、**ping**、**telnet**、**connect**、などすべての IP コマンドおよび関連する Telnet サポート操作で、IP アドレスの代わりにホスト名を使用できます。

IP によって定義される階層型の命名方式では、デバイスを場所またはドメインで特定できません。ドメイン名は、ピリオド (.) を区切り文字として使用して構成されています。たとえば、シスコは、IP で `com` というドメイン名に分類される商業組織なので、ドメイン名は `cisco.com` となります。このドメイン内のファイル転送プロトコル (FTP) システムなどの個々のデバイスは `ftp.cisco.com` のように識別されます。

IP ではドメイン名をトラッキングするために、ドメイン ネーム サーバという概念が定義されています。ドメイン ネーム サーバの役割は、名前から IP アドレスへのマッピングをキャッシュ (またはデータベース) に保存することです。ドメイン名を IP アドレスにマッピングするには、まずホスト名を特定し、ネットワーク上に存在するネーム サーバを指定し、DNS を有効にします。

ここでは、次の設定情報について説明します。

- 「DNS のデフォルト設定」 (P.5-38)
- 「DNS の設定」 (P.5-38)
- 「DNS の設定の表示」 (P.5-39)

## DNS のデフォルト設定

表 5-5 に、DNS のデフォルト設定を示します。

表 5-5 DNS のデフォルト設定

機能	デフォルト設定
DNS イネーブル ステート	ディセーブル
DNS デフォルト ドメイン名	未設定
DNS サーバ	ネーム サーバのアドレスが未設定

## DNS の設定

特権 EXEC モードから、次の手順に従って DNS を使用するようにワイヤレス デバイスを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip domain-name name</code>	ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。  ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。  ブート時にはドメイン名は設定されていませんが、ワイヤレス デバイスの設定が BOOTP または Dynamic Host Configuration Protocol (DHCP) サーバから行われている場合、BOOTP または DHCP サーバによってデフォルトのドメイン名が設定されることがあります（この情報がサーバに設定されている場合）。
ステップ 3	<code>ip name-server server-address1 [server-address2 ... server-address6]</code>	1 つまたは複数のネーム サーバのアドレスを指定して、名前およびアドレスの解決に使用します。  最大 6 つのネーム サーバを指定できます。各サーバアドレスはスペースで区切ります。最初に指定されたサーバが、プライマリ サーバです。ワイヤレス デバイスは、最初にプライマリ サーバへ DNS クエリを送信します。そのクエリが失敗した場合は、バックアップサーバにクエリが送信されます。
ステップ 4	<code>ip domain-lookup</code>	(任意) ワイヤレス デバイスで DNS ベースのホスト名からアドレスへの変換を有効にします。この機能は、デフォルトでイネーブルにされています。  ユーザのネットワークデバイスが、名前の割り当てを制御できないネットワーク内のデバイスと接続する必要がある場合、グローバルなインターネットのネーミング方式 (DNS) を使用して、ユーザのデバイスを一意に識別するデバイス名を動的に割り当てることができます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ワイヤレス デバイスの IP アドレスをホスト名として使用する場合、この IP アドレスが使用されるため DNS クエリは作成されません。ピリオド (.) を含まないホスト名を設定すると、名前を IP アドレスにマッピングする DNS クエリが作成される前に、ホスト名の後にピリオドとデフォルトのドメイン名が追加されます。デフォルトのドメイン名は、グローバル コンフィギュレーション コマンド **ip domain-name** で設定される値です。ホスト名にピリオド (.) が含まれている場合、Cisco IOS ソフトウェアはホスト名にデフォルトのドメイン名を追加せずに、IP アドレスを検索します。

ドメイン名を削除するには、**no ip domain-name name** グローバル コンフィギュレーション コマンドを使用します。ネームサーバのアドレスを削除するには、**no ip name-server server-address** グローバル コンフィギュレーション コマンドを使用します。ワイヤレス デバイスで DNS を無効にするには、グローバル コンフィギュレーション コマンド **no ip domain-lookup** を使用します。

## DNS の設定の表示

DNS 設定情報を表示するには、**show running-config** 特権 EXEC コマンドを使用します。



(注) ワイヤレス デバイスに DNS が設定されている場合、**show running-config** コマンドを実行すると、サーバの名前ではなく IP アドレスが表示される場合があります。

## バナーの作成

今日のお知らせ (MOTD) バナーとログイン バナーを設定できます。MOTD バナーはログイン時に、接続されたすべての端末に表示されます。すべてのネットワーク ユーザに影響するメッセージ (差し迫ったシステム シャットダウンの通知など) を送信する場合に便利です。

ログイン バナーも接続されたすべての端末に表示されます。表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。



(注) この項で使用されるコマンドの構文と使用方法の詳細は、リリース 12.3 の『Cisco IOS Configuration Fundamentals Command Reference』を参照してください。

ここでは、次の設定情報について説明します。

- 「バナーのデフォルト設定」(P.5-39)
- 「MoTD ログイン バナーの設定」(P.5-39)
- 「ログイン バナーの設定」(P.5-40)

## バナーのデフォルト設定

MoTD およびログイン バナーは設定されません。

## MoTD ログイン バナーの設定

ワイヤレス デバイスにログインしたときに画面に表示される 1 行以上の行のメッセージ バナーを作成できます。

MoTD ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>banner motd c message c</b>	MoTD バナーを指定します。  c にはポンド記号 (#) など希望する区切り文字を入力し、Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。  message には、255 文字までのバナー メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	入力内容を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

MoTD バナーを削除するには、**no banner motd** グローバル コンフィギュレーション コマンドを使用します。

次の例は、開始および終了区切り文字にポンド記号 (#) を使用して、ワイヤレス デバイスに MOTD バナーを設定する方法を示しています。

```
AP(config)# banner motd #
This is a secure site.Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#
```

次の例は、上記の設定で表示されるバナーを示しています。

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site.Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

## ログイン バナーの設定

接続したすべての端末に表示されるログイン バナーを設定できます。バナーが表示されるのは、MoTD バナーの後で、ログイン プロンプトが表示される前です。

ログイン バナーを設定するには、特権 EXEC モードで次の手順を実行します。



	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>banner login c message c</code>	ログイン メッセージを指定します。  <i>c</i> にはポンド記号 (#) など希望する区切り文字を入力し、Return キーを押します。区切り文字はバナー テキストの始まりと終わりを表します。終わりの区切り文字の後ろの文字は廃棄されます。  <i>message</i> には、255 文字までのログイン メッセージを入力します。メッセージ内には区切り文字を使用できません。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ログイン バナーを削除するには、`no banner login` グローバル コンフィギュレーション コマンドを使用します。

次の例は、開始および終了区切り文字にドル記号 (\$) を使用して、ワイヤレス デバイスにログイン バナーを設定する方法を示しています。

```
AP(config)# banner login $
Access for authorized users only.Please enter your username and password.
$
AP(config)#
```

## 自律 Cisco Aironet アクセスポイントを Lightweight モードにアップグレードする方法

ネットワーク上で無線 LAN コントローラと通信できるよう、自律 Cisco Aironet アクセスポイントを Lightweight モードにアップグレードするユーティリティが用意されています。このアップグレード ユーティリティの使用の詳細は、次の URL をご覧ください。

[http://www.cisco.com/en/US/docs/wireless/access\\_point/conversion/lwapp/upgrade/guide/lwapnote.html#wp156967](http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html#wp156967)

自律アクセスポイントを Lightweight モードに変換するには、アクセスポイントに Telnet し、次のコマンドを実行します。

```
archive download-sw | overwrite | reload tftp: //location/image-name
```

詳細については、『*Upgrading Cisco IOS on an Autonomous Access Point*』を参照してください。URL は、次のとおりです。

[http://www.cisco.com/en/US/tech/tk722/tk809/technologies\\_configuration\\_example09186a00809f0e94.shtml](http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00809f0e94.shtml)

## 日本の W52 ドメインへの移行方法

このユーティリティは、802.11a 無線を J52 から W52 ドメインに移行する際に使用します。このユーティリティは、1130 と 1240 アクセスポイントで動作する他、RM20、RM21 および RM22A 無線を装備した 1200 アクセスポイントで動作します。802.11a 無線が付属していないアクセスポイントには、この移行はサポートされていません。

次のインターフェイスのグローバル コンフィギュレーション モードの CLI コマンドを使用して、アクセスポイントの 802.11a 無線を W52 ドメインに移行します。

### dot11 migrate j52 w52

警告メッセージが表示されたら、**y** を入力します。移行プロセスが始まり、アクセスポイントが 2 回リブートしたら完了です。無線ハードウェアをリセットすると、ファームウェア初期化コードが規制ドメインを読み取って初期化します。ハードウェアをリセットすると、ファームウェアをリロードし、無線のイメージをフラッシュしてから初期化処理を進めます。無線が規制ドメインを選択していることを確認するため、アクセスポイントが 2 回目のリブートを開始します。

次の例は移行の完了方法を示しています。

```
ap>enable
Password:
ap#config terminal
ap(config)interface dot11radio0
ap(config-if)#dot11 migrate j52 w52
Migrate APs with 802.11A Radios in the "J"
Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies

WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated, the 802.11A radios will not operate with previous OS versions.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
This AP is eligible for migration:
ap      AIR-AP1242AG-A-K9      0013.5f0e.d1e0  "J" Regulatory Domain
Begin to migrate Access Point from J (J52) to U (W52).do you want to Continue
?(yes/[no]):yes
Burning cookie into serial eeprom:
Reading cookie from system serial eeprom...done.
Editing copy...done.
Writing cookie into system serial eeprom...done.

*Mar  1 00:09:13.844: %DOT11-4-UPGRADE: **** Send your company name and the following
report to:  migrateapj52w52@cisco.com

The following AP has been migrated from J(J52) to U(W52) Regulatory Domain:
AP Name      AP Model      Ethernet MAC
ap           AIR-AP1242AG-A-K9      0013.5f0e.d1e0 "U" Regulatory Domain
*Mar  1 00:09:13.844: Convert Regulatory Domain from J (J52) to U (W52).Writing AP nvram.
*Mar  1 00:09:14.060: %SYS-5-RELOAD: Reload requested by Exec.Reload Reason: CONVERT
REGULATORY DOMAIN FROM J to U
```

**no** を選択すると、次の例に示すように操作が停止します。

```
...
Begin to migrate Access Point from J (J52) to U (W52).do you want to Continue
?(yes/[no]):no
AP not migrated.

ap(config-if)#
```

## 移行の確認

**show controllers** コマンドを使用して、次の例に示すように移行を確認します。

```
ap#show controllers dot11Radio 1
!
interface Dot11Radio1
Radio AIR-AP1242A, Base Address 0013.5f0e.d1e0, BBlock version
0.00, Software version 5.95.7
Serial number: ALP0916W015
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: Japan (UNI1) (JP )
Uniform Spreading Required: No
Current Frequency: 0 MHz Channel 0
Allowed Frequencies: 5180(36) 5200(40) 5220(44) 5240(48)

Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) 5180(36)
5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64)
5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5600(120)
5620(124) 5640(128) 5660(132) 5680(136) 5700(140) 5745(149)
5765(153) 5785(157) 5805(161) 5825(165)
Beacon Flags: 0; Beacons are disabled; Probes are disabled High Density mode disabled
  Local Rx sensitivity (Config -127, Max -57, Min -17, Active 0) dBm
    CCA Sensitivity -64 dBm
  Cell Rx sensitivity -80 dBm, CCA Sensitivity -60 dBm, Tx Power 127 dBm
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
Current Rates: basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Active Rates:
Allowed Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: basic-6.0 basic-9.0 basic-12.0 basic-
18.0 basic-24.0 basic-36.0 basic-48.0 basic-54.0
```



(注) 移行後は、国コードが JP から JU にアップデートされます。移行されていない無線は、まだ国コード JP で表示されます。

## ポイントツーマルチポイントブリッジにおける複数のVLANとレート制限の設定

この機能は、ポイントツーマルチポイントブリッジ方法を変更したもので、複数のVLANで動作しながら各VLANでトラフィックレートを管理できるように設定するものです。この機能は、ブリッジとして設定した32 Mbの1040、1140、1240、1250、および1260アクセスポイントと、1300シリーズアクセスポイント/ブリッジで利用できます。16Mbアクセスポイント(1100、1200、350シリーズ)では利用できません。



(注) レート制限ポリシーは、非ルートブリッジのファストイーサネット入力ポートの入力ポートだけに適用できます。

通常、複数のVLANをサポートしていると、別々のVLAN上にある各リモートサイトでポイントツーマルチポイントブリッジリンクを設定できます。この設定では、各サイトへのトラフィックを切り分けて管理できてしまいます。レート制限機能は、リンク帯域幅全体のうち指

定した量を超えて消費しないようリモートサイトに設定するものです。アップリンクトラフィックを管理できるのは、非ルートブリッジのファストイーサネット入力ポートだけからです。

クラスベースのポリシング機能を使用すると、レート制限を指定して、これを非ルートブリッジのイーサネットインターフェイスの入力に適用できます。イーサネットインターフェイスの入力にレートを適用すると、すべての受信イーサネットパケットが設定したレートに適合します。

次の設定は、**class-map** コマンドを使用したトラフィッククラスの定義方法を示しています。また **policy-map** コマンドで、サービスポリシングに設定したトラフィックポリシング設定をトラフィッククラスの基準と関連付ける方法を示しています。例では、ファストイーサネット0インターフェイスの受信パケットすべてに対して、トラフィックポリシングは平均レートの8000ビット/秒、および通常バーストサイズの1000バイトで設定されています。

```
AP enable
AP#config terminal
AP(config)#class-map sample_class
AP(config-cmap)#match any
AP(config-cmap)#exit
AP(config)#policy-map police_setting
AP(config-pmap)#class sample_class
AP(config-pmap)#police 8000 1000 conform-action transmit exceed-action drop
AP(config-pmap-c)#exit
AP(config-pmap)#exit
AP(config)#interface fa0
AP(config-if)#service-policy input police_setting
```



(注) **class-map policy** コマンドには多数のオプションが用意されていますが、このリリースでサポートされているのは、**match any** オプションだけです。

## CLI コマンド

802.11Q タグを受信イーサネットパケットすべてに追加するには、**bridge non-root client vlan <vlan id>** コマンドを使用します。このコマンドは、非ルートブリッジだけに適用できます。



## 第 6 章

# 無線の設定

この章では、ワイヤレス デバイスに無線を設定する手順を説明します。この章は、次の項で構成されています。

- 「無線インターフェイスのイネーブル化」 (P.6-2)
- 「無線ネットワークの役割の設定」 (P.6-2)
- 「802.11n プラットフォームのポイントツーポイントおよびマルチポイントブリッジングのサポート」 (P.6-5)
- 「無線データ レートの設定」 (P.6-8)
- 「MCS レートの設定」 (P.6-12)
- 「無線の送信電力の設定」 (P.6-13)
- 「無線チャネルの設定」 (P.6-17)
- 「位置情報サービスの設定」 (P.6-24)
- 「ワールド モードのイネーブル化とディセーブル化」 (P.6-26)
- 「short 無線プリアンプルのイネーブル化とディセーブル化」 (P.6-27)
- 「送受信アンテナの設定」 (P.6-27)
- 「Gratuitous Probe Response の有効化と無効化」 (P.6-29)
- 「Aironet 拡張機能のディセーブル化およびイネーブル化」 (P.6-30)
- 「イーサネット カプセル化変換方式の設定」 (P.6-31)
- 「ワークグループブリッジへの信頼性のあるマルチキャストの有効化と無効化」 (P.6-32)
- 「Public Secure Packet Forwarding のイネーブル化とディセーブル化」 (P.6-33)
- 「ビーコン間隔と DTIM の設定」 (P.6-34)
- 「RTS しきい値と再試行回数の設定」 (P.6-35)
- 「最大データ再試行回数の設定」 (P.6-36)
- 「フラグメンテーションしきい値の設定」 (P.6-36)
- 「802.11g 無線の short スロット時間のイネーブル化」 (P.6-37)
- 「キャリア話中検査の実行」 (P.6-37)
- 「VoIP パケット処理の設定」 (P.6-37)
- 「VoWLAN メトリックの表示」 (P.6-38)
- 「ClientLink の設定」 (P.6-45)
- 「無線機能のデバッグ」 (P.6-46)

## 無線インターフェイスのイネーブル化

ワイヤレス デバイスの無線はデフォルトではディセーブルに設定されています。



(注) Cisco IOS Release 12.3(8)JA から、デフォルトの SSID は存在しません。無線インターフェイスを有効にする前に、SSID を作成する必要があります。

特権 EXEC モードから、次の手順に従ってアクセス ポイントの無線を有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 ssid ssid</code>	SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。
ステップ 3	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 802.11n 2.4GHz 無線は Radio 0 です。 5GHz 無線および 802.11n 5GHz 無線は Radio 1 です。
ステップ 4	<code>ssid ssid</code>	ステップ 2 で作成した SSID を適切な無線インターフェイスに割り当てます。
ステップ 5	<code>no shutdown</code>	無線ポートを有効にします。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

無線ポートをディセーブルにするには、`shutdown` コマンドを使用します。

## 無線ネットワークの役割の設定

表 6-1 は、各デバイスの無線ネットワークの役割を示しています。

表 6-1 無線ネットワーク設定でのデバイスの役割

無線ネットワークでの役割	AP 1040	AP 1100	AP 1130	AP 1140	AP 1200	AP 1240	AP 1250	AP 1260	1300 AP/BR
アクセス ポイント	X	X	X	X	X	X	X	X	X
アクセス ポイント (無線シャットダウンにフォールバック)	X	X	X	X	X	X	X	X	X
アクセス ポイント (リピータにフォールバック)	X	X	X	X	X	X	X	X	X
リピータ	X	X	X	X	X	X	X	X	X
ルートブリッジ	X	-	-	X	X	X	X	X	X
非ルートブリッジ	X	-	-	X	X	X	X	X	X

表 6-1 無線ネットワーク設定でのデバイスの役割 (続き)

無線ネットワークでの役割	AP 1040	AP 1100	AP 1130	AP 1140	AP 1200	AP 1240	AP 1250	AP 1260	1300 AP/BR
ワイヤレス クライアントを持つルートブリッジ	X	-	-	X	X	X	X	X	X
無線クライアントを持つ非ルートブリッジ	X	-	-	X	X	X	X	X	X
ワークグループブリッジ	X	X	X	X	X	X	X	X	X
ユニバーサル ワークグループブリッジ <sup>1</sup>	X	-	-	X	X	X	X	X	X
スキャナ	X	X	X	X	X	X	X	X	X

1. AES-CCM TKIP を使用してユニバーサル ワークグループブリッジを設定する場合、非ルート デバイスはルート デバイスとアソシエートするためには、TKIP または AES-CCM TKIP だけを暗号として使用する必要があります。AES-CCM だけで設定した場合、非ルート デバイスはルートとアソシエートできません。この設定により、ルート デバイスと非ルート デバイスの間でマルチキャスト暗号の不一致が発生します。

ルート アクセス ポイントにフォールバック ロールを設定することもできます。ワイヤレス デバイスは、イーサネット ポートがディセーブルになるか、または有線 LAN から切り離されたときに自動的にフォールバック ロール (モード) に移行します。フォールバック ロールとして次の 2 つが挙げられます。

- **Repeater** : イーサネット ポートが無効になった場合、ワイヤレス デバイスはリピータになり、近くのルート アクセス ポイントにアソシエートします。フォールバック リピータがアソシエートするルート アクセス ポイントを指定する必要はありません。リピータは最適な無線接続を提供するルート アクセス ポイントに自動的にアソシエートします。
- **Shutdown** : ワイヤレス デバイスは無線をシャットダウンし、すべてのクライアント デバイスの接続を解除します。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスの無線ネットワークの役割とフォールバック ロールを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	次の無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 802.11n 2.4GHz 無線はインターフェイス 0 です。  5GHz 無線および 802.11n 5GHz 無線はインターフェイス 1 です。

コマンド	目的
<p>ステップ 3 <b>station-role</b></p> <p><b>non-root {bridge   wireless-clients}</b></p> <p><b>repeater</b></p> <p><b>root {access-point   ap-only   [bridge   wireless-clients]   [fallback   repeater   shutdown]}</b></p> <p><b>scanner</b></p> <p><b>workgroup-bridge {multicast   mode &lt;client   infrastructure&gt;   universal &lt;Ethernet client MAC address&gt;}</b></p>	<p>ワイヤレス デバイスの役割を設定します。</p> <ul style="list-style-type: none"> <li>役割は、無線クライアントを持つまたは持たない非ルートブリッジ、リピータ アクセス ポイント、ルート アクセス ポイントまたはブリッジ、スキャナ、またはワークグループブリッジに設定します。</li> <li>ブリッジ モードが使用できるのは 1040、1140、1200、1240、1250、および 1260 シリーズ アクセス ポイントだけです。ブリッジ モードの場合、サポートされるブリッジ機能に限り、1300 シリーズ屋外アクセス ポイント/ブリッジと相互運用します。「サポートされないブリッジ機能」(P.6-8) を参照してください。</li> <li>ブリッジ モード無線はポイントツーポイントおよびポイントツーマルチポイント構成をサポートします。</li> <li>非ルート ブリッジとして動作する 1300 シリーズ屋外アクセス ポイント/ブリッジは、非ルート ブリッジのステーションの役割が <b>non-root wireless clients</b> に設定されている限り、他の非ルート ブリッジとアソシエートできます。</li> <li>いずれかの無線がリピータとして設定されると、イーサネット ポートはシャットダウンします。ワークグループブリッジまたはリピータとして設定できるのは、アクセス ポイントにつき 1 つの無線だけです。</li> <li><b>dot11radio 0/1 antenna-alignment</b> コマンドは、アクセス ポイントがリピータとして設定されるときに使用できます。</li> <li>他の無線クライアントがルート ブリッジまたはアクセス ポイントにアソシエートされていないと仮定すると、ワークグループブリッジは最大 254 のクライアントを持つことができます。</li> <li>ユニバーサル ワークグループブリッジでは、アクセス ポイントをワークグループブリッジ モードで設定し、シスコ以外のアクセス ポイントと相互運用できます。イーサネット クライアントの MAC アドレスを入力する必要があります。ワークグループブリッジは、設定された MAC アドレスがブリッジ テーブルに存在し、静的エントリでない場合に限り、その MAC アドレスにアソシエートされません。検証に失敗した場合、ワークグループブリッジはその BVI の MAC アドレスを使用してアソシエートします。また、ユニバーサル ワークグループブリッジの役割では、1 つの有線クライアントだけがサポートされます。</li> <li>スパニングツリー プロトコル (STP) は、1200、1240 シリーズ アクセス ポイントでブリッジ モードで設定できます。</li> <li>(任意) ルート アクセス ポイントのフォールバック ロールを選択します。ワイヤレス デバイスのイーサネット ポートが無効になるか、有線 LAN から切断された場合、ワイヤレス デバイスは無線ポートをシャットダウンするか、近くのルート アクセス ポイントにアソシエートしたリピータ アクセス ポイントになります。</li> </ul>



	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



(注)

無線ネットワーク内での役割をブリッジまたはワークグループブリッジとして有効化し、`no shut` コマンドを使用してインターフェイスを有効化する場合、インターフェイスの物理ステータスおよびソフトウェアステータスは、相手端末のアクセスポイントまたはブリッジが起動状態の場合だけ起動状態になります。それ以外の場合、デバイスの物理ステータスだけが起動状態になります。デバイスのソフトウェアステータスが起動状態になるのは、相手端末のデバイスが設定されて起動しているときだけです。

## ユニバーサルワークグループブリッジモード

ユニバーサルワークグループブリッジの役割を設定する場合は、クライアントのMACアドレスを含める必要があります。ワークグループブリッジがこのMACアドレスにアソシエートされるのは、MACアドレスがブリッジテーブルに存在し、静的エントリでない場合に限られます。検証に失敗した場合、ワークグループブリッジはそのBVIのMACアドレスを使用してアソシエートします。ユニバーサルワークグループブリッジモードでは、ワークグループブリッジはイーサネットクライアントのMACアドレスを使用してシスコまたはシスコ以外のルートデバイスとアソシエートします。ユニバーサルワークグループブリッジは透過的で、管理されません。



(注)

ユニバーサルワークグループブリッジの役割では、1つの有線クライアントだけがサポートされます。

イーサネットクライアントを無効にし、ユニバーサルワークグループブリッジが独自のBVIアドレスを使用してアクセスポイントにアソシエートするようにすることによって、復元メカニズムを有効化し、ワークグループブリッジを再び管理可能にできます。

「国境をまたいで運航する航空路線」のシナリオをサポートするために、`world-mode` コマンドに `roaming` キーワードが追加されました。このキーワードにより、ワークグループブリッジはルートアクセスポイントから認証が取り消されると、パッシブスキャンを実行します。このコマンドの詳細については、「ワールドモードのイネーブル化とディセーブル化」(P.6-26)を参照してください。

## 802.11n プラットフォームのポイントツーポイントおよびマルチポイントブリッジングのサポート

ポイントツーポイントおよびポイントツーマルチポイントブリッジングは、Cisco Aironet 1040、1140、1250 シリーズ アクセスポイント (802.11n プラットフォーム) でサポートされています。5 GHz 帯域は 20 MHz および 40 MHz をサポートし、2.4 GHz 帯域は 20 MHz をサポートします。

AP1040、AP1140、AP1250、および AP1260 ブリッジングでは、次の項目がサポートされます。

- MIMO、ショートレンジブリッジング (キャンパスまたはビルディング間での導入)、1 Km 未満の範囲内でダイポールおよび MIMO アンテナ (ラインオブサイトおよびショートレンジ) を使用

- 20 MHz および 40 MHz の 802.11n サポート
- ワークグループブリッジ (WGB) ショートレンジのサポート
- SISO (Single-In, Single-Out)、1本の屋外アンテナを使用した MCS 0-7 およびレガシーブリッジレート (802.11 a/b/g および 802.11n)



(注) 前述のサポートはショートレンジリンクでのみサポートされ、AP-1240/1300/1400 などのブリッジ製品の置き換えにはなりません。

ブリッジモードの AP1040、AP1140、AP1250 および AP1260 では、次の項目はサポートされていません。

- **distance** コマンド。**distance** コマンドは、屋外での使用が認可されているアクセスポイントでのみサポートされます。
- 外部アンテナを使用する外部 MIMO ブリッジング。

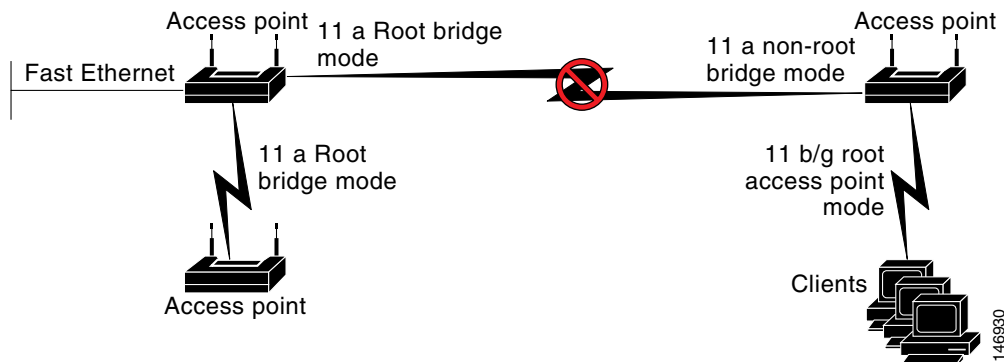


(注) ポイントツーマルチポイントブリッジングでは、ルートブリッジによる WGB は推奨されません。ポイントツーマルチポイントブリッジング設定では、WGB はルート AP に関連付ける必要があります。

## デュアル無線フォールバックの設定

デュアル無線フォールバック機能を使用すると、アクセスポイントをネットワークインフラストラクチャに接続する非ルートブリッジリンクがダウンしたとき、クライアントがアクセスポイントに接続する際に使用するルートアクセスポイントリンクがシャットダウンするようにアクセスポイントを設定できます。ルートアクセスポイントリンクをシャットダウンすると、クライアントは別のアクセスポイントにローミングを切り替えます。この機能がない場合、クライアントはアクセスポイントに接続されたままになりますが、ネットワークとデータを送受信できません。

図 6-1 デュアル無線フォールバック



(注) この機能は、AP1130、AP1140、AP1230、AP1240、および AP1250 などのデュアル無線アクセスポイントでサポートされます。



(注) この機能はシングル無線アクセスポイントのフォールバック機能に影響しません。

デュアル無線フォールバックは、次の3つの方法で設定できます。

- 無線トラッキング
- ファスト イーサネット トラッキング
- MAC アドレス トラッキング

## 無線トラッキング

アクセス ポイントのいずれかの無線の状態を追跡またはモニタするようにアクセス ポイントを設定できます。追跡対象の無線がダウンするか無効になると、アクセス ポイントは別の無線をシャットダウンします。追跡対象の無線が起動すると、アクセス ポイントは別の無線をイネーブルにします。

- Radio 0 を追跡するには、次のコマンドを入力します。  

```
# station-role root access-point fallback track d0 shutdown
```
- Radio 1 を追跡するには、次のコマンドを入力します。  

```
# station-role root access-point fallback track d1 shutdown
```



(注) このコマンドは 802.11n シリーズ アクセス ポイント (AP1260 など) ではサポートされていません。無線 インターフェイス コンフィギュレーション モードで次のコマンドを使用する必要があります。

```
# station-role root access-point fallback shutdown
```

## ファスト イーサネット トラッキング

アクセス ポイントのイーサネット ポートがディセーブルになったり、または有線 LAN から切断されたりしたときにフォールバックするようにアクセス ポイントを設定できます。アクセス ポイントをファスト イーサネット トラッキング用に設定するには、「[無線ネットワークの役割の設定](#)」(P.6-2) で説明するようにして行います。



(注) ファスト イーサネット トラッキングは、リピータ モードをサポートしません。

- ファスト イーサネット トラッキングに対して 802.11n 以外のアクセス ポイントを設定するには、無線 インターフェイス コンフィギュレーション モードで次のコマンドを入力します。  

```
# station-role root access-point fallback track fa 0
```
- ギガビット イーサネット トラッキングに対して 802.11n アクセス ポイント (AP1040、AP1140、AP1250、および AP1260) を設定するには、無線 インターフェイス コンフィギュレーション モードで次のコマンドを入力します。  

```
# station-role root fallback shutdown
```

## MAC アドレス トラッキング

クライアント アクセス ポイントをその MAC アドレスを使用して別の無線でトラッキングすることによって、ルート アクセス ポイントの役割を持つ無線を起動またはダウンするように設定できます。クライアント アクセス ポイントからのアソシエーションが解除されると、ルート アクセス ポイントの無線はダウンします。クライアントがアクセス ポイントと再アソシエートすると、ルート アクセス ポイント無線は起動状態に戻ります。

クライアントがアップストリームの有線ネットワークに接続されている非ルート ブリッジ アクセス ポイントの場合、MAC アドレス トラッキングが最も便利です。

たとえば、MAC アドレスが 12:12:12:12:12:12 のクライアントを追跡するには、次のコマンドを入力します。

```
# station-role root access-point fallback track mac-address 12:12:12:12:12:12 shutdown
```

## サポートされないブリッジ機能

1200 または 1240 シリーズ アクセス ポイントがブリッジとして設定される場合、次の機能はサポートされません。

- Clear Channel Assessment (CCA; クリア チャネル アセスメント)
- 1400 シリーズブリッジとの相互運用
- 連結
- インストール モード
- スイッチの EtherChannel および PageP 構成

## 無線データレートの設定

データレート設定を使用して、ワイヤレス デバイスのデータ転送に使用されるデータレートを選択します。レートの単位は Megabits per second (Mbps; メガビット/秒) です。ワイヤレス デバイスは常に **Basic** に設定された最大データレートで転送しようとします。なお、ブラウザベースのインターフェイスでは、**Basic** は **Require** と呼ばれます。障害や干渉などがある場合、ワイヤレス デバイスはデータ送信が可能な範囲での最速レートまで減速されます。各データレートは、次の 3 つのステートのいずれかに設定できます。

- **Basic** (GUI では Basic レートを [Required] と表示) : ユニキャストとマルチキャストの両方で、すべてのパケットをこのレートで転送します。ワイヤレス デバイスのデータレートの少なくとも 1 つは **Basic** に設定してください。
- **Enabled** : ワイヤレス デバイスでは、ユニキャスト パケットだけがこのレートで送信され、マルチキャスト パケットは、**Basic** に設定されているいずれかのデータレートで送信されます。
- **Disabled** : ワイヤレス デバイスでは、データはこのレートで送信されません。



(注) 少なくともデータレートの 1 つは **basic** に設定してください。

Data Rate の設定を使用すると、特定のレートでデータを転送するクライアント デバイスに対応するようにアクセス ポイントを設定できます。たとえば、11Mbps だけで転送を行う 2.4GHz 無線を設定する場合、11Mbps レートを **Basic** に設定し、他のデータレートを **Disabled** に設定

します。ワイヤレス デバイスを、1Mbps および 2Mbps でデータを転送するクライアント デバイスだけに対応するように設定するには、1Mbps および 2Mbps に対して **Basic** を選択し、その他のデータレートは **Disabled** に設定します。2.4GHz、802.11g 無線を、802.11g クライアント デバイスだけに対応するように設定するには、Orthogonal Frequency Division Multiplexing (OFDM; 直交周波数分割多重方式) データレート (6、9、12、18、24、36、48、54) を、すべて **Basic** に設定します。54Mbps だけで転送を行う 5GHz 無線を設定するには、54Mbps レートを **Basic** に設定し、他のデータレートを **Disabled** に設定します。

また、範囲またはスループットが最適になるようなデータレートが自動的に設定されるように、ワイヤレス デバイスを設定することも可能です。データレート設定に **range** を入力した場合、ワイヤレス デバイスでは 1Mbps レートは **Basic** に、他のレートは **Enabled** に設定されます。この **range** 設定によって、アクセスポイントではデータレートについて妥協することでカバレッジ領域を拡大できます。したがって、他のクライアントがアクセスポイントに接続できるときに接続できないクライアントがいる場合、そのクライアントがアクセスポイントのカバレッジ領域にいないことが理由の1つである場合があります。そのような場合に **range** オプションを使用すると、カバレッジ領域を拡大するために役立ち、クライアントはアクセスポイントに接続できる場合があります。通常、スループットと範囲が交換条件となります。(おそらくアクセスポイントからの距離が原因で) 信号が劣化すると、リンクを維持するために(データレートを下げて) レートが再ネゴシエートされます。これと対照をなすのはスループットを高く設定したリンクで、設定された高いデータレートを維持できなくなるほど信号が劣化すると、スループットが低下します。または、十分な適用範囲を持つ他のアクセスポイントが利用できる場合、そのアクセスポイントにローミングが切り替わります。両者のバランス(スループットと範囲)は、決定する必要がある設計上の判断の1つです。判断を下す際、無線プロジェクトに利用できるリソース、ユーザが渡すトラフィックのタイプ、必要なサービスレベル、そして常に RF 環境の品質が根拠となります。データレート設定に **throughput** を入力すると、ワイヤレス デバイスでは 4 つすべてのデータレートを **basic** に設定します。



(注)

802.11b クライアントと 802.11g クライアントが混在する環境の無線ネットワークの場合、1、2、5.5、および 11Mbps のデータレートが必須 (**basic**) に設定され、他のすべてのデータレートが **enable** に設定されていることを確認します。802.11b アダプタは 54Mbps のデータレートを認識せず、接続先のアクセスポイントで 11Mbps よりも高いデータレートが必要だと設定されている場合は動作しません。

## マルチキャスト フレームと管理フレームを最高の Basic レートで送信するアクセスポイント

最近のバージョンの Cisco IOS を実行するアクセスポイントは、設定された最高の Basic レートでマルチキャスト フレームと管理フレームを送受信し、この状況で信頼性の問題が発生することがあります。

LWAPP または自律 IOS を実行するアクセスポイントは、設定された最低の Basic レートでマルチキャスト フレームと管理フレームを送受信します。これはセルの端に十分なカバレッジを提供するために必要で、マルチキャスト無線送信を受信できないことがある受信応答しないマルチキャスト転送では特に必要です。

マルチキャスト フレームは MAC レイヤで再送信されないため、セルの端のステーションはマルチキャスト フレームを正常に受信できない場合があります。信頼性の高い受信が目的の場合、マルチキャストは低いデータレートで送信する必要があります。高いデータレートのマルチキャストをサポートする必要がある場合、セルサイズを縮小して低いデータレートをすべて無効にすることが役立つ場合があります。

特定の要件に応じて、次の処置が可能です。

- 信頼性を最大限に高めてマルチキャスト データを送信する必要があって、マルチキャストの帯域幅は大きくする必要がない場合、単一の Basic レートを設定し、無線セルの端に到達するために十分な低さにします。
- 特定のスループットを達成するために特定のデータ レートでマルチキャスト データを送信する必要がある場合、そのレートを最高の Basic レートとして設定します。また、マルチキャスト以外のクライアントのカバレッジのために、低い Basic レートを設定することも可能です。

特権 EXEC モードから、次の手順に従って無線データ レートを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4 GHz 無線および 2.4 GHz N 無線は Radio 0、5 GHz 無線および 5 GHz N 無線は Radio 1 です。
ステップ 3	<p><code>speed</code></p> <p>802.11b、2.4GHz 無線の場合：  <code>{[1.0] [11.0] [2.0] [5.5] [basic-1.0] [basic-11.0] [basic-2.0] [basic-5.5]   range   throughput}</code></p> <p>802.11g、2.4GHz 無線の場合：  <code>{[1.0] [2.0] [5.5] [6.0] [9.0] [11.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [basic-1.0] [basic-2.0] [basic-5.5] [basic-6.0] [basic-9.0] [basic-11.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0]   range   throughput [ofdm]   default }</code></p> <p>802.11a 5GHz 無線の場合：  <code>{[6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [basic-6.0] [basic-9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0]   range   throughput   default }</code></p>	<p>各データ レートを <b>Basic</b> または <b>Enabled</b> に設定するか、<b>range</b> を入力して範囲を最適化するか、あるいは <b>throughput</b> を入力してスループットを最適化します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>1.0</b>、<b>2.0</b>、<b>5.5</b>、および <b>11.0</b> を入力すると、802.11b、2.4GHz 無線でこれらのデータ レートが <b>enabled</b> に設定されます。</li> <li>• <b>1.0</b>、<b>2.0</b>、<b>5.5</b>、<b>6.0</b>、<b>9.0</b>、<b>11.0</b>、<b>12.0</b>、<b>18.0</b>、<b>24.0</b>、<b>36.0</b>、<b>48.0</b>、および <b>54.0</b> を入力すると、802.11g、2.4GHz 無線でこれらのデータ レートが <b>enabled</b> に設定されます。</li> <li>• <b>6.0</b>、<b>9.0</b>、<b>12.0</b>、<b>18.0</b>、<b>24.0</b>、<b>36.0</b>、<b>48.0</b>、および <b>54.0</b> を入力すると、5GHz 無線でこれらのデータ レートが <b>enabled</b> に設定されます。</li> <li>• (任意) <b>basic-1.0</b>、<b>basic-2.0</b>、<b>basic-5.5</b>、および <b>basic-11.0</b> を入力すると、802.11b、2.4GHz 無線でこれらのデータ レートが <b>basic</b> に設定されます。</li> <li>• <b>basic-1.0</b>、<b>basic-2.0</b>、<b>basic-5.5</b>、<b>basic-6.0</b>、<b>basic-9.0</b>、<b>basic-11.0</b>、<b>basic-12.0</b>、<b>basic-18.0</b>、<b>basic-24.0</b>、<b>basic-36.0</b>、<b>basic-48.0</b>、および <b>basic-54.0</b> を入力すると、802.11g、2.4GHz 無線でこれらのデータ レートが <b>basic</b> に設定されます。</li> </ul> <p>(注) 選択した Basic レートをクライアントがサポートしている必要があります。そうでないと、クライアントはそのワイヤレス デバイスにアソシエートできません。802.11g 無線の Basic データ レートに 12 Mbps 以上を選択した場合、802.11b クライアント デバイスは、ワイヤレス デバイスの 802.11g 無線にアソシエートできません。</p> <p><b>basic-6.0</b>、<b>basic-9.0</b>、<b>basic-12.0</b>、<b>basic-18.0</b>、<b>basic-24.0</b>、<b>basic-36.0</b>、<b>basic-48.0</b>、および <b>basic-54.0</b> を入力すると、5 GHz 無線でこれらのデータ レートが <b>basic</b> に設定されます。</p>

コマンド	目的	
<p><b>speed</b> (続き)</p> <p>802.11n 2.4GHz 無線の場合 :</p> <pre>{[1.0] [11.0] [12.0] [18.0] [2.0] [24.0] [36.0] [48.0] [5.5] [54.0] [6.0] [9.0] [basic-1.0] [basic-11.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-5.5] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.] [ofdm] [only-ofdm]   range   throughput}</pre> <p>802.11n 5GHz 無線の場合 :</p> <pre>{[12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [6.0] [9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] [basic-6.0] [basic-9.0] [default] [m0-7] [m0.] [m1.] [m10.] [m11.] [m12.] [m13.] [m14.] [m15.] [m2.] [m3.] [m4.] [m5.] [m6.] [m7.] [m8-15] [m8.] [m9.]   range   throughput}</pre>	<ul style="list-style-type: none"> <li>(任意) <b>range</b> または <b>throughput</b> を入力すると、無線範囲またはスループットが自動的に最適化されます。<b>range</b> を入力すると、ワイヤレス デバイスは最も低いデータレートを Basic に設定し、他のレートを <b>Enabled</b> に設定します。<b>throughput</b> を入力すると、ワイヤレス デバイスはすべてのデータレートを <b>basic</b> に設定します。</li> </ul> <p>(任意) 802.11g 無線で、すべての OFDM レート (6、9、12、18、24、36、および 48) を Basic (Required) に設定し、すべての Complementary Code Keying (CCK; 相補コードキー入力) レート (1、2、5.5、および 11) を Disabled に設定するには、<b>speed throughput ofdm</b> を入力します。この設定により、802.11b 保護機能がディセーブルとなり、802.11g クライアントに最大のスループットが提供されます。ただし、802.11b クライアントはそのアクセス ポイントにアソシエートできなくなります。</p> <ul style="list-style-type: none"> <li>(任意) <b>default</b> を入力すると、データレートは工場出荷時の設定になります (802.11b 無線ではサポートされていません)。</li> </ul> <p>802.11g 無線では、<b>default</b> オプションによって、レート 1、2、5.5、および 11 は Basic に、レート 6、9、12、18、24、36、48、および 54 は Enabled に設定されます。これらのレート設定を使用すると、802.11b および 802.11g の両方のクライアント デバイスをワイヤレス デバイス 802.11g 無線に関連付けできるようになります。</p> <p>5GHz 無線では、<b>default</b> オプションによって、レート 6.0、12.0、および 24.0 は Basic に、レート 9.0、18.0、36.0、48.0、および 54.0 は Enabled に設定されます。</p> <p>802.11n 2.4GHz 無線では、<b>default</b> オプションによって、レート 1.0、2.0、5.5、および 11.0 が Enabled に設定されます。</p> <p>802.11n 5GHz 無線では、<b>default</b> オプションによって、6.0、12.0、および 24.0 が Enabled に設定されます。</p> <p>802.11n 無線のデフォルト MCS レート設定は 0 ~ 15 です。</p>	
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定から 1 つ以上のデータレートを削除する場合は、**speed** コマンドの **no** 形式を使用します。次の例は、設定からデータレート basic-2.0 と basic-5.5 を削除する方法を示しています。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5
ap1200(config-if)# end
```

## MCS レートの設定

Modulation Coding Scheme (MCS; 変調および符号化方式) は、変調順序 (BPSK、QPSK、16-QAM、64-QAM) および FEC コード レート (1/2、2/3、3/4、5/6) で構成される PHY パラメータの仕様です。MCS は 1140 および 1250 シリーズの 802.11n 無線で使用され、次のような 32 の対称設定 (空間ストリームごとに 8 つ) が定義されます。

- MCS 0 ~ 7
- MCS 8 ~ 15
- MCS 16 ~ 23
- MCS 24 ~ 31

1140 および 1250 シリーズ アクセス ポイントは MCS 0 ~ 15 をサポートします。スループットが高いクライアントは、少なくとも MCS 0 ~ 7 をサポートします。

MCS は高いスループットを実現する可能性があるため、重要な設定です。高いスループットのデータレートは、MCS、帯域幅、およびガード間隔の関数です。802.11 a、b、および g 無線は 20MHz のチャンネル幅を使用します。表 6-2 は、MCS、ガード間隔、およびチャンネル幅に基づく可能なデータレートを示したものです。



(注) 2.5 GHz 無線は、40 MHz チャンネル幅をサポートしていません。

表 6-2 MCS 設定、ガード インターバル、およびチャンネル幅に基づくデータレート

MCS インデックス	ガード間隔 = 800ns		ガード間隔 = 400ns	
	20MHz のチャンネル幅のデータレート (Mbps)	40MHz のチャンネル幅のデータレート (Mbps)	20MHz のチャンネル幅のデータレート (Mbps)	40MHz のチャンネル幅のデータレート (Mbps)
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270



表 6-2 MCS 設定、ガード インターバル、およびチャネル幅に基づくデータ レート (続き)

MCS インデックス	ガード間隔 = 800ns		ガード間隔 = 400ns	
	20MHz のチャネル幅のデータ レート (Mbps)	40MHz のチャネル幅のデータ レート (Mbps)	20MHz のチャネル幅のデータ レート (Mbps)	40MHz のチャネル幅のデータ レート (Mbps)
15	130	270	144 4/9	300

レガシー レートは次のとおりです。

5GHz : 6、9、12、18、24、36、48、および 54Mbps

2.4GHz : 1、2、5.5、6、9、11、12、18、24、36、48、および 54Mbps

MCS レートは **speed** コマンドを使用して設定します。次の例は、802.11n 5GHz 無線の **speed** 設定を示しています。

```
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  ssid 1250test
  !
  speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
  m0.m1.m2.m3.m4.m8.m9.m10.m11.m12.m13.m14.m15.
```

## 無線の送信電力の設定

無線の送信電力は、使用するアクセス ポイントに導入されている 1 つ以上の無線のタイプと、アクセス ポイントが動作する規制ドメインに基づきます。アクセス ポイントで使用できる伝送電力と、アクセス ポイントが動作する規制地域について調べるには、デバイスのハードウェア インストレーション ガイドを参照してください。ハードウェア インストレーション ガイドは [cisco.com](http://cisco.com) から入手できます。表示およびダウンロードする手順は、次のとおりです。

- ステップ 1 <http://www.cisco.com> を表示します。
- ステップ 2 [Technical Support & Documentation] をクリックします。テクニカルサポート リンクのリストを含む小さいウィンドウが表示されます。
- ステップ 3 [Technical Support & Documentation] をクリックします。[Technical Support and Documentation] ページが表示されます。
- ステップ 4 [Documentation & Tools] セクションで、[Wireless] を選択します。[Wireless Support Resources] ページが表示されます。
- ステップ 5 [Wireless LAN Access] セクションで、操作するデバイスを選択します。デバイスの概要ページが表示されます。
- ステップ 6 [Install and Upgrade] セクションで、[Install and Upgrade Guides] を選択します。デバイスの [Install and Upgrade Guides] ページが表示されます。
- ステップ 7 デバイスのハードウェア インストレーション ガイドを選択します。ガイドのホームページが表示されます。
- ステップ 8 左のフレームで、[Channels and Antenna Settings] をクリックします。

表 6-3 は、mW と dBm の関係を示しています。

表 6-3 mW と dBm との変換

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

特権 EXEC モードから、次の手順に従ってアクセス ポイントの無線の伝送電力を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。  2.4GHz 802.11n 無線は 0、5GHz 802.11n 無線は 1 です。
ステップ 3	<code>power local</code>  次のオプションは、802.11b、2.4-GHz 無線について使用できません (単位 mW)。 <code>{ 1   5   20   30   50   100   maximum }</code>  次のオプションは、5GHz 無線について使用できません (単位 mW)。 <code>{ 5   10   20   40   maximum }</code>  次のオプションは、802.11a、5GHz 無線について使用できません (単位 dBm)。 <code>{ -1   2   5   8   11   14   15   17   maximum }</code>  次のオプションは、AIR-RM21A 5GHz 無線について使用できません (単位 dBm)。 <code>{ -1   2   5   8   11   14   16   17   20   maximum }</code>  次のオプションは、2.4GHz 802.11n 無線について使用できません (単位 dBm)。 <code>{ -1   2   5   8   11   14   17   20   23   maximum }</code>  次のオプションは、5GHz 802.11n 無線について使用できません (単位 dBm)。 <code>{ -1   2   5   8   11   14   17   20   maximum }</code>	802.11b、2.4GHz 無線または 5GHz 無線の伝送電力を、現在の規制地域で許可される電力レベルのいずれかに設定します。  (注) 規制ドメインの電力設定について調べるには、アクセス ポイントのハードウェア設置ガイドを参照してください。

	コマンド	目的
ステップ 4	<p><b>power local</b></p> <p>次のオプションは、802.11g、2.4GHz 無線について使用できます。</p> <p><b>power local cck</b> 設定： { -1   2   5   8   11   14   17   20   <b>maximum</b> }</p> <p><b>power local ofdm</b> 設定： { -1   2   5   8   11   14   17   <b>maximum</b> }</p>	<p>802.11g、2.4GHz 無線の伝送電力を、現在の規制地域で許可される電力レベルのいずれかに設定します。設定は dBm 単位です。</p> <p>2.4GHz の 802.11g 無線では、直交周波数分割多重方式 (OFDM) と Complementary Code Keying (CCK; 相補コードキー入力) のいずれかの電力レベルを設定できます。CCK 変調は、802.11b デバイスおよび 802.11g デバイスによってサポートされています。OFDM 変調は、802.11g デバイスおよび 802.11a デバイスによってサポートされています。</p> <p>(注) 規制地域の電力設定について調べるには、アクセスポイントのハードウェア インストレーションガイドを参照してください。</p> <p>(注) 802.11g の無線では、データレートが 1Mbps、2Mbps、5.5Mbps、および 11Mbps の場合、最大 100mW でデータが送信されます。ただし、6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、および 54Mbps のデータレートの場合、802.11g 無線の最大送信電力は 30mW です。</p>
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

電力設定をデフォルトの **maximum** に戻すには、**power** コマンドの **no** 形式を使用します。

## アソシエートしたクライアント デバイスの電力レベルの制限

ワイヤレス デバイスにアソシエートしたクライアント デバイスの電力レベルを制限することもできます。クライアント デバイスがワイヤレス デバイスにアソシエートするとき、ワイヤレス デバイスはクライアントに最大電力レベル設定を送信します。



(注) Cisco AVVID のマニュアルでは、アソシエートされたクライアント デバイスの電力レベルの制限を示すのに Dynamic Transmit Power Control (DTPC; 送信電力の動的制御) という用語を用います。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスにアソシエートするすべてのクライアント デバイスに、最大許可電力設定を指定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface dot11radio {0   1}</b>	無線 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。  2.4GHz 802.11n 無線は 0、5GHz 802.11n 無線は 1 です。
ステップ 3	<b>power client</b>  次のオプションは、802.11b、2.4GHz クライアントについて使用できます (単位 mW)。 <b>{local   1   5   20   30   50   100   maximum}</b>  次のオプションは、802.11g、2.4GHz クライアントについて使用できます (単位 mW)。 <b>{local   1   5   10   20   30   50   100   maximum}</b>  次のオプションは、5GHz クライアントについて使用できます (単位 mW)。 <b>{local   5   10   20   40   maximum }</b>  AIR-RM21A 5GHz 無線モジュールを持つアクセス ポイントでは、5GHz クライアントについて次の電力オプションを使用できます (単位 dBm)。 <b>{local   -1   2   5   8   11   14   16   17   20   maximum }</b>  次のオプションは、802.11n、2.4GHz クライアントについて使用できます (単位 dBm)。 <b>{local   -1   2   5   8   11   14   17   20   maximum }</b>  次のオプションは、802.11n、5GHz クライアントについて使用できます (単位 dBm)。 <b>{local   2   5   8   11   14   17   maximum }</b>	ワイヤレス デバイスにアソシエートするクライアント デバイスに、最大許可電力レベルを設定します。  電力レベルを <b>local</b> に設定すると、クライアントの電力レベルはアクセス ポイントの電力レベルに設定されます。  電力レベルを <b>maximum</b> に設定すると、クライアントの電力は最大許可電力に設定されます。  (注) 規制ドメインで許容される設定は、ここで取り上げる設定と異なる場合があります。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

アソシエートしたクライアントの最大電力レベルを無効にするには、`client power` コマンドの `no` 形式を使用します。



(注)

アソシエートしたクライアント デバイスの電力レベルを制限する場合は、Aironet 拡張機能をイネーブルにする必要があります。Aironet 拡張機能はデフォルトではイネーブルに設定されています。

## 無線チャネルの設定

ワイヤレス デバイスの無線のデフォルト チャネル設定は `Least Congested` です。起動時にワイヤレス デバイスは最も混雑の少ないチャネルをスキャンして選択します。ただし、サイト調査の後も一貫したパフォーマンスが維持されるように、各アクセス ポイントにスタティック チャネル設定を指定することを推奨します。ワイヤレス デバイスのチャネル設定は、規制ドメインで使用できる周波数に対応します。ドメインで許可されている周波数については、アクセス ポイントのハードウェア インストールガイドを参照してください。



(注)

RF 干渉が原因でクライアントが無線からときどき切断されている場所では、チャネル 1 (2412) などの別のチャネルで動作するように無線インターフェイスを設定すると干渉を回避できる場合があります。



(注)

Cisco Aironet CB20A クライアント無線では、AIR-RM21A 無線モジュールにアソシエートできないことがあります。これは、AIR-RM21A 無線モジュールでサポートされているチャネルの中には、CB20A クライアントでサポートされていないものがあるためです。AIR-RM21A 無線モジュールのデフォルトのチャネル設定である `Least Congested` では、アクセス ポイントで使用する周波数が、CB20A クライアント無線でサポートされていない次の周波数のいずれかに設定されることが頻繁に発生します。これらの周波数は、チャネル 149 (5745GHz)、チャネル 153 (5765GHz)、チャネル 157 (5785GHz)、およびチャネル 161 (5805GHz) です。この問題を避けるには、AIR-RM21A 無線モジュールのチャネルを、CB20A クライアントでサポートされているチャネルに設定します。

2.4GHz 帯チャネル利用帯域幅は、チャネルあたり 22MHz になります。チャネル 1、6、11 の帯域幅は重複していないため、干渉を起こさずに、同じ圏内に複数のアクセス ポイントを設定できます。802.11b および 802.11g の 2.4GHz 無線はいずれも同じチャネルと周波数を使用します。

5GHz 無線は、5180 ~ 5320MHz の 8 チャネルで稼働します。各チャネルは 20MHz に対応し、チャネルの帯域幅は少しずつ重複しています。最適なパフォーマンスを得るため、互いに近い位置にある無線の場合は、隣接していないチャネル (たとえば、44 と 46) を使用します。



(注)

同じ圏内に多くのアクセス ポイントを設定しすぎると、無線の輻輳が発生し、スループットが減少します。無線のサービス範囲とスループットを最大にするには、慎重なサイト調査を行って、アクセス ポイントの最適な設置場所を決定する必要があります。

チャネル設定は頻繁に変更されるため、このマニュアルには記載されていません。ご使用のアクセスポイントまたはブリッジのチャネル設定についての最新情報は、『*Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges*』を参照してください。このマニュアルは [cisco.com](http://cisco.com/en/US/products/ps6521/tsd_products_support_install_and_upgrade.html) の次の URL から入手できます。

[http://cisco.com/en/US/products/ps6521/tsd\\_products\\_support\\_install\\_and\\_upgrade.html](http://cisco.com/en/US/products/ps6521/tsd_products_support_install_and_upgrade.html)

## 802.11n のチャネル幅

802.11n では、20 MHz および 40 MHz の両方のチャネル幅が使用可能です。後者のチャネル幅は、2つの連続する重複しないチャネル（たとえば、2.4 GHz のチャネル 1 およびチャネル 6）で構成されます。802.11n 無線は、同じ帯域で動作します。ただし、チャネル幅は個別に設定できます。

20MHz チャネルの 1 つはコントロールチャネルと呼ばれます。レガシークライアントおよび 20MHz の高いスループットのクライアントはコントロールチャネルを使用します。ビーコンを送信できるのはこのチャネルだけです。2 番目の 20MHz チャネルは拡張チャネルと呼ばれます。40MHz のステーションは、このチャネルとコントロールチャネルを同時に使用できます。

40MHz チャネルは、1,1 のようにチャネルおよび拡張として指定されます。この例で、コントロールチャネルはチャネル 1、拡張チャネルはその上のチャネルです。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスのチャネル幅を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4 GHz 無線および 802.11n 2.4 GHz 無線は Radio 0 です。 5GHz 無線および 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	<code>channel {frequency   least-congested   width [20   40-above   40-below]   dfs}</code>	ワイヤレス デバイス無線のデフォルト チャネルを設定します。起動時に最も混雑の少ないチャネルを探すには、 <b>least-congested</b> を入力します。  使用する帯域幅を指定するには <b>width</b> オプションを使用します。このオプションは 1140 および 1250 シリズ アクセスポイントで使用でき、20、40-above、および 40-below の 3 つの使用可能な設定で構成されています。20 を選択すると、チャネル幅が 20 MHz に設定されます。40-above を選択すると、拡張チャネルをコントロールチャネルの上に重ねた状態でチャネル幅が 40 MHz に設定されます。40-below を選択すると、拡張チャネルをコントロールチャネルの下に重ねた状態でチャネル幅が 40 MHz に設定されます。  (注) 動的周波数選択 (DFS) に関する欧州連合の規制に準拠する 5 GHz の無線については、 <b>channel</b> コマンドはディセーブルに設定されています。詳細については、「802.11n ガード間隔の設定」(P.6-23) を参照してください。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## Dynamic Frequency Selection (動的周波数選択)

工場出荷時に 5GHz 無線が設定されている、米国、ヨーロッパ、シンガポール、韓国、日本、イスラエル、および台湾向けのアクセス ポイントは、無線デバイスがレーダー信号を検出して干渉しないようにする動的周波数選択 (DFS) の使用を必須とする規制に従うようになりました。アクセス ポイントが特定のチャネルでレーダーを検出すると、そのチャネルを 30 分間使用しないようにします。その他の規制地域向けに設定する無線では、DFS を使用しません。

DFS を有効に設定した 5GHz 帯無線を [表 6-4](#) に記載した 15 チャネルのいずれかで動作させると、アクセス ポイントが自動的に DFS を使用して動作周波数を設定します。DFS が有効に設定されると、アクセス ポイントが自身の動作周波数にレーダー信号がないかモニタするようになります。同じチャネルにレーダー信号を検出した場合は、アクセス ポイントが次の処理を実行します。

- チャネル上でそれ以降の伝送をブロックします。
- 省電力モードのクライアントからのキューを消去します。
- 802.11h チャネル切り替えアナウンスメントをブロードキャストします。
- 残りのクライアント デバイスのアソシエーションを解除します。
- Wireless Domain Service (WDS; 無線ドメイン サービス) に参加している場合、周波数を終了する DFS 通知をアクティブな WDS デバイスに送信します。
- 別の 5GHz チャネルを無作為に選択します。
- 選択したチャネルが [表 6-4](#) のいずれかのチャネルだった場合は、そのチャネルにレーダー信号がないか 60 秒間スキャンします。
- そのチャネルにレーダー信号がなければ、ビーコンを有効にしてクライアントのアソシエーションを受け入れます。
- WDS に参加している場合、アクティブな WDS デバイスに新しい動作周波数を知らせる DFS 通知を送信します。



(注)

規制要件に従い、一部の地域では、DFS を有効に設定した 5 GHz 帯無線のチャネルを手動で選択できません。この場合、アクセス ポイントが無作為にチャネルを選択します。

DFS が必要なチャネルのすべてのリストを、[表 6-4](#) に示します。

**表 6-4 DFS チャネル リスト**

チャネル	Frequency	チャネル	Frequency	チャネル	Frequency
52	5260MHz	104	5500MHz	124	5620MHz
56	5280MHz	108	5520MHz	128	5640MHz
60	5300MHz	112	5560MHz	132	5660MHz
64	5320MHz	116	5580MHz	136	5680MHz
100	5500MHz	120	5600MHz	140	5700MHz

自律動作を行うために、DFS では [表 6-4](#) にリストされているチャネルから無作為にチャネルを選択することが必要です。[表 6-4](#) にリストされていないチャネルは無作為な選択が不要で、手動で設定できます。

動的周波数選択 (DFS) が必要なチャネルは、-E または -M 規制ドメインを使用する 1040、1130、1140、1230、1240、1250、1260、および 1520、あるいは -A、-E、または -M 規制ドメインを使用する 1430 に対して手動で選択できます。また、手動で非 DFS チャネルを設定する場合と同じ GUI/CLI を使用して、DFS チャネルを選択することもできます。デフォルトのチャネル選択は「DFS」であり、無作為にチャネルが選択されます。

手動で設定された DFS チャネルでレーダーが検出された場合、そのチャネルは自動的に変更され、設定したチャネルには戻りません。

表 6-4 にリストされているチャネルで送信する前に、アクセス ポイント無線は Channel Availability Check (CAC) を実行します。CAC はチャネルに無線信号が存在するかを調べる 60 秒のスキャンです。次のメッセージ例は、CAC スキャンの開始と終了を示すもので、アクセス ポイントのコンソールに表示されます。

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5500 MHz for 60 seconds
```

```
*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan complete on frequency 5500 MHz
```

表 6-4 に記載されている DFS チャネルを稼働すると、アクセス ポイントでは、CAC の実行に加え、チャネル上にレーダーがないかどうかを常に監視します。レーダーが検出されると、アクセス ポイントはデータ パケットの転送を 200 ミリ秒間停止し、802.11h チャネル切り替えの通知を含む 5 つのビーコンを同報通信し、アクセス ポイントが使用を開始するチャネル番号を指示します。次のメッセージ例は、レーダーが検出されたときにアクセス ポイント コンソールに表示されます。

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5500 MHz
```

チャネルにレーダーが検出されると、そのチャネルは 30 分間使用できません。アクセス ポイントは、過去 30 分のうちにチャネルにレーダーを検出した各チャネルのフラグを不揮発性ストレージに維持します。30 分が過ぎると、対応するチャネルのフラグがクリアされます。フラグがクリアされる前にアクセス ポイントがリブートすると、チャネルの初期化中に非占有時間が 30 分にリセットされます。



(注) 適法な最大送信電力については、他のチャネルよりも 5GHz チャネルの方が大きくなるものがあります。無作為に選択した 5GHz チャネルが電力を制限されていた場合、アクセス ポイントはそのチャネルの電力上限に合うように自動的に送信電力を下げます。



(注) DFS が有効に設定された無線で国番号を設定するには、**world-mode dot11d country-code** 設定インターフェイス コマンドを使用することを推奨します。IEEE 802.11h プロトコルでは、アクセス ポイントはビーコンとプローブ応答に国情報エレメント (IE) を含める必要があります。ただしデフォルトでは、IE の国番号は空白に設定されています。**world-mode** コマンドで、国番号 IE を入力してください。

## DFS チャネルでのレーダー検出

DFS チャネルでアクセス ポイントがレーダーを検出すると、そのアクセス ポイントはフラッシュ メモリ内にファイルを作成します。このファイルは 802.11a 無線のシリアル番号に基づいたもので、レーダーが検出されたチャネルの番号が記録されています。これは正常な動作です。このファイルは削除しないでください。



## CLI コマンド

次の項では、DFS に適用される CLI コマンドを説明します。

### DFS が有効に設定されているかどうかの確認

DFS が有効に設定されているかどうかを確認するには、**show controllers dot11radio1** コマンドを使用します。コマンドには、均一拡散 (Uniform Spreading) が必須であること、およびレーダーの検出が原因で非占有期間にあるチャネルの表示も含まれます。

次の例は、DFS が有効になっているチャネルで **show controller** コマンドを実行した時の出力行を示しています。前のパラグラフにリストで表示された内容は、**太字**で記載されています。

```
ap#show controller dot11radio1
!
interface Dot11Radio1
Radio AIR-RM1251A, Base Address 011.9290ec0, BBlock version 0.00, Software version 6.00.0
Serial number FOC083114WK
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: Americas (OFDM) (US )
Uniform Spreading Required: Yes
Current Frequency: 5300 MHz Channel 60 (DFS enabled)
Current Frequency: 5300 MHz Channel 60 (DFS enabled)
Allowed Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) *5260(52) *5280(56) *5300(60) *5320(64) *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *5660(132) *5680(136) *5700(140) 5745(149) 5765(153) 5785(157) 5805(161)
* = May only be selected by Dynamic Frequency Selection (DFS)

Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) 5180(36) 5200(40) 5220(44) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64) 5500(100) 5520(104) 5540(108) 5560(112) 5580(116) 5600(120) 5620(124) 5640(128) 5660(132) 5680(136) 5700(140) 5720(144) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0; Beacons are enabled; Probes are enabled
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
...
```

### チャネルの設定

チャネルを設定するには **channel** コマンドを使用します。インターフェイスのコマンドは、特定のチャネル番号を選択して DFS を有効にすることだけをユーザに許可するように変更されています。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface dot11radio1 dfs</b>	802.11a 無線のインターフェイス設定を開始します。

	コマンド	目的
ステップ 3	<code>channel {number   dfs /band &lt;1 - 4&gt;}</code>	<p><code>number</code> には、36、40、44、48、149、153、157、161、5180、5200、5220、5240、5745、5765、5785、または 5805 のいずれかのチャネルを入力します。</p> <p>選択されたチャネルで動的周波数選択を使用するには、<b>dfs</b> および次のいずれかの周波数帯を入力します。</p> <p>1 : 5.150 ~ 5.250 GHz  2 : 5.250 ~ 5.350 GHz  3 : 5.470 ~ 5.725 GHz  4 : 5.725 ~ 5.825 GHz</p> <p>DFS だけで選択できるチャネルを設定しようとする、次のメッセージが表示されます。</p> <p>This channel number/frequency can only be used by Dynamic Frequency Selection (DFS)</p> <p>(注) <b>channel dfs</b> コマンドは、<b>-P</b> および <b>-Q</b> 規制ドメインではサポートされません。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに入力内容を保存します。

次の例は、チャネル 36 を選択し、周波数帯 1 についてチャネルで DFS を使用するように設定しています。

```
ap#configure terminal
ap(config)interface dot11radio1
ap(config-if) channel 36
ap(config-if)
```

## DFS 選択によるチャネルブロック

屋内や屋外など特定地域で使用できるチャネルを制限している規制地域の場合、DFS が有効になっている時にアクセス ポイントがそれらを選択しないようチャネルをまとめてブロックすることができます。DFS 選択によってチャネルをまとめてブロックするには、次の設定インターフェイス コマンドを使用してください。

**[no] dfs band [1] [2] [3] [4] block**

オプション 1、2、3、4 で、ブロック対象のチャネルを指定します。

- **1** : 5.150 ~ 5.250GHz の周波数を指定します。この周波数グループは UNII-1 帯域とも呼ばれています。
- **2** : 5.250 ~ 5.350GHz の周波数を指定します。この周波数グループは UNII-2 帯域とも呼ばれています。
- **3** : 5.470 ~ 5.725GHz の周波数を指定します。
- **4** : 5.725 ~ 5.825GHz の周波数を指定します。この周波数グループは UNII-3 帯域とも呼ばれています。

次の例は、DFS 中にアクセス ポイントが 5.150 ~ 5.350GHz の周波数を選択しないようにする方法を示しています。

```
ap(config-if)# dfs band 1 2 block
```

次の例は、DFS について 5.150 ~ 5.350GHz の周波数をブロック解除する方法を示しています。

```
ap(config-if)# no dfs band 1 2 block
```

次の例は、DFS についてすべての周波数をブロック解除する方法を示しています。

```
ap(config-if)# no dfs band block
```

## 802.11n ガード間隔の設定

802.11n ガード間隔は、パケット間のナノ秒単位の時間です。短時間（400ns）および長時間（800ns）の2つの設定が可能です。

特権 EXEC モードから、次の手順に従って 802.11n ガード間隔を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	<code>guard-interval {any   long}</code>	ガード間隔を入力します。 <ul style="list-style-type: none"> <li>any の場合、短時間（400ns）または長時間（800ns）のいずれかのガード間隔が可能です。</li> <li>long の場合、長時間（800ns）のガード間隔だけが可能です。</li> </ul>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

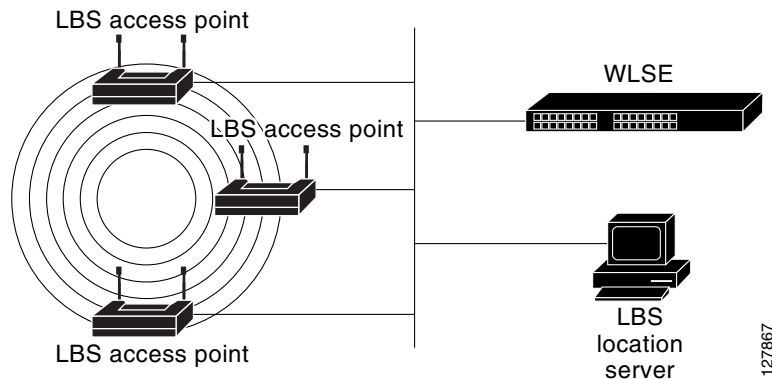
## 位置情報サービスの設定

この項では、アクセスポイントの CLI で、Location Based Service (LBS; 位置情報サービス) を設定する方法について説明します。他のアクセスポイント機能と同じように、ネットワークで Wireless LAN Solutions Engine (WLSE; 無線 LAN ソリューション エンジン) を使用して LBS を複数のアクセスポイントに設定することができます。LBS 設定は、このリリースのアクセスポイント GUI には表示されません。

## 位置情報サービスの概要

LBS には、少なくとも 3 つのアクセスポイントを設定することを推奨します。位置情報サービス (LBS) をアクセスポイントに設定すると、追跡対象のアセットに記載された LBS 位置決定タグから送信された位置パケットをアクセスポイントがモニタするようになります。アクセスポイントが位置決定パケットを受信すると、Received Signal Strength Indication (RSSI; 受信信号強度表示) を測定し、RSSI 値と位置パケットを受信した時刻を記載した UDP パケットを作成します。この UDP パケットをアクセスポイントが位置サーバに転送します。ロケーションサーバは、LBS に対応したアクセスポイントから受信した位置情報に基づいて LBS タグの位置を算出します。ネットワークに WLSE がある場合は、位置サーバがこの WLSE を照会して LBS に対応したアクセスポイントの状態を調べることができます。図 6-2 は、LBS 対応ネットワークの基本的な部分を示しています。

図 6-2 LBS ネットワークの基本構成



LBS を設定するアクセスポイントは、同じ圏内である必要があります。タグによるメッセージを報告したアクセスポイントが 1 箇所または 2 箇所だけである場合、位置サーバは報告してきたこの 2 つのアクセスポイントのカバレッジ領域内にそのタグがあることを報告できます。設定の詳細は、LBS タグと位置サーバのマニュアルを参照してください。

## アクセスポイントへのLBSの設定

アクセスポイントにLBSを設定するには、CLIを使用します。特権 EXEC モードから、次の手順に従ってLBSを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 lbs profile-name</code>	アクセスポイントにLBSプロファイルを作成し、LBS コンフィギュレーション モードを開始します。
ステップ 3	<code>server-address ip-address port port</code>	位置サーバの IP アドレス、および位置情報を記載した UDP パケットの送信先サーバのポートを入力します。
ステップ 4	<code>method {rssi}</code>	(任意) 位置サーバに位置情報を報告する際にアクセスポイントが使用する位置決定方法を選択します。このリリースでは、アクセスポイントが位置パケットの RSSI を計測する <code>rssi</code> が唯一のオプションでありデフォルトにも設定されています。
ステップ 5	<code>packet-type {short   extended}</code>	(任意) アクセスポイントがLBS タグから受け取るパケットタイプを選択します。 <ul style="list-style-type: none"> <li><b>short</b> : アクセスポイントがタグからショート位置パケットを受け入れます。ショートパケットでは、タグパケットのフレームボディからLBS情報が欠落し、タグの送信チャンネルがパケットに記載されます。</li> <li><b>extended</b> : これはデフォルト設定です。アクセスポイントがタグから拡張パケットを受け入れます。拡張パケットでは、フレームボディに2バイトのLBS情報を格納します。パケットのフレームボディに2バイトのLBS情報が格納されていない場合、アクセスポイントはそのパケットをドロップします。</li> </ul>
ステップ 6	<code>channel-match</code>	(任意) タグにより送信されたLBSパケットと、パケットの受信先無線チャンネルが一致するよう指定します。タグで使用しているチャンネルとアクセスポイントで使用しているチャンネルが一致しない場合、アクセスポイントはそのパケットをドロップします。Channel match はデフォルトで有効に設定されています。
ステップ 7	<code>multicast-address mac-address</code>	(任意) LBSパケットの送信にタグがマルチキャストアドレスを使用するよう指定します。デフォルトのマルチキャストアドレスは01:40:96:00:00:10に設定されています。
ステップ 8	<code>interface dot11 { 0   1 }</code>	このLBSプロファイルを有効に設定している無線インターフェイスを指定します。2.4GHz無線はRadio 0、5GHz無線はRadio 1です。このコマンドを入力しない限り、プロファイルはアクティブになりません。
ステップ 9	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。

次の例では、プロファイル `southside` がアクセスポイントの 802.11g 無線で有効に設定されています。

```
ap# configure terminal
ap(config)# dot11 lbs southside
```

```
ap(dot11-lbs)# server-address 10.91.105.90 port 1066
ap(dot11-lbs)# interface dot11 0
ap(dot11-lbs)# exit
```

## ワールド モードのイネーブル化とディセーブル化

ワイヤレス デバイスで、802.11d ワールド モード、Cisco レガシー ワールド モード、または ワールド モード ローミングをサポートするよう設定できます。ワールド モードをイネーブルにすると、ワイヤレス デバイスはそのビーコンにチャンネル キャリア設定情報を追加します。ワールド モードがイネーブルになっているクライアント デバイスは、キャリア セット情報を受信して、それぞれの設定を自動的に調整します。たとえば、日本で主に使用されるクライアント デバイスがイタリアに移され、そこでネットワークに参加した場合、ワールド モードに依存して、そのチャンネルと電力の設定を自動的に調整することができます。ファームウェア バージョン 5.30.17 以降を実行しているシスコのクライアント デバイスは、ワイヤレス デバイスが 802.11d ワールド モードとシスコのレガシー ワールド モードのどちらを使用しているかを検出し、ワイヤレス デバイスが使用しているモードと一致するワールド モードを自動的に使用します。

ワールド モードを常にオンに設定することも可能です。この構成では、アクセス ポイントは必要に応じて設定を変更することで、国と国との間でローミングを切り替えます。

ワールド モードはデフォルトではディセーブルに設定されています。

特権 EXEC モードから、次の手順に従ってワールド モードを有効にします。

コマンド	目的
ステップ 1 <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <b>interface dot11radio {0   1}</b>	無線 インターフェイスの インターフェイス コンフィギュレーション モードを開始します。
ステップ 3 <b>world-mode</b> <b>dot11d country_code code</b> <b>{ both   indoor   outdoor }</b> <b>world-mode roaming</b> <b>  legacy</b>	<p>ワールド モードを有効にします。</p> <ul style="list-style-type: none"> <li>802.11d ワールド モードをイネーブルにするには、<b>dot11d</b> オプションを入力します。 <ul style="list-style-type: none"> <li><b>dot11d</b> オプションを入力する場合、2 文字の ISO 国番号（たとえば、米国の ISO 国番号は <b>US</b>）を入力する必要があります。ISO 国番号の一覧は ISO の Web サイトに掲載されています。</li> <li>国番号の後に、ワイヤレス デバイスの配置場所を示すために <b>indoor</b>、<b>outdoor</b>、または <b>both</b> と入力します。</li> </ul> </li> <li>シスコのレガシー ワールド モードをイネーブルにするには、<b>legacy</b> オプションを入力します。</li> <li>アクセス ポイントを継続的なワールド モード構成に配置するには、<b>world-mode roaming</b> と入力します。</li> </ul> <p>(注) レガシー ワールド モードを使用するには、Aironet 拡張機能をイネーブルにする必要がありますが、802.11d ワールド モードではこの拡張機能は不要です。Aironet 拡張機能はデフォルトではイネーブルに設定されています。</p>

	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ワールド モードを無効にするには、コマンドの `no` 形式を使用します。

## short 無線プリアンブルのイネーブル化とディセーブル化

無線プリアンブル（ヘッダーと呼ばれる場合もある）は、パケットの先頭にあるデータ部です。ここには、ワイヤレス デバイスとクライアント デバイスのパケットの送受信に必要な情報が含まれています。無線プリアンブルを `long` または `short` に設定できます。

- **Short** : `short` プリアンブルを使用すると、スループットのパフォーマンスが向上します。Cisco Aironet 無線 LAN クライアント アダプタは、短いプリアンブルをサポートします。Cisco Aironet の初期の無線 LAN アダプタ (PC4800-J および PC4800A-J) には、長いプリアンブルが必要です。
- **Long** : 長いプリアンブルを使用すると、ワイヤレス デバイスと Cisco Aironet 無線 LAN アダプタのすべての初期モデル (PC4800-J および PC4800A-J) との互換性が保証されます。これらのクライアント デバイスがワイヤレス デバイスにアソシエートしない場合、`short` プリアンブルを使用する必要があります。

5 GHz 無線では無線プリアンブルに `short` と `long` を設定できません。

特権 EXEC モードから、次の手順に従って短い無線プリアンブルを無効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0 }</code>	2.4GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。
ステップ 3	<code>no preamble-short</code>	短いプリアンブルを無効にし、長いプリアンブルを有効にします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

デフォルトでは `short` プリアンブルがイネーブルに設定されています。`short` プリアンブルがディセーブルになっている場合、イネーブルにするには `preamble-short` コマンドを使用します。

## 送受信アンテナの設定

ワイヤレス デバイスがデータの送受信に使用するアンテナを選択できます。受信アンテナと送信アンテナでそれぞれ 3 つのオプションがあります。

- **Gain** : 結果のアンテナ ゲインを dB 単位で設定します。

- **Diversity** : デフォルト設定。最適な信号を受信するアンテナがワイヤレス デバイスで使用されます。ワイヤレス デバイスに2つの固定 (取り外し不能) アンテナが使用されている場合は、受信と送信の両方にこの設定を使用します。デバイスに3つの取り外し可能アンテナが使用されている場合、この設定を使用して、それらすべてのアンテナを **Diversity** モードで動作させることが可能です。
- **Right** : ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの右側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、右にあるのが右側のアンテナになります。
- **Middle** : 無線デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナが無線デバイスの中央コネクタに取り付けられている場合は、この設定を受信だけに使用する必要があります。3 アンテナ構成での送信に使用できるアンテナは、右と左のアンテナです。
- **Left** : ワイヤレス デバイスに取り外し可能なアンテナが使用されており、高ゲイン アンテナがワイヤレス デバイスの左側のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。ワイヤレス デバイスの背面パネルに向かって、左にあるのが左側のアンテナになります。

特権 EXEC モードから、次の手順に従ってワイヤレス デバイスがデータの送受信に使用するアンテナを選択します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。  802.11n 2.4GHz 無線は Radio 0 です。  802.11n 5GHz 無線は Radio 1 です。
ステップ 3	<code>gain dB</code>	デバイスに接続されたアンテナの結果のゲインを指定します。-128 ~ 128 dB の値を入力します。必要に応じて、1.5 などの小数値を使用できます。  (注) この設定は無線デバイスの動作に影響せず、ネットワークの WLSE にデバイスのアンテナ ゲインを通知するだけです。
ステップ 4	<code>antenna receive {diversity   left   middle   right}</code>	受信アンテナを <b>diversity</b> 、 <b>left</b> 、 <b>middle</b> 、 <b>right</b> 、または <b>all</b> に設定します。  (注) 2つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの <b>diversity</b> を使用します。1つのアンテナの場合、アンテナを右側に取り付け、アンテナを <b>right</b> に設定します。



	コマンド	目的
ステップ 5	<code>antenna transmit</code> {diversity   left   right}	送信アンテナを Diversity、Left、Right のいずれかに設定します。  (注) 2つのアンテナを使用してパフォーマンスを最適にするには、受信アンテナの設定にデフォルトの <b>diversity</b> を使用します。1つのアンテナの場合、アンテナを右側に取り付け、アンテナを <b>right</b> に設定します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## Gratuitous Probe Response の有効化と無効化

Gratuitous Probe Response (GPR) は、携帯および WLAN の動作モードをサポートするデュアルモード電話で、バッテリー残量を節約します。GPR は 5GHz 無線で使用可能で、デフォルトで無効に設定されています。GPR の設定には、次の 2 種類の設定があります。

- **Period** : (ビーコン間隔と同じように) GPR 伝送間の時間を 10 ~ 255 の Kusec 間隔で決定します。
- **Speed** : GPR の伝送に使用するデータ レートの速度です。

長い期間を選択すると、GPR によって消費される RF 帯域幅の量が減少し、バッテリー寿命が短くなる可能性があります。高い伝送速度を選択すると、消費される帯域幅の量が減少し、代わりにセル サイズが小さくなります。

特権 EXEC モードから、次の手順に従って GPR を有効にし、パラメータを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {1}</code>	5GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。
ステップ 3	<code>probe-response gratuitous</code> {period   speed}	デフォルトの period (10 Kusec) および speed (6.0 Mbps) を使用して Gratuitous Probe Response 機能を有効にします。
ステップ 4	<code>period Kusec</code>	(任意) 10 ~ 255 の範囲の値を入力します。デフォルト値は 10 です。
ステップ 5	<code>speed</code> {[6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0]}	(任意) 応答速度を Mbps 単位で設定します。デフォルト値は 6.0 です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

オプション パラメータのデフォルトを使用したくない場合、次の例に示すようにオプション パラメータを個別に設定したり、または結合して設定したりできます。

```
(config-if)# probe-response gratuitous speed 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30 speed 12.0
```

GPR 機能を無効にするには、コマンドの **no** 形式を使用します。

## Aironet 拡張機能のディセーブル化およびイネーブル化

デフォルトでは、ワイヤレス デバイスは Cisco Aironet 802.11 拡張機能を使用して Cisco Aironet クライアント デバイスの機能を検出し、ワイヤレス デバイスとアソシエートしたクライアント デバイスとの間での特定の相互作用に必要な機能をサポートします。次の機能をサポートするには、Aironet 拡張機能をイネーブルにする必要があります。

- **ロード バランシング**：ワイヤレス デバイスは Aironet 拡張機能を使用して、ネットワークとの最適な接続性を確保できるアクセス ポイントにクライアント デバイスを自動的に誘導します。これは、ユーザ数、ビット エラー レート、信号強度などの要因に基づいて行われます。
- **メッセージ完全性チェック (MIC)**：暗号化されたパケットへの攻撃 (ビットフリップ攻撃) を阻止するために新しく追加された WEP セキュリティ機能。MIC は、ワイヤレス デバイスと、それにアソシエートされたすべてのクライアント デバイスに実装され、数バイトを各パケットに付加することによって、パケットの改ざんを防ぎます。
- **Cisco Key Integrity Protocol (CKIP)**：IEEE 802.11i セキュリティ タスク グループによって提供された初期アルゴリズムに基づく、シスコの WEP キー置換技術です。標準規格に基づくアルゴリズムである Temporal Key Integrity Protocol (TKIP) では、Aironet 拡張機能を有効にする必要はありません。
- **リピータ モード**：Aironet 拡張機能はリピータ アクセス ポイントと、それらがアソシエートするルート アクセス ポイントで有効に設定されていなければなりません。
- **ワールド モード (レガシーのみ)**：レガシー ワールド モードがイネーブルになっているクライアント デバイスは、ワイヤレス デバイスからキャリア セット情報を受信して、それぞれの設定を自動的に調整します。802.11d ワールド モードを使用する場合、Aironet 拡張機能は不要です。
- **アソシエートされたクライアント デバイスの電力レベルの制限**：クライアント デバイスがワイヤレス デバイスにアソシエートするとき、そのワイヤレス デバイスは最大許可電力レベル設定をクライアントに送信します。

Aironet 拡張機能をディセーブルにすると、上記の機能はディセーブルになりますが、シスコ以外のクライアント デバイスがワイヤレス デバイスにアソシエートしやすくなる場合があります。

Aironet 拡張機能はデフォルトではイネーブルに設定されています。特権 EXEC モードから、次の手順に従って Aironet 拡張機能を無効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。  802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	<code>no dot11 extension aironet</code>	Aironet 拡張機能を無効にします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

Aironet 拡張機能がディセーブルになっている場合、イネーブルにするには `dot11 extension aironet` コマンドを使用します。

## イーサネット カプセル化変換方式の設定

ワイヤレス デバイスが 802.3 パケット以外のデータ パケットを受信する場合、そのワイヤレス デバイスはカプセル化変換方式を使用してパケットを 802.3 にフォーマットする必要があります。この変換方式には次の 2 種類があります。

- 802.1H : Cisco Aironet 無線製品に対して良好なパフォーマンスを提供します。
- RFC1042 : Cisco Aironet 以外の無線機器との良好な相互運用性を確保するには、この設定を使用します。RFC 1042 は、他の無線機器の製造業者によって使用されており、デフォルト設定となっています。

特権 EXEC モードから、次の手順に従ってカプセル化変換方式を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。  802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	<code>payload-encapsulation rfc1042   dot1h</code>	カプセル化変換方式を RFC 1042 ( <code>rfc1042</code> 、デフォルト設定) または 802.1h ( <code>dot1h</code> ) に設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## ワークグループブリッジへの信頼性のあるマルチキャストの有効化と無効化

*Reliable multicast messages from the access point to workgroup bridges* 設定は、マルチキャストメッセージの信頼できる送信を、ワイヤレスデバイスにアソシエートしている約 20 の Cisco Aironet ワークグループブリッジに制限します。デフォルト設定の **disabled** は、マルチキャスト送信の信頼性を下げて、より多くのワークグループブリッジがワイヤレスデバイスにアソシエートできるようにします。

通常、アクセスポイントやブリッジでは、ワークグループブリッジはクライアントデバイスとしてではなく、アクセスポイントやブリッジと同じインフラストラクチャデバイスとして扱われます。ワークグループブリッジがインフラストラクチャデバイスとして扱われる場合、ワイヤレスデバイスはアドレス解決プロトコル (ARP) パケットなどのマルチキャストパケットを、確実にワークグループブリッジに配信します。

信頼性の高いマルチキャスト配信のパフォーマンスコストのため (マルチキャストパケットが各ワークグループブリッジに二重に送信されるので)、ワークグループブリッジなどワイヤレスデバイスにアソシエートできるインフラストラクチャデバイスの数は制限されます。ワイヤレスデバイスへの無線リンクを維持できるワークグループブリッジの数を 21 以上にするには、ワイヤレスデバイスがマルチキャストパケットをワークグループブリッジに配信するときの信頼性を低くする必要があります。信頼性が低くなると、ワイヤレスデバイスはマルチキャストパケットが目的のワークグループブリッジに到達したかどうかを確認できなくなるため、ワイヤレスデバイスのカバレッジ領域の端にあるワークグループブリッジでは IP 接続が失われる可能性があります。ワークグループブリッジをクライアントデバイスとして扱うと、パフォーマンスは向上しますが、信頼性は低くなります。



(注) この機能は、固定型のワークグループブリッジでの使用に最適です。モバイル型のワークグループブリッジの場合、ワイヤレスデバイスのカバレッジ領域内でマルチキャストパケットを受信できないスポットに入る可能性があり、この場合、ワイヤレスデバイスにアソシエートされていても接続が失われてしまいます。

Cisco Aironet ワークグループブリッジでは、最大 8 つのイーサネット対応デバイスとの無線 LAN 接続を提供します。

この機能は、5GHz 無線ではサポートされていません。

特権 EXEC モードから、次の手順に従ってカプセル化変換方式を設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface dot11radio { 0 }</b>	2.4GHz 無線インターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。
ステップ 3	<b>infrastructure-client</b>	ワークグループブリッジへの信頼性のあるマルチキャストメッセージを有効にします。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

ワークグループブリッジへの信頼性のあるマルチキャストメッセージを無効にするには、コマンドの **no** 形式を使用します。

# Public Secure Packet Forwarding のイネーブル化とディセーブル化

Public Secure Packet Forwarding (PSPF) を使用すると、アクセス ポイントにアソシエートされているクライアント デバイスと、同じアクセス ポイントにアソシエートする他のクライアント デバイスとの偶発的なファイル共有や通信を防ぐことができます。PSPF は、クライアント デバイスに LAN におけるインターネット アクセスだけを許可し、その他の権限は与えません。この機能は、空港や大学の構内などに敷設されている公衆ワイヤレス ネットワークに有用です。



(注)

異なるアクセス ポイントにアソシエートするクライアント間での通信を防ぐために、ワイヤレス デバイスを接続するスイッチに保護ポートを設定する必要があります。保護ポートの設定方法については、「[保護ポートの設定](#)」(P.6-34) を参照してください。

ワイヤレス デバイス上で CLI コマンドを使用して PSPF をイネーブルまたはディセーブルにするには、ブリッジ グループを使用します。次の文書に、ブリッジ グループに関する詳細な説明と、ブリッジ グループを実装する手順が収められています。

- 『*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*』。このリンクをクリックすると、「[Configuring Transparent Bridging](#)」の章が表示されます。  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm\\_c/bcftp1/bcftb.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftp1/bcftb.htm)

PSPF は Web ブラウザ インターフェイスを使用して有効および無効にできます。PSPF 設定は [Radio Settings] ページで行います。

PSPF はデフォルトでディセーブルに設定されています。特権 EXEC モードから、次の手順に従って PSPF を有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線 インターフェイスの インターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。  802.11n 2.4GHz 無線は Radio 0 です。 802.11n 5GHz 無線は Radio 1 です。
ステップ 3	<code>bridge-group group port-protected</code>	PSPF を有効にします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

PSPF を無効にするには、コマンドの `no` 形式を使用します。

## 保護ポートの設定

無線 LAN の異なるアクセス ポイントにアソシエートするクライアント デバイス間での通信を防ぐために、ワイヤレス デバイスを接続するスイッチにプロテクトド ポートを設定する必要があります。

特権 EXEC モードから、次の手順に従ってスイッチ上のポートをプロテクトド ポートとして定義します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、設定するスイッチポート インターフェイスのタイプと番号を <code>gigabitethernet0/1</code> のように入力します。
ステップ 3	<code>switchport protected</code>	インターフェイスを保護ポートに設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show interfaces interface-id switchport</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

保護ポートをディセーブルにするには、`no switchport protected` インターフェイス コンフィギュレーション コマンドを使用します。

保護ポートとポート ブロックングについての詳細は、『*Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EAI*』の「Configuring Port-Based Traffic Control」の章を参照してください。次のリンクをクリックすると上記のガイドを参照できます。

[http://www.cisco.com/en/US/products/hw/switches/ps646/products\\_configuration\\_guide\\_book09186a008011591c.html](http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_book09186a008011591c.html)

## ビーコン間隔と DTIM の設定

ビーコン間隔はアクセス ポイントのビーコン間の時間 (キロマイクロ秒) です。1 K $\mu$ sec は 1,024 マイクロ秒に相当します。常にビーコン間隔の倍数となるデータ ビーコンレートにより、ビーコンに Delivery Traffic Indication Message (DTIM) が格納される頻度が決定されます。DTIM は、省電力モードのクライアント デバイスに、パケットがクライアント待ちであることを通知します。

たとえば、ビーコン間隔をデフォルトの 100 に設定し、データ ビーコンレートをデフォルトの 2 に設定すると、ワイヤレス デバイスは DTIM を含むビーコンを 200 K $\mu$ sec ごとに送信します。1 K $\mu$ sec は 1,024 マイクロ秒に相当します。

デフォルトのビーコン間隔は 100、デフォルトの DTIM は 2 です。特権 EXEC モードから、次の手順に従ってビーコン間隔および DTIM を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 802.11n 2.4GHz 無線は 0 です。 5GHz 無線および 802.11n 5GHz 無線は 1 です。
ステップ 3	<code>beacon period value</code>	ビーコン間隔を設定します。値をキロマイクロ秒で入力します。
ステップ 4	<code>beacon dtim-period value</code>	DTIM を設定します。値をキロマイクロ秒で入力します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## RTS しきい値と再試行回数の設定

Request To Send (RTS; 送信要求) しきい値は、パケットの送信前にワイヤレス デバイスが RTS を発行するときのパケット サイズを決定します。多数のクライアント デバイスがワイヤレス デバイスにアソシエートされているエリアや、クライアントが遠く分散しているために、ワイヤレス デバイスは検知できても、クライアント同士が互いに検知できないエリアでは、RTS しきい値を低く設定すると効果的です。設定値を 0 ~ 2347 バイトの範囲で入力します。

最大 RTS リトライは、ワイヤレス デバイスが無線を介したパケット送信の試行を中止するまでに RTS を発行する最大回数です。1 ~ 128 の範囲の値を入力します。

すべてのアクセス ポイントおよびブリッジに対するデフォルトの RTS しきい値は 2347、デフォルトの最大 RTS リトライ設定は 32 です。特権 EXEC モードから、次の手順に従って RTS しきい値と最大 RTS リトライを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>rts threshold value</code>	RTS しきい値を設定します。RTS しきい値は 0 ~ 2347 の範囲で入力します。
ステップ 4	<code>rts retries value</code>	最大 RTS リトライ回数を設定します。1 ~ 128 の範囲の値を入力します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RTS 設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

## 最大データ再試行回数の設定

最大データリトライ設定は、ワイヤレス デバイスがパケット送信を放棄し、そのパケットをドロップするまでに行うパケット送信の最大再送回数です。

デフォルト設定は 32 です。特権 EXEC モードから、次の手順に従って最大データリトライを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0 1}</code>	無線 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>packet retries value</code>	最大データリトライ回数を設定します。1 ~ 128 の範囲の値を入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

## フラグメンテーションしきい値の設定

フラグメンテーションしきい値は、断片化されて複数のブロックとして送信されるパケットの最小サイズを決定します。通信状態の悪いエリアや電波干渉が非常に多いエリアでは、低い数値を設定します。

デフォルト設定は 2338 バイトです。特権 EXEC モードから、次の手順に従ってフラグメンテーションしきい値を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0 1}</code>	無線 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>fragment-threshold value</code>	フラグメンテーションしきい値を設定します。2.4GHz 無線の場合は 256 ~ 2346 バイトの間で入力します。5GHz 無線の場合は 256 ~ 2346 バイトの間で入力します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



設定をデフォルトにリセットする場合は、コマンドの **no** 形式を使用します。

## 802.11g 無線の short スロット時間のイネーブル化

802.11g、2.4GHz 無線のスループットは、短いスロット時間を有効にすることで向上します。スロット時間を標準の 20 マイクロ秒から 9 マイクロ秒の short スロット時間まで短縮すると、全体のバックオフが減少し、スループットが向上します。バックオフは、スロット時間の倍数であり、LAN 上にパケットを送信するまでにステーションが待機するランダムな長さの時間です。

多くの 802.11g 無線は short スロット時間をサポートしていますが、サポートしていないものもあります。短いスロット時間を有効にした場合、ワイヤレス デバイスは、802.11g、2.4GHz 無線にアソシエートされたすべてのクライアントが短いスロット時間をサポートしている場合だけこれを使用します。

短いスロット時間は、802.11g、2.4GHz 無線だけでサポートされています。short スロット時間は、デフォルトではディセーブルに設定されています。

無線インターフェイス モードで、次のコマンドを入力して短いスロット時間を有効にします。

```
ap(config-if)# short-slot-time
```

**no short-slot-time** を入力し、Short スロット時間をディセーブルにします。

## キャリア話中検査の実行

キャリア ビジー テストを実行して、ワイヤレス チャネルでの無線活動をチェックします。キャリア ビジー テストでは、キャリア検査を実行して検査結果を表示するまでの約 4 秒間、ワイヤレス デバイスはワイヤレス ネットワーキング デバイスとのアソシエーションをすべて停止します。

特権 EXEC モードで、次のコマンドを入力して、キャリア ビジー テストを実行します。

```
dot11 interface-number carrier busy
```

*interface-number* については、**dot11radio 0** を入力して、2.4GHz 無線上の検査を実行するか、**dot11radio 1** を入力して、5GHz 無線上の検査を実行します。

**show dot11 carrier busy** コマンドを入力して、キャリア話中検査結果を再表示します。

## VoIP パケット処理の設定

CoS 5 (Video) および CoS 6 (Voice) のユーザの優先順位について、低いレイテンシの 802.11 MAC 動作を改善することによって、アクセス ポイントでの無線ごとの VoIP パケット処理の品質を向上させることができます。

アクセス ポイントの VoIP パケット処理を設定する手順は、次のとおりです。

- ステップ 1** ブラウザを使用して、アクセス ポイントにログインします。
- ステップ 2** Web ブラウザ インターフェイスの左側にあるタスク メニューで [Services] をクリックします。
- ステップ 3** Services のリストが展開されたら、[Stream] をクリックします。  
[Stream] ページが表示されます。

**ステップ 4** 設定する無線のタブをクリックします。

**ステップ 5** CoS 5 (ビデオ) および CoS 6 (音声) の両方のユーザの優先順位について、[Packet Handling] ドロップダウン リストから [Low Latency] を選択し、パケット廃棄の最大リトライ回数の値を、対応するフィールドに入力します。

最大再試行回数のデフォルト値は、Low Latency 設定では 3 です (図 6-3)。この値は、損失したパケットを廃棄する前に、アクセス ポイントがパケットを取得しようとする回数を示します。



(注) CoS 4 (負荷制御) ユーザの優先順位およびその最大再試行回数も設定できます。

**ステップ 6** [Apply] をクリックします。

図 6-3 パケット処理の設定

**Packet Handling per User Priority:**

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Low Latency	3 (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

146920

CLI を使用して VoIP パケット処理を設定することも可能です。CLI を使用して VoIP パケット処理を設定するための Cisco IOS コマンドのリストについては、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。

## VoWLAN メトリックの表示

VoWLAN メトリックによって、VoIP のパフォーマンスに関する診断情報が提供されます。この情報は、WLAN または有線ネットワークのどちらで問題が発生しているのかを判別するために役立ちます。VoWLAN メトリックは WLSE に保存されます。



(注) WLSE では VoWLAN メトリックを 90 秒ごとに更新し、最大 1.5 時間のメトリックを保存します。

## 音声レポートの表示

WLSE に保存されている VoWLAN メトリックをリストした音声レポートに、ブラウザを使用してアクセスできます。アクセスポイントグループおよび個々のアクセスポイントについてのレポートを表示できます。

音声レポートを表示する手順は、次のとおりです。

- ステップ 1 WLSE にログインします。
- ステップ 2 [Reports] タブをクリックします。
- ステップ 3 [Voice] をクリックします。
- ステップ 4 [Report Name] ドロップダウン リストから、[AP Group Metrics Summary: Current] を選択します。
- ステップ 5 左側からアクセスポイントグループをクリックします。

図 6-4 の例に示すように、グループメトリックが右側に表示されます。各行はグループ内のアクセスポイントを表します。

図 6-4 アクセスポイントメトリックの要約

Time	AP Name	Interface Name	OOS	% PL R (Downlink)	% PL R (Uplink)	Avg. Queuing Delay (ms) (Downlink)	Avg. Queuing Delay (ms) (Uplink)	% Packets > 40ms Queuing Delay	% Packets > 20ms Queuing Delay	Client(s) Using IL APSD	Roaming Delay (ms)
02-03-11.24	sjc14-42a-ap26.cisco.com	Dot11Radio0	0.0	0.0	0.0	0	0	0.0	0.0	No	0

グループメトリックの要約に表示されている情報は、グループに属する個々のアクセスポイントのすべての音声クライアントからのメトリックを集約したものです。

- ステップ 6 1つのアクセスポイントまたはアクセスポイントのグループの音声メトリックを表示するには、左側の [Device Selector] ツリーからグループまたはデバイスを選択して、[Report Name] ドロップダウンリストから表示するレポート名を選択します。
  - アクセスポイントの現在のメトリックを表示するには、[Report Name] ドロップダウンリストから [AP Detail: Current] を選択します。結果のレポートには、アクセスポイントに接続されている各クライアントのメトリックが表示されます。
  - 過去1時間に記録されたメトリックの集約を表示するには、[Report Name] ドロップダウンリストから [AP Detail: Last Hour] を選択します。
  - 過去1時間のキューイング遅延のグラフを表示するには、[Report Name] ドロップダウンリストから [Voice Queuing Delay] を選択します。
  - 過去1時間のパケット損失のグラフを表示するには、[Report Name] ドロップダウンリストから [Voice Packet Loss] を選択します。

- 過去 1 時間の音声ローミングのグラフを表示するには、[Report Name] ドロップダウン リストから [Voice Roaming] を選択します。
- 過去 1 時間に使用された音声帯域幅のグラフを表示するには、[Report Name] ドロップダウン リストから [Bandwidth In Use (% Allowed)] を選択します。
- 処理中の音声ストリームのグラフを表示するには、[Report Name] ドロップダウン リストから [Voice Streams In Progress] を選択します。
- 拒否された音声ストリームのグラフを表示するには、[Report Name] ドロップダウン リストから [Rejected Voice Streams] を選択します。

図 6-5 は、音声キューイング遅延グラフの例です。

図 6-5 キューイング遅延が 40ms を超えるパケットの割合

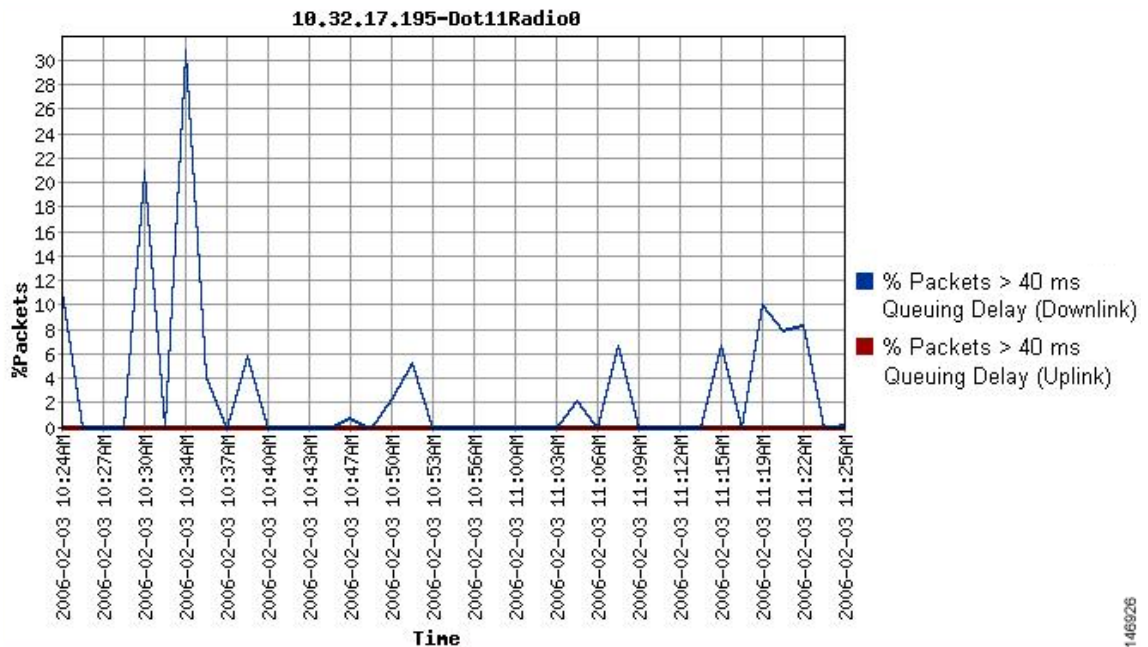
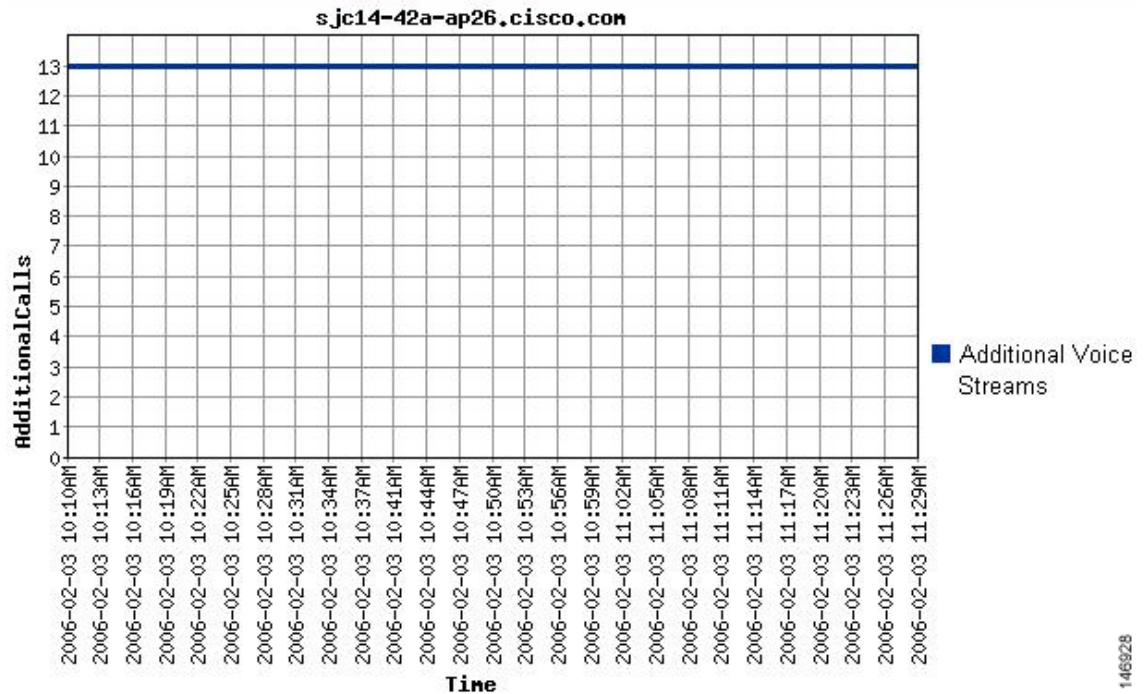


図 6-6 は、処理中の音声ストリーミングを示すグラフの例です。

図 6-6 処理中の音声ストリーミング



146928

## 無線クライアント レポートの表示

音声レポートはアクセス ポイントの観点から表示するだけでなく、クライアントの観点からも表示できます。WLSE では各クライアントについて、クライアントがアソシエートされているアクセス ポイントと、記録された VoWLAN メトリックが表示されます。

無線クライアントの音声レポートを表示する手順は、次のとおりです。

- ステップ 1** WLSE にログインします。
- ステップ 2** [Reports] タブをクリックします。
- ステップ 3** [Wireless Clients] をクリックします。
- ステップ 4** [Report Name] ドロップダウン リストから、表示するレポートのタイプを選択します。  
たとえば、過去 1 時間の VoWLAN メトリックを表示するには、[Voice Client Detail: Last Hour] を選択します。
- ステップ 5** 左側の [Search] フィールドを使用して、MAC アドレスが特定の基準に一致するクライアントを検索します。
- ステップ 6** 左側からクライアントの MAC アドレスをクリックして、対応する VoWLAN メトリックを表示します。  
図 6-7 の例に示すように、メトリックが右側に表示されます。

図 6-7 無線クライアントのメトリック

Client MAC Address(18)

Voice Client Details: Last Hour - 000d282e86a2

Time	QOS	AP Name	Interface Name	Packet Count (Downlink)	Packet Count (Uplink)	% PLR (Downlink)	% PLR (Uplink)	Avg. Queuing Delay (ms) (Downlink)	Avg. Queuing Delay (ms) (Uplink)	% Packets > 40ms Queuing Delay	% Packets > 20ms Queuing Delay	Using U-APSD	Roaming Delay (ms)	Roaming Count
02-03-10.24	Red	sjc14-42a-ap26.cisco.com	Dot11Radio0	10	0	0.0	0.0	78	0	10.0	0.0	No	0	0
02-03-10.26	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	65	0	0.0	0.0	0	0	0.0	0.0	No	0	0
02-03-10.27	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	23	0	0.0	0.0	1	0	0.0	0.0	No	0	0
02-03-10.29	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	6	0	0.0	0.0	0	0	0.0	0.0	No	0	0
02-03-10.30	Red	sjc14-42a-ap26.cisco.com	Dot11Radio0	16	0	0.0	0.0	65	0	12.5	0.0	No	0	0
02-03-10.32	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	2	0	0.0	0.0	1	0	0.0	0.0	No	0	0
02-03-10.34	Red	sjc14-42a-ap26.cisco.com	Dot11Radio0	6	0	0.0	0.0	146	0	12.5	0.0	No	0	0
02-03-10.35	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	45	0	0.0	0.0	40	0	2.2222223	0.0	No	0	0
02-03-10.37	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	11	0	0.0	0.0	0	0	0.0	0.0	No	0	0
02-03-10.39	Green	sjc14-42a-ap26.cisco.com	Dot11Radio0	13	0	0.0	0.0	14	0	3.8461537	0.0	No	0	0

> > Page 1 of 5      Show 10 20 All rows

## 音声障害の要約の表示

WLSE の [Faults] > [Voice Summary] ページには、次の音声障害の種類について検出された障害の要約が表示されます。

- 過剰な音声帯域幅 (CAC)
- 低下した音声 QOS (TSM)

音声障害の要約を表示する手順は、次のとおりです。

- ステップ 1** WLSE にログインします。
- ステップ 2** [Faults] タブをクリックします。
- ステップ 3** [Voice Summary] をクリックします。

図 6-8 の例に示すように、両方の障害のタイプについて検出された障害の数が画面にリストされます。



図 6-8 音声障害の要約

Wireless LAN Solution Engine

Wizard | Overview | Help | About | Logout  
Fri Feb 3, 2006 11:35:15

IDS | Faults | Devices | Configure | Firmware | Reports | Radio Mgr | Sites | Admin

Display Faults - Manage Fault Settings - Voice Summary - Voice QoS Settings - Notification Settings

Voice Summary

Refresh(Sec)

Voice Fault Type	Number Detected
Excessive Voice Bandwidth (CAC)	0
Degraded Voice QoS (TSM)	0

QoS Status	Number of Reports
APs with Degraded QoS	0
APs with Fair QoS	0
APs with Normal QoS	1

146923

## 音声の QoS 設定

WLSE の [Faults] > [Voice QoS Settings] 画面を使用して、次のパラメータについての音声 QoS のしきい値を定義できます。

- Downstream Delay with U-ASPD not used (U-ASPD を使用しない場合のダウンストリーム遅延)
- Downstream Delay with U-ASPD used (U-ASPD を使用する場合のダウンストリーム遅延)
- Upstream Delay (アップストリーム遅延)
- Downstream Packet Loss Rate (ダウンストリームのパケット損失レート)
- Upstream Packet Loss Rate (アップストリームのパケット損失レート)
- Roaming Time (ローミング時間)

音声障害の要約を表示する手順は、次のとおりです。

- 
- ステップ 1** WLSE にログインします。
- ステップ 2** [Faults] タブをクリックします。
- ステップ 3** [Voice QoS Settings] をクリックします。
- ステップ 4** 設定を変更するには、対応するドロップダウン リストから新しい値を選択します。  
たとえば、90 % 以上のパケットの遅延が 20 ms 未満のときに緑色に表示されるように Upstream Delay パラメータの QoS インジケータを設定するには、図 6-9 の例に示すように、[Green] 列のパラメータのドロップダウン リストから [90] を選択します。
- ステップ 5** 操作が終了したら [Apply] をクリックします。
-

図 6-9 音声の QoS 設定

	Green	Yellow	Red
Downstream Delay with U-ASPD not used	90 percent or more of packets have delay less than 20 ms	90 percent or more of packets have delay less than 40 ms	More than 10 percent of packets have delay equal or greater than 40 ms
Downstream Delay with U-ASPD used	50 percent or more of packets have delay less than 20 ms	90 percent or more of packets have delay less than 40 ms	More than 10 percent of packets have delay equal or greater than 40 ms
Upstream Delay	90 percent or more of packets have delay less than 20 ms	90 percent or more of packets have delay less than 40 ms	More than 10 percent of packets have delay equal or greater than 40 ms
Downstream Packet Loss Rate	Less than 2.5 percent	Less than 5.0 percent	Equal or greater than 5.0 percent
Upstream Packet Loss Rate	Less than 2.5 percent	Less than 5.0 percent	Equal or greater than 5.0 percent
Roaming Time	Less than 125 ms	Less than 350 ms	Equal or greater than 350 ms

Reset Apply

146924

## 音声障害の設定

WLSE の [Faults] > [Manage Fault Settings] 画面を使用して、障害の生成を有効化し、生成される障害の優先順位を指定できます。

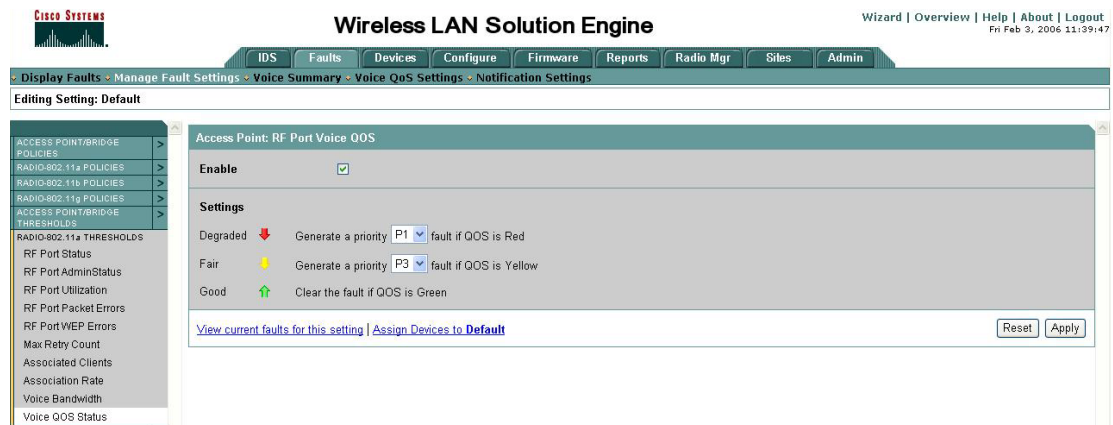
障害設定を行う手順は、次のとおりです。

- ステップ 1 WLSE にログインします。
- ステップ 2 [Faults] タブをクリックします。
- ステップ 3 [Manage Fault Settings] をクリックします。
- ステップ 4 QoS が赤色 (Fair) の場合に生成される障害の優先順位を、対応するドロップダウン リストから選択します。
- ステップ 5 操作が終了したら [Apply] をクリックします。

図 6-8 の例では、QoS が Degraded のときに P1 障害、QoS が Fair のときに P3 障害が生成されます。QoS が緑色の場合、生成された障害は消去されます。



図 6-10 障害設定



## ClientLink の設定

Cisco ClientLink (Beam Forming と呼ばれます) はインテリジェントなビームフォーミングテクノロジーです。RF 信号を 802.11a/g デバイスに送信して、パフォーマンスを 65 % 向上させ、カバレッジを最大 27 % 拡大し、カバレッジ ホールを減少させます。

Cisco ClientLink は、クライアントが混在するネットワークにおける既存の 802.11a/g デバイスの耐用年数の延長に寄与します。Cisco ClientLink は、802.11n に移行し、種類に関係なく、ネットワーク上のすべてのクライアントに必要な帯域幅およびスループットを確保することを求める組織にとって有益です。



(注) ClientLink は、1140、1260、1500、1600、2600、3500、および 3600 シリーズのアクセス ポイントでのみ使用可能です。



(注) 1040 アクセス ポイントでは、ClientLink はサポートされていません。

## CLI を使用した ClientLink の設定

ClientLink を有効にするには、インターフェイス コンフィギュレーション モードの 802.11n 無線インターフェイスで、次の CLI コマンドを入力します。

```
beamform ofdm
```



(注) 現在、ClientLink 設定オプションは、GUI では使用できません。

ClientLink はデフォルトでは無効に設定されています。詳細は、cisco.com の次の URL を参照してください。

[http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white\\_paper\\_c11-516389.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white_paper_c11-516389.html)

## 無線機能のデバッグ

無線機能のデバッグを開始するには、**debug dot11** 特権 EXEC コマンドを使用します。デバッグ操作を停止するには、このコマンドの **no** 形式を使用します。コマンド構文は次のとおりです。

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map | syslog | virtual-interface}
```

構文は、表 6-5 に示すとおりです。

表 6-5 *debug dot11* コマンドの構文

Syntax	説明
events	無線に関連するすべてのイベントのデバッグをアクティブにします。
packets	送受信された無線パケットのデバッグをアクティブにします。
forwarding	転送された無線パケットのデバッグをアクティブにします。
mgmt	無線アクセス ポイントの管理アクティビティのデバッグをアクティブにします。
network-map	無線アソシエーション管理のネットワークマップのデバッグをアクティブにします。
syslog	無線システム ログのデバッグをアクティブにします。
virtual interface	無線仮想インターフェイスのデバッグをアクティブにします。

この例では、無線に関連するすべてのイベントのデバッグを開始する方法を示します。

```
AP# debug dot11 events
```

この例では、無線パケットのデバッグを開始する方法を示します。

```
AP# debug dot11 packets
```

この例では、無線システム ログのデバッグを開始する方法を示します。

```
AP# debug dot11 syslog
```

この例では、無線に関連するすべてのイベントのデバッグを停止する方法を示します。

```
AP# no debug dot11 events
```



(注)

デバッグが有効になっていない状態が、コマンドのデフォルトです。



## 複数の SSID の設定

---

この章では、アクセス ポイントで複数の Service Set Identifier (SSID) を設定および管理する方法について説明します。この章の内容は、次のとおりです。

- 「複数の SSID の概要」 (P.7-2)
- 「複数の SSID の設定」 (P.7-4)
- 「複数の基本 SSID の設定」 (P.7-9)
- 「SSID に対する IP リダイレクションの割り当て」 (P.7-12)
- 「SSIDL IE への SSID の追加」 (P.7-15)
- 「MBSSID の NAC サポート」 (P.7-15)

## 複数の SSID の概要

SSID は、無線ネットワークング デバイスが無線接続を確立および維持するために使用する、一意の識別子です。ネットワークまたはサブネットワーク上の複数のアクセス ポイントは、同じ SSID を使用できます。SSID では大文字と小文字が区別され、最大 32 文字の英数字を使用できます。SSID には、スペースを含めないようにしてください。

アクセス ポイントには、最大 16 の SSID を設定でき、各 SSID に異なる設定を割り当てることができます。すべての SSID は同時にアクティブになります。つまり、クライアント デバイスは、どの SSID を使用してもアクセス ポイントにアソシエートできます。各 SSID には、次の設定を割り当てることができます。

- VLAN
- クライアント 認証方式



(注) クライアント認証タイプの詳細は、[第 11 章「認証タイプの設定」](#)を参照してください。

- SSID を使用するクライアント アソシエーションの最大数
- SSID を使用するトラフィックの RADIUS アカウンティング
- ゲスト モード
- リピータ モード (認証ユーザ名とパスワードを含む)
- クライアント デバイスから受信されたパケットのリダイレクション

アクセス ポイントに対し、設定内に SSID が指定されていないクライアント デバイスからのアソシエーションを許可する場合、ゲスト SSID を設定できます。アクセス ポイントでは、ビーコンにゲスト SSID が追加されます。ゲスト モードが無効になっていると、SSID がビーコンメッセージでブロードキャストされません。設定済み SSID のないクライアントが無線ネットワークに接続しないようにするには、このゲスト SSID 機能を無効に設定してください。ゲスト モード SSID の設定方法とゲスト モード SSID の無効化する方法については、「[SSID のグローバルな作成](#)」(P.7-4)を参照してください。

アクセス ポイントをリピータとして使用する場合、またはリピータの親として機能するルートアクセス ポイントとする場合は、SSID をリピータ モードで使用するよう設定できます。リピータ モードの SSID に認証ユーザ名とパスワードを割り当てると、クライアント デバイス同様、リピータでネットワークへの認証が可能になります。

ネットワークで複数の VLAN を使用する場合は、各 VLAN に 1 つの SSID を割り当てることができます。この割り当てた SSID を使用するクライアント デバイスは、その VLAN にグループ化されます。

## ソフトウェア バージョンの SSID に対する影響

Cisco IOS Release 12.3(2)JA には、複数インターフェイス環境で SSID パラメータを簡単に設定できるよう、グローバル モードの SSID 設定が導入されました。Cisco IOS Release 12.3(2)JA リリースでは、下位互換性があるようインターフェイス レベルで SSID パラメータを設定できましたが、Cisco IOS Release 12.3(4)JA 以降のリリースではインターフェイス レベルで SSID パラメータをまったく設定できなくなります。[表 7-1](#) は、Cisco IOS リリースでサポートされている SSID 設定方法を示しています。

表 7-1 Cisco IOS リリースでサポートされている SSID 設定方法

Cisco IOS リリース	サポートされている SSID 設定方法
12.2(15)JA	インターフェイス レベルだけ。
12.3(2)JA	インターフェイス レベルとグローバルの両方。
12.3(4)JA および 12.3(7)JA	インターフェイス レベルとグローバルの両方。グローバル モードではすべての SSID を保存。
12.3(4)JA 以降	グローバルだけ。

Cisco IOS Release 12.3(10b)JA は、CLI を使用してインターフェイス レベルで SSID パラメータを設定できますが、SSID はグローバル モードで保存されます。SSID をすべてグローバル モードで保存すると、Cisco IOS Release 12.4(21a)JA1 以降のリリースにアップグレードしても SSID 設定が維持されます。

Cisco IOS Release 12.3(2)JA 以前を 12.3(4)JA 以降のリリースにアップグレードする必要がある場合は、まず Cisco IOS Release 12.3(4)JA にアップグレードしてコンフィギュレーション ファイルを保存してから、目的のリリースにアップグレードし、保存しておいたコンフィギュレーション ファイルをロードします。この手順を行うと、インターフェイス レベルの SSID 設定がグローバル モードに正しく変換されます。12.3(4)JA 以前のリリースから 12.3(4)JA 以降のリリースに直接アップグレードすると、インターフェイス レベルの SSID 設定は削除されます。

Cisco IOS Release 12.4(21a)JA1 からソフトウェア バージョンをダウングレードすると、以前に作成した SSID はすべて無効になります。ダウングレード後に SSID を再設定しなくて済むよう、Cisco IOS Release 12.3(7)JA にアップグレードする前に旧ソフトウェア バージョンのコンフィギュレーション ファイルのコピーを保存しておいてください。Cisco IOS Release 12.3(7)JA からソフトウェア バージョンをダウングレードする場合は、ダウングレード後に、保存しておいたこのコンフィギュレーション ファイルをロードしてください。

表 7-2 は、Cisco IOS Release 12.2(15)JA を実行しているアクセス ポイントでの SSID 設定と、Cisco IOS Release 12.3(7)JA にアップグレードした後の設定の例を示しています。

表 7-2 例：アップグレード後にグローバル モードに変換された SSID 設定

12.2(15)JA での SSID 設定	12.3(7)JA にアップグレードした後の SSID 設定
<pre>interface dot11Radio 0   ssid engineering   authentication open   vlan 4  interface dot11Radio 1   ssid engineering   authentication open   vlan 5</pre>	<pre>dot11 ssid engineering   authentication open   vlan 5   ! interface dot11Radio 0   ssid engineering  interface dot11Radio 1   ssid engineering</pre>

インターフェイスごとの VLAN 設定が、グローバルの SSID 設定に残っていることに注意してください。



(注) SSID、VLAN、および暗号化方式は、1対1対1の関係で相互にマッピングされます。つまり、1つの SSID を 1つの VLAN にマッピングでき、1つの VLAN を 1つの暗号化方式にマッピングできます。グローバル SSID 設定を使用する場合、1つの SSID を 2つの異なる暗号化方式に設定できません。たとえば、インターフェイス dot11 0 では SSID *north* を Temporal Key Integrity Protocol (TKIP) に適用して、インターフェイス dot11 1 では SSID *north* を Wired Equivalent Privacy (WEP) 128 に適用することはできません。

## 複数の SSID の設定

次の項では、複数の SSID の設定情報を説明します。

- 「デフォルトの SSID 設定」(P.7-4)
- 「SSID のグローバルな作成」(P.7-4)
- 「RADIUS サーバを使用した SSID の制限」(P.7-8)



(注) Cisco IOS Release 12.3(4)JA 以降では、SSID をグローバルに設定できる他、特定の無線インターフェイスに適用することもできます。SSID をグローバルに設定するには、「SSID のグローバルな作成」(P.7-4) の手順に従ってください。

## デフォルトの SSID 設定

Cisco IOS Release 12.3(7)JA には、デフォルトの SSID は存在しません。

## SSID のグローバルな作成

Cisco IOS Release 12.3(2)JA 以降では、SSID をグローバルに設定できる他、特定の無線インターフェイスについて設定することもできます。**dot11 ssid** グローバル コンフィギュレーション コマンドを使用して SSID を作成すると、**ssid** 設定インターフェイス コマンドを使用して、特定のインターフェイスにその SSID を割り当てることができます。

グローバル コンフィギュレーション モードで SSID を作成しておき、**ssid** 設定インターフェイス コマンドを実行すると、目的のインターフェイスにその SSID が割り当てられますが、SSID コンフィギュレーション モードにはなりません。SSID をグローバル コンフィギュレーション モードで作成していない場合は、**ssid** コマンドを実行すると、CLI が新しい SSID についての SSID コンフィギュレーション モードとなります。



(注) ソフトウェア バージョンを旧バージョンのリリースにダウングレードすると、Cisco IOS Release 12.3(7)JA 以前で作成した SSID は無効になります。

特権 EXEC モードから、次の手順に従って SSID をグローバルに作成します。SSID を作成した後、SSID を特定の無線インターフェイスに割り当てることができます。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>dot11 ssid <i>ssid-string</i></b>	<p>SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。</p> <p>SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。</p> <p>(注) 先頭の文字に !、#、; の文字は使用できません。</p> <p>(注) +、]、/、"、TAB、末尾のスペースは、SSID には無効な文字です。</p>
ステップ 3	<b>authentication client username <i>username</i> password <i>password</i></b>	(任意) アクセス ポイントがリピータ モードのときにネットワークへの認証に使用する、認証ユーザ名とパスワードを設定します。リピータ アクセス ポイントがルート アクセス ポイントまたは別のリピータにアソシエートするために使用するユーザ名およびパスワードを、SSID に設定します。
ステップ 4	<b>accounting <i>list-name</i></b>	(任意) この SSID の RADIUS アカウンティングを有効にします。 <i>list-name</i> には、アカウンティング方式のリストを指定します。方式のリストの詳細は、次のリンクをクリックしてください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2</a>
ステップ 5	<b>vlan <i>vlan-id</i></b>	(任意) ネットワーク上の VLAN に SSID を割り当てます。この SSID を使用してアソシエートするクライアント デバイスは、この VLAN にグループ化されます。1 つの VLAN には、1 つの SSID だけを割り当てることができます。
ステップ 6	<b>guest-mode</b>	(任意) SSID をアクセス ポイントのゲスト モード SSID として指定します。アクセス ポイントはビーコンに SSID を追加し、SSID を指定していないクライアント デバイスからのアソシエーションを許可します。



	コマンド	目的
ステップ 7	<code>infrastructure-ssid [optional]</code>	<p>このコマンドは、アクセス ポイントとブリッジが互いにアソシエートする際に使用する SSID を制御します。ルート アクセス ポイントでは、インフラストラクチャ SSID を使用してアソシエートができるのは、リピータ アクセス ポイントだけです。ルート ブリッジでは、インフラストラクチャ SSID を使用してアソシエートができるのは、非ルート ブリッジだけです。リピータ アクセス ポイントと非ルート ブリッジは、この SSID を使用してルート デバイスとアソシエートします。</p> <p>アクセス ポイントとブリッジの GUI では、リピータの役割および非ルート ブリッジの役割にインフラストラクチャ SSID の設定が必要です。ワークグループブリッジの役割にインフラストラクチャ SSID を設定する必要はありません。ただし、デバイスの役割の設定に CLI を使用すれば、複数の SSID が無線に設定されていない限り、インフラストラクチャ SSID の設定は不要になります。複数の SSID が無線に設定されている場合は、<code>infrastructure-ssid</code> コマンドを使用して、非ルートブリッジがルートブリッジとの接続に使用する SSID を指定する必要があります。</p> <p>しかし、12.4(21a)JA1 および 12.3(8)JEC リリース以降では、1 つまたは複数の SSID の有無に関係なく、インフラストラクチャ SSID が設定されない場合、リピータはブリッジとアソシエートしません。</p>
ステップ 8	<code>interface dot11radio { 0   1 }</code>	<p>SSID の割り当て先とする無線インターフェイスに対して、インターフェイス コンフィギュレーション モードを開始します。</p> <p>2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。</p> <p>5GHz 無線および 5GHz 802.11n 無線は 1 です。</p>
ステップ 9	<code>ssid ssid-string</code>	<p>ステップ 2 で作成したグローバル SSID を無線インターフェイスに割り当てます。</p>
ステップ 10	<code>end</code>	<p>特権 EXEC モードに戻ります。</p>
ステップ 11	<code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>



(注) 各 SSID に認証タイプを設定する場合は、`ssid` コマンドの認証オプションを使用します。認証タイプの設定方法については、第 9 章「ローカル認証サーバとしてのアクセス ポイントの設定」を参照してください。



(注) 802.11b と 802.11g が同じ 2.4GHz 帯で動作するため、802.11g 無線にゲストの SSID モードを有効にすると、802.11b 無線にも適用されます。

SSID または SSID 機能を無効にするには、コマンドの `no` 形式を使用します。



次の例は、次の方法を示します。

- SSID の名前の指定
- RADIUS アカウンティングの SSID の設定
- この SSID を使用してアソシエートするクライアント デバイスの最大数を 15 に設定
- SSID の VLAN への割り当て
- SSID の無線インターフェイスへの割り当て

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if)#end
```

## グローバルに設定された SSID の表示

グローバルに設定された SSID の設定詳細を表示するには、次のコマンドを使用します。

```
AP# show running-config ssid ssid-string
```

## SSID でのスペースの使用

Cisco IOS Release 12.3(7)JA 以降では、SSID にスペースを含めることができますが、末尾のスペース（SSID の末尾のスペース）は無効になります。ただし、以前のバージョンで作成した SSID に末尾のスペースがある場合は、認識されます。末尾のスペースがあると、同じアクセス ポイント上で、同一の SSID が複数設定されているように表示されます。アクセス ポイント上で同一の複数の SSID があると考えられる場合は、特権 EXEC コマンド **show dot11 associations** を使用して、以前のリリースで作成した SSID に末尾にスペースがないか確認してください。

たとえば、次の特権 EXEC コマンド **show configuration** からの出力例では、SSID 中のスペースが表示されません。

```
ssid buffalo
  vlan 77
  authentication open

ssid buffalo
  vlan 17
  authentication open

ssid buffalo
  vlan 7
  authentication open
```

ただし、次の特権 EXEC コマンド **show dot11 associations** からの出力例では、SSID 中のスペースが表示されます。

```
SSID [buffalo] :
SSID [buffalo ] :
SSID [buffalo ] :
```



(注) このコマンドで表示するのは、SSID の最初の 15 文字だけです。15 文字を超えた SSID を表示するには、**show dot11 associations client** コマンドを使用してください。

## RADIUS サーバを使用した SSID の制限

クライアント デバイスが、不正な SSID を使用してアクセス ポイントにアソシエートするのを防ぐために、RADIUS 認証サーバでクライアントが使用する必要のある、許可された SSID のリストを作成します。

SSID 許可のプロセスは、次の手順で行われます。

1. クライアント デバイスはアクセス ポイントに設定された任意の SSID を使用して、アクセス ポイントにアソシエートします。
2. クライアントは、RADIUS 認証を開始します。
3. RADIUS サーバは、クライアントが使用を許可された SSID のリストを返します。アクセス ポイントは、このリスト内に、クライアントが使用する SSID と一致する SSID があるかどうかをチェックします。次の 3 とおりの結果が予測されます。
  - a. クライアントがアクセス ポイントとのアソシエーションに使用した SSID が、RADIUS サーバが返した許可リスト内のエン트리に一致する場合、クライアントはすべての認証要件を満たした後にネットワークへのアクセスを許可されます。
  - b. アクセス ポイントが、SSID の許可リストにクライアントと一致するエントリを検出できなかった場合は、このクライアントはアソシエーションを解除されます。
  - c. RADIUS サーバがクライアントに SSID をまったく返さない場合（リストなし）は、管理者がリストを設定していないことを意味します。この場合、クライアントはアソシエーションと認証の試行を許可されます。

RADIUS サーバの返す SSID の許可リストは、シスコ Vendor-Specific Attribute (VSA; ベンダー固有の属性) の形式です。Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) のドラフト規格では、アクセス ポイントと RADIUS サーバ間で、ベンダー固有の属性 (属性 26) を使用してベンダー固有の情報をやり取りする方法を指定しています。各ベンダーは、Vendor-Specific Attribute (VSA) を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートするオプションはベンダー タイプ 1、名前は *cisco-avpair* です。RADIUS サーバには、クライアントあたり 0 以上の SSID VSA を指定できます。

次の例では、次の AV ペアにより、ユーザの SSID 許可リストに SSID *batman* が追加されます。

```
cisco-avpair= "ssid=batman"
```

VSA を認識して使用できるようにアクセス ポイントを設定する方法については、「[ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定](#)」(P.13-17) を参照してください。

## 複数の基本 SSID の設定

アクセス ポイント 802.11a、802.11g、802.11n 無線は、MAC アドレスと同様、最大 8 つの基本 SSID (BSSID) をサポートします。複数の BSSID を使用して SSID ごとに固有の Delivery Traffic Indication Message (DTIM) 設定を割り当て、複数の SSID をビーコンにブロードキャストできます。DTIM を大きな値に設定すると、SSID を使用する省電力モードのクライアント デバイスではバッテリーの寿命が延びます。また、複数の SSID をブロードキャストすると、ゲストが無線 LAN にアクセスしやすくなります。



(注)

アクセス ポイントの MAC アドレスに基づいて特定のアクセス ポイントにアソシエートするよう設定していた場合 (クライアント デバイス、リピータ、ホット スタンバイユニット、ワークグループブリッジなど)、複数の BSSID の追加または削除を行うと、無線 LAN 上のデバイスがアソシエーションを損失することがあります。複数の BSSID を追加または削除する際には、特定のアクセス ポイントにアソシエートするよう設定されていたデバイスのアソシエーション状態を確認してください。必要に応じて、アソシエートされていないデバイスを再設定して、BSSID の MAC アドレスを使用するようにします。

## 複数 BSSID の設定要件

複数の BSSID を設定するには、アクセス ポイントが少なくとも次の要件を満たしている必要があります。

- VLAN が設定されていること。
- アクセス ポイントが Cisco IOS Release 12.3(4)JA 以降を実行していること。
- アクセス ポイントに、複数の BSSID をサポートする 802.11a または 802.11g 無線が組み込まれていること。無線が複数の基本 SSID をサポートしているかどうかを調べるには、**show controllers radio\_interface** コマンドを入力してください。結果に次の行が含まれていれば、その無線は複数の基本 SSID をサポートしています。

```
Number of supported simultaneous BSSID on radio_interface: 8
```

## 複数の BSSID を使用する際のガイドライン

複数の BSSID を設定する際は、次のガイドラインに留意してください。

- 複数の BSSID を有効に設定すると、RADIUS サーバによる VLAN 割り当て機能がサポートされなくなります。
- BSSID を有効に設定すると、アクセス ポイントが各 SSID に BSSID を自動的にマッピングします。BSSID を特定の SSID に手動でマッピングすることはできません。
- アクセス ポイントで複数の BSSID を有効に設定すると、SSIDL IE には、SSID リストは追加されず、拡張機能だけが追加されます。
- Wi-Fi 認定済みクライアント デバイスであれば、どれでも複数 BSSID を使用したアクセス ポイントにアソシエートできます。
- Wireless Domain Service (WDS; 無線ドメイン サービス) を構成するアクセス ポイントでは、複数の BSSID を有効に設定できます。

## 複数のBSSIDの設定

複数のBSSIDを設定する手順は、次のとおりです。

- ステップ 1** アクセスポイントのGUIから、[Global SSID Manager] ページを表示します（GUIではなくCLIを使用する場合は、この項の最後のCLIの設定例に記載しているCLIコマンドを参照してください）。[図 7-1](#) は、[Global SSID Manager] ページの上部を示しています。

**図 7-1** [Global SSID Manager] ページ

The screenshot displays the Cisco Aironet 1240AG Series Access Point GUI. The top navigation bar includes the Cisco Systems logo and the device name. The main content area is titled "Security: Global SSID Manager". On the left, there is a sidebar menu with options like HOME, EXPRESS SET-UP, SECURITY, and SERVICES. The main content area is divided into several sections: "SSID Properties", "Current SSID List", "Client Authentication Settings", and "Client Authenticated Key Management". The "Current SSID List" section shows a table with one entry: "< NEW >" and "test". The "Client Authentication Settings" section includes "Methods Accepted" (Open Authentication checked, Shared Authentication and Network EAP unchecked) and "Server Priorities" (EAP and MAC Authentication Servers both set to "Use Defaults").

- ステップ 2** [SSID] フィールドに SSID 名を入力します。

- ステップ 3** [VLAN] ドロップダウン リストから、SSID を割り当てる VLAN を選択します。
- ステップ 4** SSID を有効に設定している無線インターフェイスを選択します。無線インターフェイスに SSID を有効に設定しない限り、SSID はアクティブになりません。
- ステップ 5** [Network ID] フィールドに、SSID のネットワーク ID を入力します。
- ステップ 6** このページの [Authentication Settings]、[Authenticated Key Management]、[Accounting Settings] セクションから、認証、認証済みキー管理、アカウントिंग設定を SSID に設定します。BSSID は、SSID でサポートされているすべての認証タイプをサポートします。
- ステップ 7** (任意) SSID をビーコンに追加するには、[Multiple BSSID Beacon Settings] セクションで [Set SSID as Guest Mode] チェックボックスをオンにします。
- ステップ 8** (任意) この SSID を使用する省電力モードのクライアントのバッテリーの寿命を延ばすには、[Set Data Beacon Rate (DTIM)] チェックボックスをオンにして SSID のビーコン レートを入力します。ビーコン レートによって、Delivery Traffic Indicator Message (DTIM) を追加したビーコンをアクセス ポイントが送信する頻度が決まります。

DTIM を追加したビーコンをクライアント デバイスが受信すると、通常は、保留中のパケットをチェックするためにクライアント デバイスが再起動します。DTIM の間隔が長くなると、クライアントのスリープ時間が長くなり、電力を節約できます。反対に、DTIM の間隔が短くなるとパケットの受信の遅延を抑えられますが、クライアントが頻繁に起動するためバッテリー残量が消費されます。

デフォルトのビーコン レートは 2 に設定されています。つまり、ビーコン 1 つおきに DTIM が追加されます。ビーコン レートは 1 ~ 100 の値で入力します。



(注) DTIM 期間のカウントを増やすと、マルチキャスト パケットの送信は遅れます。マルチキャスト パケットはバッファリングされるため、DTIM 期間のカウントを大きくするとバッファがオーバーフローする可能性があります。

- ステップ 9** [Guest Mode/Infrastructure SSID Settings] セクションで、[Multiple BSSID] を選択します。
- ステップ 10** [Apply] をクリックします。

## CLI の設定例

次の例は、無線インターフェイスで複数の BSSID を有効に設定する CLI コマンド、*visitor* を呼び出した SSID を作成する CLI コマンド、SSID を BSSID に指定する CLI コマンド、BSSID がビーコンに追加されていることを指定する CLI コマンド、BSSID に DTIM 間隔を設定する CLI コマンド、無線インターフェイスに SSID *visitor* を設定する CLI コマンドを示しています。

```
ap(config)# interface d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
ap(config-if)# ssid visitor
```

また、**dot11 mbssid** グローバル コンフィギュレーション コマンドを使用すると、複数の BSSID をサポートしているすべての無線インターフェイスで、複数の BSSID を同時に有効にすることもできます。

## 設定済み BSSID の表示

SSID と BSSID の関係、または MAC アドレスを表示するには、`show dot11 bssid` 特権 EXEC コマンドを使用します。次の例はコマンドの出力を示しています。

```
AP1230#show dot11 bssid
Interface      BSSID          Guest  SSID
Dot11Radio1   0011.2161.b7c0 Yes    atlantic
Dot11Radio0   0005.9a3e.7c0f Yes    WPA2-TLS-g
```

## SSID に対する IP リダイレクションの割り当て

SSID に IP リダイレクションを設定すると、その SSID にアソシエートされたクライアント デバイスからアクセス ポイントに送信されたパケットはすべて、指定した IP アドレスにリダイレクトされます。IP リダイレクションが主に使用されるのは、特定の IP アドレスと通信するように静的に設定され、中央にあるソフトウェア アプリケーションを使用するハンドヘルド デバイスをクライアントとする無線 LAN です。たとえば、小売店や商品倉庫の無線 LAN 管理者は、バーコード スキャナに IP リダイレクションを設定できます。これらすべてのバーコード スキャナでは、同じスキャナ アプリケーションが使用され、すべてのデータは同じ IP アドレスに送信されます。

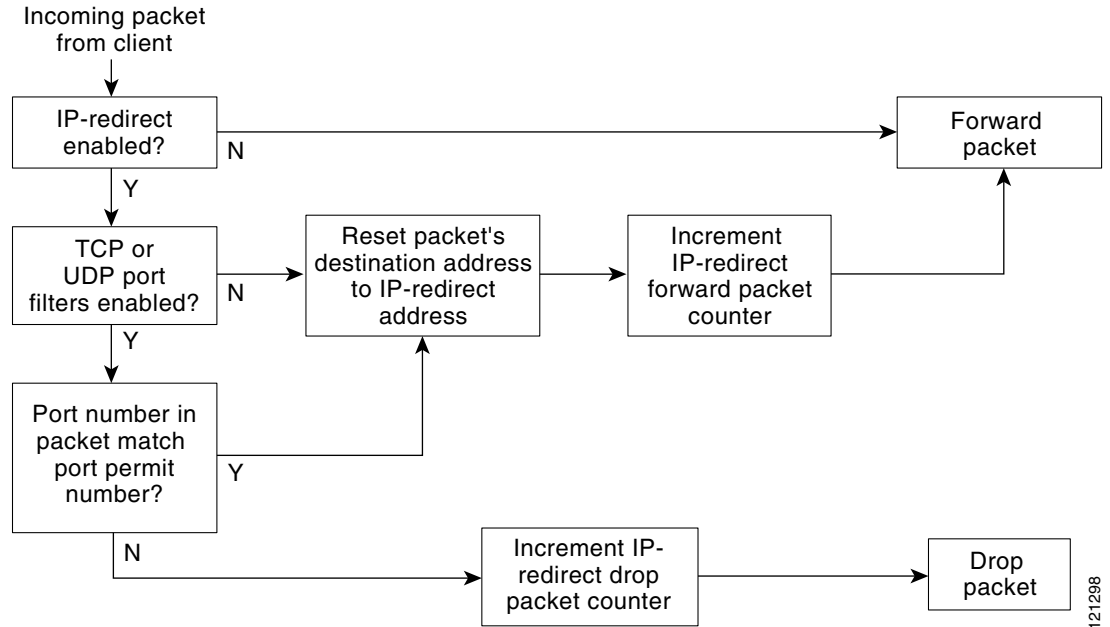
SSID を使用してアソシエートされているクライアント デバイスからのパケットをすべてリダイレクトできる他、アクセス コントロール リストで定義された特定の TCP ポートや UDP ポート宛てのパケットだけをリダイレクトすることもできます。特定のポート宛てのパケットだけがリダイレクトされるようにアクセス ポイントを設定すると、その SSID を使用しているクライアントからの該当のパケットがアクセス ポイントからリダイレクトされます。また、同じ SSID を使用しているクライアントからのその他のパケットは、アクセス ポイントでドロップされます。



(注) IP リダイレクトが設定された SSID を使用してアソシエートされているクライアント デバイスに対して、アクセス ポイントから ping テストを実行すると、そのクライアントからの応答パケットは、指定した IP アドレスにリダイレクトされ、アクセス ポイントでは受信されません。

図 7-2 は、IP リダイレクトが設定された SSID を使用してアソシエートされているクライアントからのパケットを、アクセス ポイントで受信した場合の処理フローを示しています。

図 7-2 IP リダイレクションの処理フロー



121298

## IP リダイレクションを使用する際のガイドライン

IP リダイレクションを使用する際は、次のガイドラインに留意してください。

- クライアント デバイスからブロードキャスト、ユニキャスト、またはマルチキャストで送信された BOOTP/DHCP パケットは、アクセス ポイントからリダイレクトされません。
- 受信パケットに対する ACL フィルタが存在する場合は、IP リダイレクションより優先して適用されます。

## IP リダイレクションの設定

特権 EXEC モードから、次の手順に従って SSID に IP リダイレクションを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	特定の SSID に対するコンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 4	<b>ip redirection host <i>ip-address</i></b>	目的の IP アドレスに対して、IP リダイレクション コンフィギュレーション モードを開始します。10.91.104.92 のように、ドットを使用して IP アドレスを入力します。  リダイレクションの対象となる TCP ポートや UDP ポートを定義したアクセス コントロール リスト (ACL) を指定しない場合は、クライアント デバイスから受信されたパケットはすべてアクセス ポイントからリダイレクトされます。
ステップ 5	<b>ip redirection host <i>ip-address</i> access-group <i>acl</i> in</b>	(任意) パケットのリダイレクションに適用する ACL を指定します。ACL で定義した特定の UDP ポートまたは TCP ポート宛てに送信されたパケットだけがリダイレクトされます。ACL で定義した設定に一致しない受信パケットはすべて廃棄されます。 <b>in</b> パラメータを指定すると、アクセス ポイントの受信インターフェイスに ACL が適用されます。



(注) ACL ロギングは、アクセス ポイントのプラットフォームのブリッジング インターフェイスではサポートされていません。ブリッジング インターフェイスに適用すると、インターフェイスがログ オプションなしで設定されたように動作し、ロギングは実施されません。BVI インターフェイスに別の ACL を使用している限り、ACL ロギングは、BVI インターフェイスで動作します。

次の例は、ACL を適用せずに SSID に IP リダイレクションを設定する方法を示しています。*batman* という SSID にアソシエートされているクライアント デバイスから受信されたパケットはすべて、アクセス ポイントからリダイレクトされます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

次の例は、BVI1 インターフェイスに適用済みの ACL で指定された特定の TCP ポートまたは UDP ポート宛てに送信されたパケットだけを対象とする IP リダイレクションを設定する方法を示しています。*robin* という SSID を使用してアソシエートされているクライアント デバイスから受信されたパケットは、指定の IP アドレス宛てにアクセス ポイントからリダイレクトされます。それ以外のパケットはすべて廃棄されます。

```
AP# configure terminal
AP(config)# interface bvi1
AP(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
AP(config-if-ssid)# end
```



## SSID IE へのSSIDの追加

アクセスポイントのビーコンでアドバタイズできるSSIDは、1つのブロードキャストSSIDだけです。ただし、アクセスポイントのビーコンにSSIDL Information Elements (SSIDL IE)を使用すれば、そのアクセスポイントには他にもSSIDがあることをクライアントデバイスに通知できます。あるSSIDを指定してSSIDL IEに追加しておく、クライアントデバイスではそのSSIDの存在が検出され、さらにそのSSIDを使用したアソシエートに必要なセキュリティ設定も検出されます。



(注) アクセスポイントで複数のBSSIDを有効に設定すると、SSIDL IEには、SSIDリストは追加されず、拡張機能だけが追加されます。

特権 EXEC モードから、次の手順に従ってSSIDをSSIDL IEに追加します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線 インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。  5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	特定のSSIDに対するコンフィギュレーション モードを開始します。
ステップ 4	<code>information-element ssid [advertisement] [wps]</code>	アクセスポイントの拡張機能をアドバタイズするアクセスポイントビーコンに、SSIDL IEを追加します。この拡張機能には、802.1x、Microsoft Wireless Provisioning Services (WPS) のサポートなどがあります。  SSIDL IEにSSIDの名前と機能を追加するには、 <b>advertisement</b> オプションを使用します。SSIDL IEにWPS機能フラグを設定するには、 <b>wps</b> オプションを使用します。

SSIDL IEを無効にするには、コマンドの **no** 形式を使用します。

## MBSSIDのNACサポート

ネットワークは、ウイルス、ワーム、スパイウェアなどのセキュリティ脅威から保護する必要があります。これらのセキュリティ脅威によって業務に支障をきたし、ダウンタイムが生じたり、パッチの適用に追われたりすることになります。ネットワークにアクセスしようとするすべての有線/無線デバイスが、企業のセキュリティポリシーに適合するように、エンドポイントを視覚化して管理することが必要です。感染したエンドポイントや脆弱なエンドポイントを自動的に検出して切り離し、クリーンな状態にする必要があります。

NACは、ネットワークリソースにアクセスするすべての有線/無線のエンドポイントデバイス(PC、ノートパソコン、サーバ、PDAなど)が適切にセキュリティ脅威から保護されるよう厳密に設計されています。NACを使用することにより、企業は、ネットワークに参加するすべてのデバイスを分析して管理できるようになります。すべてのエンドポイントデバイスが企業の

セキュリティポリシーに準拠し最新のセキュリティ保護策を確実に実行することにより、企業はウイルス感染やネットワークのセキュリティ侵害の経路となりやすいエンドポイントデバイスを大幅に削減または排除できます。

WLAN は、ウイルス、ワーム、スパイウェアなどのセキュリティ脅威から保護する必要があります。NAC アプライアンスも NAC フレームワークも、WLAN クライアントがネットワークにアクセスしようとするときにデバイスセキュリティポリシーを施行することで、WLAN をセキュリティ脅威から保護します。これらのソリューションは、ポリシーに準拠しない WLAN クライアントを検疫し、ポリシーに準拠するように修復するサービスを提供しています。

クライアントは、ソフトウェアのバージョンやウイルスのバージョンなどの状態に応じて、別々の VLAN に配置されます。必要なソフトウェアをダウンロードするよう VLAN を設定して、クライアントをネットワークのアクセスに必要なソフトウェアのバージョンにアップグレードします。NAC サポートには 4 つの VLAN が設定されます。そのうちの 1 つは通常の VLAN で、ここには、正しいソフトウェアバージョンを搭載したクライアントが配置されます。その他の VLAN は指定された検疫処理用に確保されています。クライアントがアップグレードされるまで、感染したすべてのクライアントはいずれか 1 つの VLAN に配置されます。

各 SSID では、最大 3 つの VLAN を「有害な」VLAN として設定できます。感染したクライアントは、感染状態に応じて、いずれか 1 つの VLAN に配置されます。クライアントがアソシエーション要求を送信すると、クライアントの感染ステータスをその要求に含めて RADIUS サーバへ送信します。クライアントを特定の VLAN に配置するポリシーのプロビジョニングが RADIUS サーバ上で行われます。

感染したクライアントがアクセスポイントにアソシエートして RADIUS サーバにそのステータスを送信すると、RADIUS サーバは状態に応じてそのクライアントを検疫 VLAN の 1 つに配置します。この VLAN は、dot1x クライアント認証プロセスの途中で、RADIUS サーバの Access Accept 応答内で送信されます。クライアントが健全な状態で、NAC に準拠している場合、RADIUS サーバは通常の VLAN 割り当てを SSID に返し、クライアントは正しい VLAN と BSSID に配置されます。

各 SSID には、通常の VLAN が割り当てられます。通常の VLAN とは、健全なクライアントが配置される VLAN のことです。また、SSID では、ステートに応じてクライアントが配置される検疫 VLAN 対応するバックアップ VLAN を最大 3 つまで設定できます。SSID 用のこれらの VLAN には、SSID の MBSSID によって割り当てた BSSID と同じものを使用します。

設定済み VLAN はそれぞれ異なり、同じ SSID 内で VLAN が重複することはできません。このため、VLAN を設定できるのは 1 つのインターフェイスにつき一度だけで、2 つの異なる SSID で VLAN は使用できません。

検疫 VLAN は、通常の VLAN を設定したインターフェイスで自動的に設定されます。検疫 VLAN は、通常 VLAN と同じ暗号プロパティを継承します。VLAN には、同じキー/認証タイプがあり、検疫 VLAN のキーは自動的に派生します。

Dot11 サブインターフェイスが生成され、dot1q カプセル化 VLAN（設定済み VLAN 数と同数）とともに自動的に設定されます。また、有線側のサブインターフェイスも、ファストイーサネット 0 サブインターフェイスのブリッジグループ設定に合わせて自動的に設定されます。

クライアントがアソシエートして RADIUS サーバが有害な状態と判断すると、dot1x 認証の RADIUS 認証応答内でサーバが検疫 NAC の VLAN のいずれかを返します。この VLAN は、クライアントの SSID で設定したバックアップ用 VLAN のうちの 1 つでなければなりません。この VLAN が、すでに設定したバックアップ用 VLAN のうちの 1 つでなければ、クライアントはアソシエートされません。

すべてのバックアップ用 VLAN に対応するデータは、SSID に割り当てられた BSSID を使用して送受信されます。このため、その SSID に対応する BSSID をリッスンしているすべてのクライアント（健全なクライアントおよび有害なクライアント）が再起動します。VLAN が健全か有害かに応じて、使用中のマルチキャストキーに基づき、クライアントでパケットの復号化が

行われます。有線側のトラフィックは、別のVLANを使用しているため隔離されます。このようにして、感染したクライアントのトラフィックと感染していないクライアントのトラフィックが混在しないようにしています。

次に示すように、`dot11 ssid <ssid>` では、これまでの `vlan <name> / <id>` に、新キーワード `backup` が追加されます。

```
vlan <name> | <id> [backup <name> | <id>, <name> | <id>, <name> | <id>
```

## MBSSID への NAC 設定

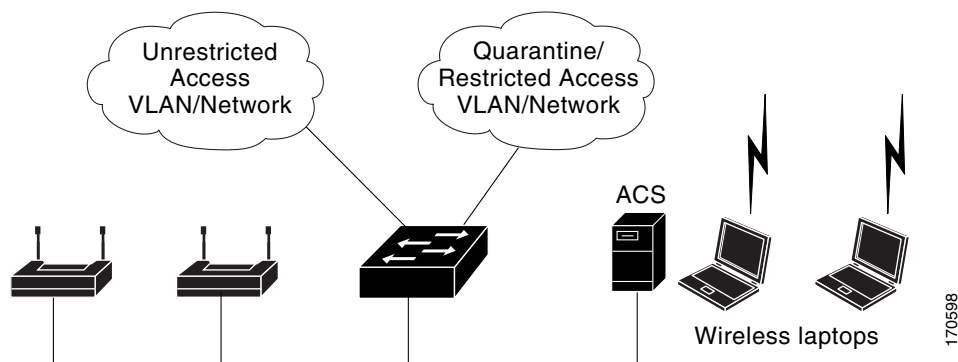


(注) この機能がサポートするのは、VLAN 内のレイヤ 2 モビリティだけです。この機能は、ネットワーク ID を使用するレイヤ 3 モビリティをサポートしません。



(注) アクセスポイントでMBSSIDのNACを有効にする前に、NACが正しく機能するようにしてください。図7-3は、一般的なネットワーク設定を示しています。

図7-3 一般的なNACネットワーク設定



詳細については、シスコ無線ネットワークにNACを展開する方法のマニュアルを参照してください。

アクセスポイントのMBSSIDにNACを設定する手順は、次のとおりです。

- ステップ 1 図7-3に示すように、ネットワークを設定します。
- ステップ 2 スタンドアロンのアクセスポイントと、NAC対応クライアントのEAP認証を設定します。
- ステップ 3 ポスチャを確認するため、ACSサーバにローカルプロファイルを設定します。
- ステップ 4 クライアントがEAP-FASTを使用して正常に認証できるよう、クライアントとアクセスポイントを設定します。
- ステップ 5 クライアントのポスチャが有効であることを確認します。
- ステップ 6 認証とポスチャ確認が完了したら、クライアントがアクセスポイントとアソシエートしていること、クライアントが制限のないVLANに配置されていることを確認します。

設定例を次に示します。

```

dot11 mbssid
dot11 vlan-name engg-normal vlan 100
dot11 vlan-name engg-infected vlan 102
dot11 vlan-name mktg-normal vlan 101
dot11 vlan-name mktg-infected1 vlan 103
dot11 vlan-name mktg-infected2 vlan 104
dot11 vlan-name mktg-infected3 vlan 105
!
dot11 ssid engg
    vlan engg-normal backup engg-infected authentication open
    authentication network-eap eap_methods
!
dot11 ssid mktg
    vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
    authentication open
    authentication network-eap eap_methods
!
interface Dot11Radio0
!
encryption vlan engg-normal key 1 size 40bit 7 482CC74122FD transmit-key
encryption vlan engg-normal mode ciphers wep40
!
encryption vlan mktg-normal key 1 size 40bit 7 9C3A6F2CBFBC transmit-key
encryption vlan mktg-normal mode ciphers wep40
!
ssid engg
!
ssid mktg
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1

```

```
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
```





## スパンニングツリー プロトコルの設定

この章では、アクセス ポイント/ブリッジにスパンニングツリー プロトコル (STP) を設定する方法について説明します。この章の内容は、次のとおりです。

- 「スパンニングツリー プロトコルの概要」 (P.8-2)
- 「STP 機能の設定」 (P.8-9)
- 「スパンニングツリー ステータスの表示」 (P.8-15)



(注)

この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Access Points and Bridges*』を参照してください。



(注)

STP は、アクセス ポイントがブリッジ モードのときだけ使用できます。

# スパニングツリープロトコルの概要

この項では、スパニングツリー機能の仕組みについて説明します。内容は次のとおりです。

- 「STP の概要」 (P.8-2)
- 「アクセス ポイント/ブリッジのプロトコル データ ユニット」 (P.8-3)
- 「スパニングツリー ルートの選択」 (P.8-4)
- 「スパニングツリー タイマー」 (P.8-5)
- 「スパニングツリー トポロジの作成」 (P.8-5)
- 「スパニングツリー インターフェイス ステート」 (P.8-6)

## STP の概要

STP は、ネットワーク上でループを防止しながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に動作するには、任意の 2 つのステーション間で存在できるアクティブ パスは 1 つだけです。スパニングツリーはエンドステーションに対して透過的に動作するため、エンドステーションが単一の LAN セグメントに接続されているのか、複数セグメントから成る LAN に接続されているのかを検出することはできません。

フォールトトレラントなインターネットワークを作成する場合、ネットワーク上のすべてのノード間にループフリーパスを構築する必要があります。スパニングツリー アルゴリズムは、レイヤ 2 ネットワーク全体でループのない最適なパスを計算します。無線アクセス ポイント/ブリッジやスイッチなどのインフラストラクチャ デバイスは、ブリッジプロトコル データ ユニット (BPDU) というスパニングツリーのフレームを一定間隔で送受信します。デバイスはこれらのフレームを転送せずに、ループのないパスを構成するために使用します。

エンドステーション間に複数のアクティブパスがあると、ネットワークにループが生じます。このループがネットワークに発生すると、エンドステーションにメッセージが重複して到着する可能性があります。また、インフラストラクチャ デバイスでも、複数のレイヤ 2 インターフェイス上でエンドステーションの MAC アドレスを学習する場合があります。このような状況によって、ネットワークが不安定になります。

STP は、レイヤ 2 ネットワーク内のルートブリッジと、ルートからすべてのインフラストラクチャ デバイスまでのループのないパスでツリーを定義します。



(注)

STP の説明において、ルートという用語は 2 つの概念を指して使用されます。1 つは、スパニングツリーの中央ポイントとして機能するネットワーク上のブリッジのことで、ルートブリッジと呼ばれます。もう 1 つは、各ブリッジでルートブリッジまでの最も効率的なパスを提供するポートのことで、ルートポートと呼ばれます。これらの意味は、ルートおよび非ルートのオプションを持つ無線ネットワーク設定の役割とは区別されます。無線ネットワーク設定の役割がルートブリッジとなっているブリッジが、必ずしもスパニングツリーのルートブリッジになるわけではありません。この章では、スパニングツリーのルートブリッジをスパニングツリールートと呼びます。

STP は冗長データパスを強制的にスタンバイ (ブロック) ステートにします。スパニングツリーのネットワークセグメントでエラーが発生したときに冗長パスが存在する場合は、スパニングツリーアルゴリズムがスパニングツリートポロジを再計算し、スタンバイパスをアクティブにします。



ブリッジ上の2つのインターフェイスがグループの一部を形成する場合、スパニングツリーポートの優先順位およびパスコストの設定により、2つのうちフォワーディングステートにするインターフェイスと、ブロッキングステートにするインターフェイスが決まります。ポートの優先順位の値は、ネットワークトポロジにおけるインターフェイスの位置を表し、その位置がトラフィックを渡すのにどの程度適しているかを示します。パスコスト値はメディアの速度を表します。

アクセスポイント/ブリッジは、Per-VLAN Spanning Tree (PVST) と VLAN を使用しない単一の 802.1q スパニングツリーの両方をサポートします。アクセスポイント/ブリッジは、複数の VLAN を1つのインスタンスのスパニングツリーにマッピングする 802.1s MST または 802.1d Common Spanning Tree を実行できません。

アクセスポイント/ブリッジは、設定されているアクティブな VLAN ごとに個別のスパニングツリーインスタンスを保持します。ブリッジの優先順位およびアクセスポイント/ブリッジの MAC アドレスから成るブリッジ ID は、各インスタンスに関連付けられます。VLAN ごとに、最も小さいアクセスポイント/ブリッジ ID を持つアクセスポイント/ブリッジが、その VLAN のスパニングツリールートになります。

## 1300 および 350 シリーズブリッジの相互運用性

Cisco Aironet 1300 および 350 シリーズブリッジは、STP が有効になっていて、かつ VLAN が設定されていない場合に相互運用が可能です。この設定を使用できるのは、次の理由がある場合に限られます。

- STP が無効になっているとき、350 シリーズブリッジが、350 シリーズアクセスポイントとして動作し、非ルートの 350、1200、および 1240 シリーズアクセスポイントなどの非ルートブリッジのアソシエーションを禁止する場合。
- 350 シリーズブリッジでは、非 VLAN および VLAN のどちらの設定でも STP の単一インスタンスだけをサポートするが、1300 シリーズブリッジでは、非 VLAN 設定で STP の単一インスタンスを、VLAN 設定で STP の複数インスタンスをサポートする場合。
- STP の単一インスタンスと複数インスタンスの間に互換性がないため、VLAN を設定すると、トラフィックのブロックに矛盾が生じる可能性がある場合。ネイティブ VLAN がブロックされると、ブリッジのフラッピングが発生する場合があります。

したがって、STP の相互運用性を考慮する場合、350 および 1300 シリーズアクセスポイント/ブリッジの STP 機能を有効にして、VLAN を設定しないのが最適な設定です。



(注) 350 および 1300 シリーズアクセスポイント/ブリッジは、ワークグループブリッジとして設定された場合、STP が無効化されて動作し、アクセスポイントとのアソシエーションを許可することができます。ただし、この設定は、技術的にはブリッジツーブリッジのシナリオではありません。

## アクセスポイント/ブリッジのプロトコルデータユニット

安定して有効なネットワークのスパニングツリートポロジは、次の要素によって決まります。

- 各無線アクセスポイント/ブリッジ上の各 VLAN に関連付けられた固有のアクセスポイント/ブリッジ ID (無線アクセスポイント/ブリッジの優先順位および MAC アドレス)
- スパニングツリールートまでのスパニングツリーパスコスト

- 各レイヤ 2 インターフェイスに対応付けられたポート ID (ポート プライオリティおよび MAC アドレス)

ネットワーク内のアクセス ポイント/ブリッジに電源が入ると、各アクセス ポイント/ブリッジは STP ルートとして機能します。アクセス ポイント/ブリッジは、イーサネット ポートおよび無線ポートを使用してコンフィギュレーション BPDU を送信します。BPDU によって通信が行われ、スパニングツリー トポロジが計算されます。各コンフィギュレーション BPDU には、次の情報が含まれます。

- 送信側のアクセス ポイント/ブリッジがスパニングツリー ルートとして識別する無線アクセス ポイント/ブリッジの固有のアクセス ポイント/ブリッジ ID
- ルートまでのスパニングツリー パス コスト
- 送信側のアクセス ポイント/ブリッジのアクセス ポイント/ブリッジ ID
- メッセージ エージ
- 送信側インターフェイス ID
- hello タイマー、転送遅延タイマー、および max-age プロトコル タイマーの値

アクセス ポイント/ブリッジは、*上位*の情報 (より小さいアクセス ポイント/ブリッジ ID やパス コストなど) を含むコンフィギュレーション BPDU を受信すると、そのポートの情報を保存します。この BPDU をアクセス ポイント/ブリッジのルート ポート上で受信した場合、そのアクセス ポイント/ブリッジが指定アクセス ポイント/ブリッジとなっているすべての接続 LAN に、更新したメッセージを付けて BPDU を転送します。

アクセス ポイント/ブリッジは、そのポートに現在保存されている情報よりも *下位*の情報を含むコンフィギュレーション BPDU を受信した場合は、その BPDU を廃棄します。アクセス ポイント/ブリッジが下位 BPDU を受信した LAN の指定アクセス ポイント/ブリッジである場合、そのポートに保存されている最新情報を含む BPDU をその LAN に送信します。このようにして下位情報は廃棄され、優位情報がネットワークで伝播されます。

BPDU の交換によって、次の処理が行われます。

- スパニングツリー ルートとしてアクセス ポイント/ブリッジが 1 つ選択されます。
- アクセス ポイント/ブリッジごとに (スパニングツリー ルートを除く) ルート ポートが 1 つ選択されます。このポートは、アクセス ポイント/ブリッジからスパニングツリー ルートにパケットを転送するときの最適パス (最小コスト) を提供します。
- スパニングツリー ルートへの最短距離は、パス コストに基づいてアクセス ポイント/ブリッジごとに計算されます。
- LAN セグメントごとに指定アクセス ポイント/ブリッジが選択されます。指定アクセス ポイント/ブリッジは、その LAN からスパニングツリー ルートにパケットを転送するときの最小パス コストを提供します。指定アクセス ポイント/ブリッジを LAN に接続しているポートのことを *指定ポート* と呼びます。
- スパニングツリー インスタンスに含めるインターフェイスが選択されます。ルート ポートおよび指定ポートは、フォワーディング ステートになります。
- スパニングツリーに含まれないすべてのインターフェイスはブロックされます。

## スパニングツリー ルートの選択

STP に参加しているレイヤ 2 ネットワークのすべてのアクセス ポイント/ブリッジは、BPDU データ メッセージの交換を通して、ネットワーク内の他のアクセス ポイント/ブリッジに関する情報を集めます。このメッセージ交換により、次の操作が発生します。

- スパニングツリー インスタンスごとに固有のスパニングツリー ルートを選択

- LAN セグメントごとに指定アクセス ポイント/ブリッジを1 つずつ選択
- 冗長リンクに接続されたレイヤ 2 インターフェイスをブロックすることにより、ネットワーク内のループを排除

VLAN ごとに、アクセス ポイント/ブリッジの優先順位が最も高いアクセス ポイント/ブリッジ（最も小さい数字の優先順位の値）がスパニングツリールートとして選択されます。すべてのアクセス ポイント/ブリッジがデフォルトの優先順位（32768）で設定されている場合、VLAN 内で MAC アドレスの最も小さいアクセス ポイント/ブリッジがスパニングツリールートになります。アクセス ポイント/ブリッジの優先順位の値は、アクセス ポイント/ブリッジ ID の最上位ビットに該当します。

アクセス ポイント/ブリッジの優先順位の値を変更すると、アクセス ポイント/ブリッジがルート アクセス ポイント/ブリッジとして選択される確率が変化します。大きい値を設定すると可能性が低下し、値が小さいと可能性が増大します。

スパニングツリールートは、スパニングツリートポロジにおいて論理的な中心に位置します。ネットワーク内のどこからもスパニングツリールートに到達する必要のないすべてのパスは、スパニングツリーのブロッキング モードになります。

BPDU には、アクセス ポイント/ブリッジおよび MAC アドレス、アクセス ポイント/ブリッジの優先順位、ポートの優先順位、およびパス コストを含む、送信側アクセス ポイント/ブリッジとそのポートに関する情報が含まれます。STP はこの情報を使用して、ネットワークのスパニングツリールートとルート ポート、および各 LAN セグメントのルート ポートと指定ポートを選択します。

## スパニングツリー タイマー

表 8-1 で、スパニングツリーのパフォーマンス全体を左右するタイマーについて説明します。

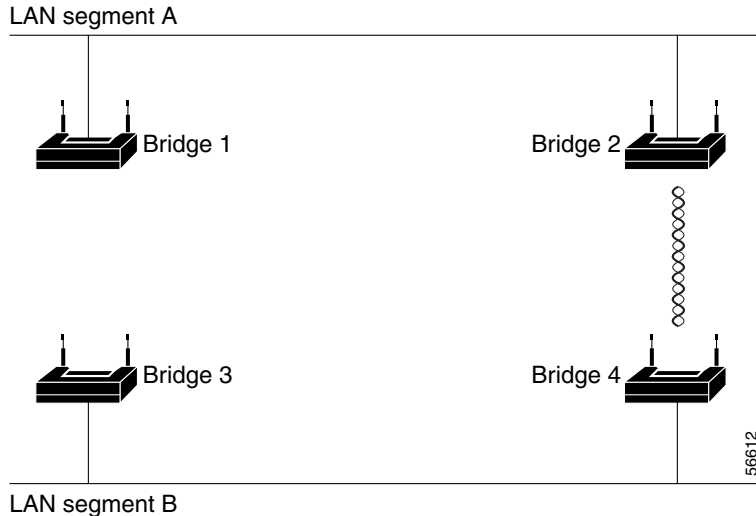
表 8-1 スパニングツリー タイマー

変数	説明
ハロー タイマー	アクセス ポイント/ブリッジが hello メッセージを他のアクセス ポイント/ブリッジにブロードキャストする頻度が決まります。
転送遅延タイマー	インターフェイスが転送を開始するまでに、リスニング ステートおよびラーニング ステートがそれぞれ持続する時間が決まります。
最大エイジング タイマー	アクセス ポイント/ブリッジがインターフェイス上で受信したプロトコル情報を保存する時間が決まります。

## スパニングツリートポロジの作成

図 8-1 では、すべてのアクセス ポイント/ブリッジの優先順位がデフォルト（32768）に設定されていて、ブリッジ 4 の MAC アドレスが最も小さいため、ブリッジ 4 がスパニングツリールートとして選択されています。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプが原因で、ブリッジ 4 が理想的なスパニングツリールートではない場合もあります。理想的なブリッジがスパニングツリールートになるように優先順位を上げる（数値を小さくする）ことにより、強制的にスパニングツリーを再計算させて、理想的なブリッジをスパニングツリールートとして使用する新しいトポロジを構成します。

図 8-1 スパニングツリー トポロジ



## スパニングツリー インターフェイス ステート

プロトコル情報が無線 LAN を通過する場合、伝播遅延が生じる可能性があります。結果として、その時々やさまざまな場所で、トポロジの変更が行われる場合があります。インターフェイスがスパニングツリー トポロジに含まれていない状態からフォワーディング ステートに直接移行すると、一時的にデータループが形成されることがあります。インターフェイスは、LAN 経由で伝播される新しいトポロジ情報を待ってから、フレームの転送を開始しなければなりません。インターフェイスはさらに、古いトポロジで使用されていた転送フレームのフレーム存続時間を満了させることも必要です。

スパニングツリーを使用しているアクセス ポイント/ブリッジ上の各インターフェイスは、次のいずれかのステートで存在します。

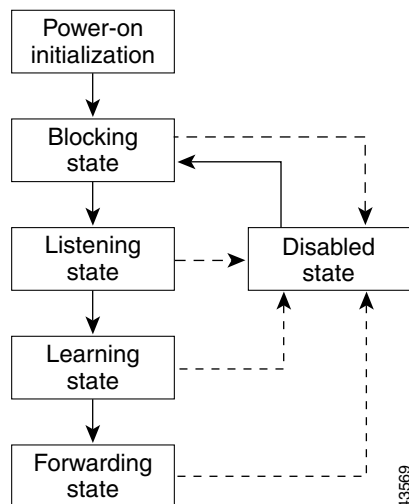
- **ブロッキング**：インターフェイスはフレーム転送に関与しません。
- **リスニング**：スパニングツリーでインターフェイスがフレーム転送に参加する必要があると判断された場合、ブロッキング ステートの次に最初に遷移するステート。
- **ラーニング**：インターフェイスはフレーム転送に関与する準備をしている状態です。
- **フォワーディング**：インターフェイスはフレームを転送します。
- **ディセーブル**：インターフェイスはスパニングツリーに含まれません。シャットダウンポートであるか、ポート上にリンクがないか、またはポート上でスパニングツリー インスタンスが稼働していないためです。

インターフェイスは次のように、ステートを移行します。

- 初期化からブロッキング
- ブロッキングからリスニングまたはディセーブル
- リスニングからラーニングまたはディセーブル
- ラーニングからフォワーディングまたはディセーブル
- フォワーディングからディセーブル

図 8-2 に、インターフェイスがステートをどのように移行するかを示します。

図 8-2 スパニングツリー インターフェイス ステート



アクセス ポイント/ブリッジで STP を有効にすると、イーサネット インターフェイスおよび無線インターフェイスは一度ブロッキング ステートになってから、リスニングおよびラーニングの一時的なステートに遷移します。スパニングツリーは、フォワーディング ステートまたはブロッキング ステートで各インターフェイスを安定させます。

スパニングツリー アルゴリズムがレイヤ 2 インターフェイスをフォワーディング ステートにする場合、次のプロセスが発生します。

1. インターフェイスをブロッキング ステートに遷移させるプロトコル情報をスパニングツリーが待っている間、そのインターフェイスはリスニング ステートの状態です。
2. スパニングツリーは転送遅延タイマーの満了を待ち、インターフェイスをラーニング ステートに移行させ、転送遅延タイマーをリセットします。
3. ラーニング ステートの間、アクセス ポイント/ブリッジが転送データベースのエンド ステーションの位置情報を学習しているとき、インターフェイスはフレーム転送をブロックし続けます。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行させ、このときラーニングとフレーム転送の両方が可能になります。

## ブロッキング ステート

ブロッキング ステートのインターフェイスは、フレーム転送に参加しません。初期化後、BPDU はアクセス ポイント/ブリッジのイーサネット ポートおよび無線ポートに送信されます。アクセス ポイント/ブリッジは、他のアクセス ポイント/ブリッジと BPDU 交換するまで、最初にスパニングツリー ルートとして機能します。この交換により、ネットワーク内のどのアクセス ポイント/ブリッジがスパニングツリー ルートになるかが決まります。ネットワークにアクセス ポイント/ブリッジが 1 つだけしかない場合、交換は行われず、転送遅延タイマーが切れた後にインターフェイスがリスニング ステートに遷移します。STP を有効にすると、インターフェイスは常にブロッキング ステートから開始されます。

ブロッキング ステートのインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。

- アドレスを学習しません。
- BPDU を受信します。



(注)

アクセスポイント/ブリッジの1つのポートがブロックされている場合、ブロードキャストパケットやマルチキャストパケットは同じアクセスポイント/ブリッジ上のフォワーディングポートに到達するため、ブリッジングロジックによって、ブロックポートでパケットがドロップされる前に、一時的にブロックポートがリスニングステートに切り替わることがあります。

## リスニングステート

リスニングステートは、インターフェイスがブロッキングステートの次に開始する最初のステートです。インターフェイスは、STPによってインターフェイスがフレーム転送に参加する必要があると判断された場合、このステートを開始します。

リスニングステートのインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

## ラーニングステート

ラーニングステートのインターフェイスは、フレーム転送に参加する準備を行います。インターフェイスはリスニングステートからラーニングステートに移行します。

ラーニングステートのインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

## フォワーディングステート

フォワーディングステートのインターフェイスは、フレームを転送します。インターフェイスはラーニングステートからフォワーディングステートに移行します。

フォワーディングステートのインターフェイスは次のように動作します。

- ポート上でのフレームの受信と受信したフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

## ディセーブルステート

ディセーブルステートのインターフェイスは、フレーム転送にもスパニングツリーにも参加しません。ディセーブルステートのインターフェイスは動作不能です。

無効のインターフェイスは次のように動作します。

- ポートで受信したフレームを廃棄します。

- アドレスを学習しません。
- BPDU を受信しません。

## STP 機能の設定

アクセス ポイント/ブリッジに STP を設定するには、3 つの主要な手順を完了させます。

1. 必要に応じて、インターフェイスおよびサブインターフェイスをブリッジ グループに割り当てます。
2. ブリッジ グループごとに STP を有効にします。
3. ブリッジ グループごとに STP の優先順位を設定します。

次の各項にはスパニングツリーの設定情報が含まれています。

- 「STP のデフォルト設定」 (P.8-9)
- 「STP の設定」 (P.8-10)
- 「STP の設定例」 (P.8-11)

## STP のデフォルト設定

STP はデフォルトでは無効に設定されています。表 8-2 に、STP を有効に設定したときのデフォルトの STP 設定を示します。

**表 8-2** STP を有効にしたときのデフォルトの STP 値

設定	デフォルト値
ブリッジプライオリティ	32768
ブリッジの最大経過時間	20
ブリッジの hello タイム	2
ブリッジの転送遅延	15
イーサネット ポートのパスコスト	19
イーサネット ポートの優先順位	128
無線ポートのパスコスト	33
無線ポートの優先順位	128

アクセス ポイント/ブリッジ上の無線インターフェイス、イーサネット インターフェイス、およびネイティブ VLAN は、デフォルトではブリッジ グループ 1 に割り当てられます。STP を有効にして、ブリッジ グループ 1 の優先順位を割り当てると、無線インターフェイス、イーサネット インターフェイス、およびプライマリ VLAN 上で STP が有効になり、これらのインターフェイスはブリッジ グループ 1 に割り当てられている優先順位を採用します。サブインターフェイスのブリッジ グループを作成し、そのブリッジ グループに異なる STP 設定を割り当てることができます。

## STP の設定

特権 EXEC モードから、次の手順に従ってアクセス ポイント/ブリッジに STP を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface { dot11radio number   fastethernet number }</code>	無線またはイーサネットのインターフェイスまたはサブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。 ファスト イーサネット インターフェイスは 0 です。
ステップ 3	<code>bridge-group number</code>	インターフェイスをブリッジ グループに割り当てます。ブリッジ グループには 1 ~ 255 の範囲で番号を付けることができます。
ステップ 4	<code>no bridge-group number spanning-disabled</code>	ブリッジ グループに対して STP を自動的に無効にするコマンドを抑制します。 <code>bridge n protocol ieee</code> コマンドを入力すると、STP がインターフェイス上で有効になります。
ステップ 5	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<code>bridge number protocol ieee</code>	ブリッジ グループに対して STP を有効にします。 <code>bridge-group</code> コマンドを使用して作成するブリッジ グループごとに STP を有効にする必要があります。
ステップ 7	<code>bridge number priority priority</code>	(任意) ブリッジ グループに優先順位を割り当てます。優先順位を低くすると、ブリッジがスパニングツリー ルートになる可能性が高くなります。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>show spanning-tree bridge</code>	入力内容を確認します。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。



## STP の設定例

次の設定例では、VLAN の使用する場合と使用しない場合それぞれで、ルートおよび非ルートのアクセス ポイント/ブリッジに STP を有効に設定する方法を示します。

- 「VLAN を使用しないルート ブリッジ」(P.8-11)
- 「VLAN を使用しない非ルート ブリッジ」(P.8-12)
- 「VLAN を使用するルート ブリッジ」(P.8-12)
- 「VLAN を使用する非ルート ブリッジ」(P.8-14)

### VLAN を使用しないルート ブリッジ

次に、VLAN が設定されていないルート ブリッジに STP を有効に設定する例を示します。

```
hostname master-bridge-south
ip subnet-zero
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid tsunami
authentication open
guest-mode
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
no cdp enable
infrastructure-client
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
!
interface BVI1
ip address 1.4.64.23 255.255.0.0
no ip route-cache
!
ip default-gateway 1.4.0.1
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 9000
!
line con 0
exec-timeout 0 0
line vty 0 4
login
line vty 5 15
login
!
end
```

## VLAN を使用しない非ルート ブリッジ

次に、VLAN が設定されていない非ルート ブリッジに STP を有効に設定する例を示します。

```
hostname client-bridge-north
ip subnet-zero
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid tsunami
authentication open
guest-mode
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role non-root
no cdp enable
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1 path-cost 40
!
interface BVI1
ip address 1.4.64.24 255.255.0.0
no ip route-cache
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 10000
!
line con 0
line vty 0 4
login
line vty 5 15
login
!
end
```

## VLAN を使用するルート ブリッジ

次に、VLAN が設定されているルート ブリッジに STP を有効に設定する例を示します。

```
hostname master-bridge-hq
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
bridge irb
!
interface Dot11Radio0
```

```
no ip address
no ip route-cache
!
ssid vlan1
vlan 1
infrastructure-ssid
authentication open
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
no cdp enable
infrastructure-client
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
no cdp enable
bridge-group 1
!
interface Dot11Radio0.2
encapsulation dot1Q 2
no ip route-cache
no cdp enable
bridge-group 2
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
bridge-group 3 path-cost 500
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
bridge-group 2
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
!
interface BVI1
ip address 1.4.64.23 255.255.0.0
no ip route-cache
!
ip default-gateway 1.4.0.1
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 9000
bridge 2 protocol ieee
bridge 2 priority 10000
bridge 3 protocol ieee
```

```
bridge 3 priority 3100
!
line con 0
exec-timeout 0 0
line vty 5 15
!
end
```

## VLAN を使用する非ルート ブリッジ

次に、VLAN が設定されている非ルート ブリッジに STP を有効に設定する例を示します。

```
hostname client-bridge-remote
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid vlan1
vlan 1
authentication open
infrastructure-ssid
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role non-root
no cdp enable
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
no cdp enable
bridge-group 1
!
interface Dot11Radio0.2
encapsulation dot1Q 2
no ip route-cache
no cdp enable
bridge-group 2
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
no cdp enable
bridge-group 3
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
```

```

bridge-group 1
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
bridge-group 2
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
bridge-group 3 path-cost 400
!
interface BVI1
ip address 1.4.64.24 255.255.0.0
no ip route-cache
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 10000
bridge 2 protocol ieee
bridge 2 priority 12000
bridge 3 protocol ieee
bridge 3 priority 2900
!
line con 0
line vty 5 15
!
end

```

## スパニングツリーステータスの表示

スパニングツリーステータスを表示するには、表 8-3 の特権 EXEC コマンドを 1 つまたは複数使用します。

表 8-3 スパニングツリーステータス表示用のコマンド

コマンド	目的
<b>show spanning-tree</b>	ネットワークのスパニングツリーに関する情報を表示します。
<b>show spanning-tree blocked-ports</b>	このブリッジのブロックポートのリストを表示します。
<b>show spanning-tree bridge</b>	このブリッジのステータスおよび設定を表示します。
<b>show spanning-tree active</b>	アクティブ インターフェイスに関するスパニングツリー情報だけを表示します。
<b>show spanning-tree root</b>	スパニングツリールートに関する情報の詳細な要約を表示します。
<b>show spanning-tree interface <i>interface-id</i></b>	指定したインターフェイスのスパニングツリー情報を表示します。
<b>show spanning-tree summary [totals]</b>	ポート ステータスの要約または STP ステート セクションの全行を表示します。

**show spanning-tree** 特権 EXEC コマンドのその他のキーワードの詳細は、このリリースの『Cisco Aironet IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。

## ■ スパニングツリー ステータスの表示



## ローカル認証サーバとしてのアクセスポイントの設定

この章では、アクセスポイントをローカル認証サーバとして設定して、小規模無線 LAN 用のスタンドアロン認証サーバとして機能させるか、またはバックアップ認証サービスを提供する方法について説明します。アクセスポイントはローカル認証サーバとして、最大 50 のクライアントデバイスに対して Light Extensible Authentication Protocol (LEAP; 拡張認証プロトコル) 認証、Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) 認証、および Media Access Control (MAC; メディア アクセス コントロール) ベースの認証を実行します。この章の内容は、次のとおりです。

- 「ローカル認証の概要」(P.9-2)
- 「ローカル認証サーバの設定」(P.9-2)

## ローカル認証の概要

802.1x 認証を使用すればさらにセキュリティを強化できる小規模な無線 LAN の多くは、RADIUS サーバにアクセスできません。802.1x 認証を使用する多くの無線 LAN でも、アクセスポイントはクライアント デバイスの認証を、遠隔地にある RADIUS サーバに依存しているため、認証トラフィックは WAN リンクを通過する必要があります。この WAN リンクに不具合が発生した場合、または何らかの理由でアクセスポイントが RADIUS サーバにアクセスできない場合、クライアント デバイスが必要とする作業が完全にローカルで行えるものであったとしても、このクライアント デバイスは無線ネットワークにアクセスできません。

WAN リンクやサーバが不具合を起こした場合にローカル認証サービスやバックアップ認証サービスを提供するため、アクセスポイントをローカル認証サーバとして動作するよう設定できます。このように設定したアクセスポイントは、LEAP 認証、EAP-FAST 認証、または MAC ベースの認証を使用して最大 50 の無線クライアント デバイスを認証できます。このアクセスポイントは毎秒最大 5 つの認証を実行できます。

ローカル認証サーバのアクセスポイントはクライアント ユーザ名とパスワードを使って手動で設定します。これは、このアクセスポイントはメインの RADIUS サーバとデータベースを同期しないからです。また、クライアントが使用できる VLAN や Service Set Identifier (SSID; サービスセット ID) リストを指定することもできます。



**(注)** 使用している無線 LAN にアクセスポイントが 1 箇所しかない場合、このアクセスポイントを 802.1x 認証サーバ、およびローカル認証サーバの両方として設定できます。ただし、ローカル認証サーバとして稼働するアクセスポイントにアソシエートされているユーザは、アクセスポイントがクライアント デバイスを認証する際、パフォーマンスが低下することに気づく場合があります。

アクセスポイントがメインサーバに到達できない場合には、ローカル認証サーバを使用するように設定できます。または、RADIUS サーバを所有していない場合に、ローカル認証サーバを使用するようにアクセスポイントを設定したり、アクセスポイントをメイン認証サーバとして設定したりできます。ローカル認証サーバをメインサーバのバックアップとして設定する場合、アクセスポイントは定期的にメインサーバへのリンクをチェックし、メインサーバへのリンクが復元された場合は、ローカル認証サーバの使用を自動的に停止します。



**注意**

認証サーバとして使用するアクセスポイントには、使用している無線 LAN に関する詳細な認証情報が含まれているため、このアクセスポイントを物理的に保護して、構成を守る必要があります。

## ローカル認証サーバの設定

この項では、アクセスポイントをローカル認証サーバとして設定する方法について、次の項に分けて説明します。

- 「ローカル認証サーバに対するガイドライン」(P.9-3)
- 「コンフィギュレーションの概要」(P.9-3)
- 「ローカル認証サーバアクセスポイントの設定」(P.9-4)
- 「他のアクセスポイントがローカル認証サーバを使用するための設定」(P.9-6)
- 「EAP-FAST の設定」(P.9-7)



- 「ロックされたユーザ名のロック解除」 (P.9-10)
- 「ローカル認証サーバ統計情報の表示」 (P.9-10)
- 「デバッグ メッセージの使用」 (P.9-11)

## ローカル認証サーバに対するガイドライン

アクセスポイントをローカル認証サーバとして設定する場合は、次のガイドラインに従ってください。

- サービスを提供するクライアント デバイスの数が少ないアクセスポイントを使用します。アクセスポイントを認証サーバとして使用すると、アソシエートされているクライアントデバイスに対するパフォーマンスが低下します。
- アクセスポイントを物理的に安全な場所に設置し、設定内容を保護してください。

## コンフィギュレーションの概要

ローカル認証サーバの設定は、大きく次の4つの手順に分けて実行します。

1. クライアント デバイスを認証するためにローカル認証サーバの使用が許可されているアクセスポイントのリストをローカル認証サーバに作成します。ローカル認証サーバを使用する各アクセスポイントは、ネットワーク アクセス サーバ (NAS) です。



**(注)** 使用するローカル認証サーバ アクセスポイントがクライアント デバイスにもサービスを提供する場合は、このローカル認証サーバ アクセスポイントを NAS として入力する必要があります。クライアントがこのローカル認証サーバ アクセスポイントとアソシエートしている場合、このアクセスポイントはクライアント認証のために自分自身を使用します。

2. ローカル認証サーバで、ユーザ グループを作成し、パラメータを各グループに対して適用されるように設定します (任意)。
3. ローカル認証サーバで、ローカル認証サーバが認証を許可された最大 50 の LEAP ユーザ、EAP-FAST ユーザ、または MAC アドレスのリストを作成します。



**(注)** ローカル認証サーバで実行する認証タイプを指定する必要はありません。認証サーバでは、そのユーザ データベースに記録されているユーザについて、LEAP 認証、EAP-FAST 認証、または MAC アドレス認証のいずれかが自動的に実行されます。

4. ローカル認証サーバを使用するアクセスポイントで、ローカル認証サーバを RADIUS サーバとして入力します。



**(注)** 使用するローカル認証サーバ アクセスポイントがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバの設定時に、このローカル認証サーバを RADIUS サーバとして入力する必要があります。クライアントがこのローカル認証サーバ アクセスポイントとアソシエートしている場合、このアクセスポイントはクライアント認証のために自分自身を使用します。

## ローカル認証サーバアクセスポイントの設定

特権 EXEC モードから、次の手順に従って、アクセスポイントをローカル認証サーバとして設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>radius-server local</code>	アクセスポイントをローカル認証サーバとして有効にし、認証サーバのコンフィギュレーション モードを開始します。
ステップ 4	<code>nas ip-address key shared-key</code>	<p>ローカル認証サーバを使用する装置のリストにアクセスポイントを追加します。ローカル認証サーバとその他のアクセスポイントの間の認証通信に使用される共有キーとアクセスポイントの IP アドレスを入力します。ローカル認証サーバを使用するアクセスポイントで、この共有キーを入力する必要があります。使用するローカル認証サーバがクライアント デバイスにもサービスを提供する場合は、ローカル認証サーバアクセスポイントを NAS として入力する必要があります。</p> <p>(注) キー スtring の先頭にある空白は無視されますが、キー内およびキーの末尾の空白は有効です。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。</p> <p>このステップを繰り返して、ローカル認証サーバを使用する各アクセスポイントを追加します。</p>
ステップ 5	<code>group group-name</code>	(任意) ユーザ グループ コンフィギュレーション モードを開始して、共有設定を割り当てることができるユーザ グループを設定します。
ステップ 6	<code>vlan vlan</code>	(任意) ユーザ グループのメンバーが使用する VLAN を指定します。アクセスポイントにより、グループメンバーがその VLAN に移動されます。その他の VLAN 割り当ては無効になります。グループに割り当てられる VLAN は 1 つだけです。
ステップ 7	<code>ssid ssid</code>	(任意) 最大 20 までの SSID を入力して、ユーザ グループのメンバーをそれらの SSID に制限します。アクセスポイントは、クライアントがアソシエートに使用した SSID が、このリスト内の SSID の 1 つと一致するかどうかをチェックします。SSID が一致しない場合、このクライアントのアソシエーションが解除されます。
ステップ 8	<code>reauthentication time seconds</code>	(任意) アクセスポイントがグループのメンバーを再認証するまでの秒数を入力します。この再認証により、ユーザには新しい暗号キーが与えられます。デフォルトの設定は 0 です。これは、グループのメンバーを再認証する必要がないことを表しています。

	コマンド	目的
ステップ 9	<code>block count count time { seconds   infinite }</code>	<p>(任意) パスワード攻撃から保護するために、ここで設定した回数だけ誤ったパスワードが入力されると、一定の期間、そのグループ メンバーをロックアウトできます。</p> <ul style="list-style-type: none"> <li>• <code>count</code> : ここで設定した回数だけ誤ったパスワードが入力されると、そのユーザ名がロックアウトされます。</li> <li>• <code>time</code> : ロックアウトの継続時間を秒単位で指定します。<b>infinite</b> と入力した場合、ロックされたユーザ名を管理者が手動で解除する必要があります。クライアント デバイスのロック解除手順については、「<a href="#">ロックされたユーザ名のロック解除</a>」(P.9-10) を参照してください。</li> </ul>
ステップ 10	<code>exit</code>	グループ コンフィギュレーション モードを終了し、認証サーバ コンフィギュレーション モードに戻ります。
ステップ 11	<code>user username { password   nhash } password [ group group-name ] [ mac-auth-only ]</code>	<p>ローカル認証サーバを使用した認証が許可されている LEAP ユーザおよび EAP-FAST ユーザを入力します。各ユーザについて、ユーザ名とパスワードを入力する必要があります。認証サーバ データベースでよく見かけられる、パスワードの NT 値しかわからない場合は、16 進数のストリングの NT ハッシュを入力することができます。</p> <p>MAC ベースの認証のためにクライアント デバイスを追加するには、ユーザ名とパスワードの両方にクライアントの MAC アドレスを入力します。このユーザ名とパスワードには、12 桁の 16 進数を入力します。数字の間にピリオドやダッシュは使用しません。たとえば、MAC アドレスが 0009.5125.d02b である場合は、ユーザ名とパスワードの両方に <code>00095125d02b</code> と入力します。</p> <p>ユーザを MAC 認証だけに制限するには、<code>mac-auth-only</code> と入力します。</p> <p>このユーザをユーザ グループに追加するには、グループ名を入力します。グループを指定しない場合、ユーザは特定の VLAN には割り当てられず、再認証するように強制されることはありません。</p>
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、3つのユーザグループと数人のユーザが存在する3つのアクセスポイントによって使用されるローカル認証サーバを設定する方法を表しています。

```

AP# configure terminal
AP(config)# radius-server local
AP(config-radiusrv)# nas 10.91.6.159 key 110337
AP(config-radiusrv)# nas 10.91.6.162 key 110337
AP(config-radiusrv)# nas 10.91.6.181 key 110337
AP(config-radiusrv)# group clerks
AP(config-radiusrv-group)# vlan 87
AP(config-radiusrv-group)# ssid batman
AP(config-radiusrv-group)# ssid robin
AP(config-radiusrv-group)# reauthentication time 1800
AP(config-radiusrv-group)# block count 2 time 600
AP(config-radiusrv-group)# group cashiers

```

```

AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user 00095125d02b password 00095125d02b group clerks mac-auth-only
AP(config-radsrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radsrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end

```

## 他のアクセスポイントがローカル認証サーバを使用するための設定

ローカル認証サーバを、他のサーバを追加するのと同じ方法で、アクセスポイント上のサーバリストに追加します。アクセスポイントにRADIUSサーバを設定する手順の詳細は、[第13章「RADIUSサーバとTACACS+サーバの設定」](#)を参照してください。



**(注)** 使用するローカル認証サーバアクセスポイントがクライアントデバイスにもサービスを提供する場合は、ローカル認証サーバが自分自身を使用してクライアントデバイスを認証するように設定する必要があります。

ローカル認証サーバを使用するアクセスポイントで、**radius-server host** コマンドを使用して、ローカル認証サーバをRADIUSサーバとして入力します。アクセスポイントがサーバの使用を試みる順序は、アクセスポイント設定でサーバを入力した順序と同じになります。RADIUSを使用するためにアクセスポイントを初めて設定している場合は、まず、メインRADIUSサーバを入力し、最後にローカル認証サーバを入力してください。



**(注)** 認証ポートには**1812**を、アカウントングポートには**1813**を入力する必要があります。ローカル認証サーバは、RADIUSアカウントングパケットを傍受するためにUDPポート**1813**をモニタします。アカウントングパケットはローカル認証サーバにより廃棄されますが、サーバがダウンしているとRADIUSクライアントが仮定しないように、確認応答パケットを送り返します。

**radius-server deadtime** コマンドを使って、アクセスポイントが応答のなかったサーバへ認証を試みるのを中止する間隔を設定します。これにより、要求がタイムアウトするまで待機しなくても、次に設定されたサーバを試行することができます。**dead**とマークされているサーバは、指定した期間(分単位)、その他の要求にもスキップされます。この期間は最高1440分(24時間)まで指定できます。

次の例では、2つのメインサーバとローカル認証サーバについて、サーバのデッドタイムを10分間に設定する方法を示します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
AP(config)# radius-server deadtime 10
```

この例では、メインサーバへのWANリンクに不具合が発生すると、LEAP対応クライアントデバイスがアソシエートされている場合、アクセスポイントは次の手順を実行します。

1. 最初のサーバを試し、複数回タイムアウトしたら、最初のサーバを **dead** とマークします。
2. 2番目のサーバを試し、複数回タイムアウトしたら、2番目のサーバを **dead** とマークします。
3. ローカル認証サーバを試し、正常に処理を終了します。

10分間の **dead-time** 間隔中に、他のクライアントデバイスが認証を行う必要がある場合、このアクセスポイントは最初の2台のサーバをスキップして、まず、ローカル認証サーバを試します。デッドタイム間隔後、アクセスポイントはメインサーバを使用して認証を試みます。デッドタイムを設定する場合、**dead** サーバをスキップする必要性と、WANリンクをチェックする必要性との間でバランスをとり、できるだけ早く、メインサーバの使用を再開する必要があります。

メインサーバがダウンしているときに、アクセスポイントがそのサーバの使用を試みるたびに、認証しようとしているクライアントデバイスが認証タイムアウトを報告する可能性があります。このクライアントデバイスは、メインサーバがタイムアウトし、アクセスポイントがローカル認証サーバの使用を試みている場合、再試行し、正常に処理を行います。予想されるサーバタイムアウトに対応するために、シスコクライアントデバイス上でタイムアウト値を延長することができます。

アクセスポイント設定からローカル認証サーバを削除するには、グローバルコンフィギュレーションコマンド **no radius-server host hostname | ip-address** を使用します。

## EAP-FAST の設定

ほとんどの無線LAN環境におけるEAP-FAST認証では、デフォルトの設定のままでも問題ありません。それでも、ネットワークの要件に合わせて、クレデンシャルのタイムアウト値、機関ID、およびサーバキーをカスタマイズすることはできます。

## PAC の設定

この項では、Protected Access Credential (PAC) を設定する方法について説明します。EAP-FASTクライアントデバイスがローカル認証サーバに対する認証を初めて試みると、ローカル認証サーバではそのクライアントのPACが生成されます。PACを手動で生成し、Aironet Client Utilityを使用してそのPACファイルをインポートすることもできます。

## PACの有効期限

PACに有効期間を設定し、さらにその有効期間が切れた後も暫定的にそのPACを有効にしておく猶予期間を指定できます。デフォルトでは、PACの有効期間は2日（1日のデフォルト期間プラス1日の暫定期間）です。ユーザグループに対しても有効期限と猶予期間の設定を適用できます。

PACに有効期限と猶予期間を設定するには、次のコマンドを使用します。

```
AP(config-radsrv-group)# [no] eapfast pac expiry days [grace days]
```

2～4095の範囲で日数を入力します。有効期限と猶予期間をリセットして無期限にするには、コマンドの **no** 形式を入力します。

次の例では、ユーザグループのPACに100日間の有効期限と2日間の猶予期間を設定します。

```
AP(config-radsrv-group)# eapfast pac expiry 100 grace 2
```

## PACの手動生成

ローカル認証サーバでは、EAP-FASTクライアントからの要求に応じて、そのクライアントのPACが自動的に生成されます。しかし、クライアントデバイスによっては、PACを手動で生成することが必要な場合もあります。コマンドを入力すると、ローカル認証サーバでPACファイルが生成され、指定したネットワーク上の場所にそのファイルが書き出されます。ユーザは、そのPACファイルをクライアントのプロファイルにインポートします。

PACを手動で生成するには、次のコマンドを使用します。

```
AP# radius local-server pac-generate filename username [password password] [expiry days]
```

PACのファイル名を入力するときは、ローカル認証サーバからそのPACファイルが書き出される場所へのフルパスを指定します（`tftp://172.1.1.1/test/user.pac` など）。パスワードはオプションです。指定しなかった場合、CCXクライアントに有効なデフォルトのパスワードが使用されます。失効もオプションです。指定しなかった場合、デフォルトの期間は1日です。

次の例では、ローカル認証サーバでユーザ名 *joe* のPACを生成し、パスワード *bingo* を設定してそのファイルを保護します。さらに、10日間の有効期限をそのPACに設定して、アドレス10.0.0.5のTrivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバにPACファイルを書き出します。

```
AP# radius local-server pac-generate tftp://10.0.0.5 joe password bingo expiry 10
```

## 機関IDの設定

すべてのEAP-FAST認証サーバは、Authority Identity（AID; 機関ID）で識別されます。認証対象のクライアントには、ローカル認証サーバからそのAIDが送信されます。受信したクライアントは、それに一致するAIDが自身のデータベースにあるか確認します。送信されたAIDが確認できない場合、クライアントは新しいPACを要求します。

ローカル認証サーバにAIDを割り当てるには、次のコマンドを使用します。

```
AP(config-radserv)# [no] eapfast authority id identifier
```

```
AP(config-radserv)# [no] eapfast authority info identifier
```

**eapfast authority id** コマンドにより、認証の際にクライアントデバイスで使用されるAIDが割り当てられます。

## サーバキーの設定

ローカル認証サーバでは、生成した PAC の暗号化、およびクライアントを認証する際の PAC の復号化にサーバキーが使用されます。ローカル認証サーバには、プライマリキーとセカンダリキーという2種類のキーが保持されていますが、PACの暗号化ではプライマリキーが使用されます。デフォルトでは、プライマリキーとしてデフォルト値が使用されます。セカンダリキーは、設定しない限り、使用されません。

クライアントの PAC を受信したローカル認証サーバは、プライマリキーを使用してその PAC を復号化しようとします。プライマリキーによる復号化に失敗した場合、セカンダリキーが設定されていれば、それを使用して PAC を復号化しようとします。復号化に失敗した認証サーバでは、その PAC は無効として拒否されます。

サーバキーを設定するには、次のコマンドを使用します。

```
AP(config-radsrv)# [no] eapfast server-key primary {[auto-generate] | [ [0 | 7] key]}
```

```
AP(config-radsrv)# [no] eapfast server-key secondary [0 | 7] key
```

キーには、最大 32 桁の 16 進数を設定できます。暗号化されていないキーを入力するには、キーの前に **0** を入力します。暗号化されているキーを入力するには、キーの前に **7** を入力します。ローカル認証サーバをデフォルトの設定にリセットするには、コマンドの **no** 形式を使用します。これにより、プライマリキーとしてデフォルト値が使用されるようになります。

## アクセスポイントのクロックが原因で発生する PAC の失敗

ローカル認証サーバでは、PACの生成とPACの有効性確認の両方でアクセスポイントのクロックが使用されています。ただし、アクセスポイントのクロックに依存することで、PACの失敗が発生することがあります。

NTPサーバから時間設定を取得しているローカル認証サーバのアクセスポイントの場合、起動してからNTPサーバに同期するまでに若干の時間がかかります。この間、そのアクセスポイントでは、自身のデフォルトの時間設定が使用されることとなります。このときにローカル認証サーバでPACが生成されていると、NTPサーバから新しい時間設定がアクセスポイントに取得された場合に、このPACが期限切れになることがあります。また、アクセスポイントの起動からNTP同期までの間にEAP-FASTクライアントが認証を試みると、ローカル認証サーバではそのクライアントのPACが無効として拒否されることがあります。

さらに、NTPサーバから時間設定を取得していないローカル認証サーバが頻繁にリブートする環境の場合、そのローカル認証サーバで生成されたPACが、有効期限を過ぎても期限切れにならないことがあります。アクセスポイントのクロックは、アクセスポイントがリブートするたびにリセットされます。その結果、クロックの経過時間が、PACの有効期間に達しないこととなります。

## ローカル認証サーバにおける認証タイプの制限

ローカル認証サーバのアクセスポイントでクライアントデバイスに対して実行できる認証は、デフォルトでLEAP認証、EAP-FAST認証、およびMACベースの認証です。ただし、ローカル認証サーバが実行できる認証タイプを1～2種類に制限できます。認証サーバの認証タイプを1種類に制限するには、次のように認証コマンドの **no** 形式を使用します。

```
AP(config-radsrv)# [no] authentication [eapfast] [leap] [mac]
```

デフォルトではすべての認証タイプが有効なため、コマンドの **no** 形式を使用して認証タイプを無効にします。たとえば、認証サーバでLEAP認証だけを実行するには、次のコマンドを入力します。

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

## ロックされたユーザ名のロック解除

ロックアウト時間が満了する前、またはロックアウト時間が `infinite` に設定されている場合でもユーザ名のロックを解除できます。ロックされたユーザ名のロックを解除するには、特権 EXEC モードに設定されているローカル認証サーバ上で、次のコマンドを入力します。

```
AP# clear radius local-server user username
```

## ローカル認証サーバ統計情報の表示

特権 EXEC モードで、次のコマンドを入力して、ローカル認証サーバが収集した統計情報を表示します。

```
AP# show radius local-server statistics
```

次の例は、ローカル認証サーバ統計情報を示しています。

```
Successes           : 0           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Unknown NAS         : 0           Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes           : 0           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Corrupted packet    : 0           Unknown RADIUS message : 0
No username attribute : 0       Missing auth attribute : 0
Shared key mismatch : 0           Invalid state attribute: 0
Unknown EAP message : 0           Unknown EAP auth type : 0
Auto provision success : 0       Auto provision failure : 0
PAC refresh         : 0           Invalid PAC received  : 0

Username            Successes  Failures  Blocks
nicky                0          0         0
jones                 0          0         0
jsmith                0          0         0
Router#sh radius local-server statistics
Successes           : 1           Unknown usernames   : 0
Client blocks       : 0           Invalid passwords   : 0
Unknown NAS         : 0           Invalid packet from NAS: 0
```

統計情報の最初のセクションは、ローカル認証サーバからの累積統計情報を示しています。

2 番目のセクションは、ローカル認証サーバを使用する権限を持つ各アクセスポイント (NAS) の統計情報を表示しています。このセクションの EAP-FAST 統計情報には、次の情報が記録されています。

- Auto provision success : 自動的に生成された PAC の数
- Auto provision failure : 無効なハンドシェイク パケットが原因で、あるいは無効なユーザ名またはパスワードが原因で生成されなかった PAC の数
- PAC refresh : クライアントによって更新された PAC の数



- **Invalid PAC received** : 受信した PAC のうち、期限切れだったもの、認証サーバで復号化できなかったもの、および認証サーバのデータベースに記録されていないクライアント ユーザ名に割り当てられていたものの合計数

この3番目のセクションには、個々のユーザの統計情報が表示されます。ユーザがブロックされていて、ロックアウト時間が **infinite** に設定されている場合、このユーザの統計行の末尾には **blocked** と表示されます。ロックアウト時間が **infinite** ではない場合、この行の末尾には **Unblocked in x seconds** と表示されます。

ローカル認証サーバ統計情報を 0 にリセットするには、次の特権 EXEC モード コマンドを使用します。

```
AP# clear radius local-server statistics
```

## デバッグ メッセージの使用

ローカル認証サーバに対するデバッグ メッセージの表示を制御するには、特権 EXEC モードで次のコマンドを入力します。

```
AP# debug radius local-server { client | eapfast | error | packets }
```

このデバッグ情報を表示するには、次のコマンド オプションを使用します。

- 失敗したクライアント認証に関連するエラー メッセージを表示するには、**client** オプションを使用します。
- EAP-FAST 認証に関連するエラー メッセージを表示するには、**eapfast** オプションを使用します。特定のデバッグ情報を選択するには、次のサブオプションを使用します。
  - **encryption** : 受信されたパケットおよび送信されたパケットの暗号化と複合化に関する情報が表示されます。
  - **events** : すべての EAP-FAST イベントに関する情報が表示されます。
  - **pac** : PAC の生成や検証など、PAC に関連するイベントの情報が表示されます。
  - **pkts** : EAP-FAST クライアントとの間で送受信されたパケットが表示されます。
- ローカル認証サーバに関連するエラー メッセージを表示するには、**error** オプションを使用します。
- 送受信された RADIUS パケットの内容が表示されるようにするには、**packets** オプションを使用します。





## 暗号スイートと WEP の設定

---

この章では、Wi-Fi Protected Access (WPA) および Cisco Centralized Key Management (CCKM) 認証済みキー管理、Wired Equivalent Privacy (WEP)、高度暗号化規格 (AES) などの WEP 機能、メッセージ完全性チェック (MIC)、Temporal Key Integrity Protocol (TKIP)、およびブロードキャスト キー ローテーションを使用するために必要な暗号スイートの設定方法について説明します。この章の内容は、次のとおりです。

- 「暗号スイートと WEP の概要」(P.10-2)
- 「暗号スイートと WEP の設定」(P.10-3)

## 暗号スイートとWEPの概要

この項では、無線 LAN 上のトラフィックを WEP と暗号スイートを使って保護する仕組みについて説明します。

ラジオ局の受信範囲内にいる人すべてが、局の周波数にチューニングして信号を聞くことができるのと同様に、アクセスポイントの範囲内にあるすべての無線ネットワークング デバイスは、アクセスポイントの無線伝送を受信できます。WEP は、不正侵入者に対する第一の防衛ラインであるため、無線ネットワークに完全な暗号化を使用することを推奨します。

WEP 暗号化は、アクセスポイントとクライアントデバイス間の通信をスクランブルし、通信機密を維持します。アクセスポイントとクライアントデバイスはいずれも同じ WEP キーを使用して、無線信号の暗号化および復号化を行います。WEP キーは、ユニキャストおよびマルチキャストの両方のメッセージを暗号化します。ユニキャストメッセージは、ネットワーク上の1つのデバイスだけに送信されます。マルチキャストメッセージは、ネットワーク上の複数のデバイスに送信されます。

Extensible Authentication Protocol (EAP; 拡張認証プロトコル) 認証は 802.1x 認証とも呼ばれ、無線ユーザに動的な WEP キーを提供します。動的な WEP キーは、静的な、つまり変化のない WEP キーより安全性が高くなります。不正侵入者は、同じ WEP キーで暗号化されたパケットが多数送られてくるのを待つだけで、WEP キーを割り出す計算を実行し、そのキーを使ってネットワークに侵入できます。動的な WEP キーは頻繁に変化するため、不正侵入者は計算を実行してキーを割り出すことができなくなります。EAP とその他の認証タイプの詳細は、[第 11 章「認証タイプの設定」](#)を参照してください。

暗号スイートは、無線 LAN 上の無線通信を保護するように設計された暗号と完全性アルゴリズムのセットです。WPA または CCKM をイネーブルにするには、暗号スイートを使用する必要があります。暗号スイートは認証済みキー管理の使用を許可しながら WEP の保護を行うため、CLI で **encryption mode cipher** コマンドを使用するか、Web ブラウザ インターフェイスの暗号化ドロップダウンリストを使用して WEP を有効にすることを推奨します。TKIP を含む暗号スイートは、無線 LAN に最適なセキュリティを提供しますが、WEP だけを含む暗号スイートは、安全性が最も劣ります。

無線 LAN 上のデータトラフィックは、次のセキュリティ機能によって保護されます。

- AES-CCMP : 米国立標準技術研究所による *FIPS Publication 197* で定義されている高度暗号化規格 (AES) に基づいています。AES-CCMP は、128 ビット、192 ビット、および 256 ビットのキーを使用してデータの暗号化および復号化を行う対称ブロック暗号です。AES-CCMP は、WEP 暗号化よりも優れており IEEE 802.11i 規格で定義されています。



(注)

Cisco Aironet 1130 および 1230 シリーズ アクセスポイントは WPA2 をサポートしています。Cisco IOS ソフトウェアをリリース 12.3(2)JA 以降にアップグレードした Cisco Aironet 1100、1200、および 1300 シリーズ 802.11g 無線は WPA2 をサポートしています。



(注)

部品番号 AIR-RM21A または AIR-RM22A の Cisco Aironet 1200 シリーズの無線モジュールは WPA2 または AES をサポートしています。



(注)

Cisco 802.11n 無線では、正常な動作のために、暗号化が設定されていないか、AES-CCMP を設定する必要があります。

- **Wired Equivalent Privacy (WEP)** : WEP は 802.11 標準暗号アルゴリズムであり、もともとは有線 LAN で可能なレベルのプライバシーを、無線 LAN で実現できるように設計されたものです。しかし、基本の WEP 構造には不備な点があり、侵入者はそれほど苦勞することなく機密性を侵害できます。
- **Temporal Key Integrity Protocol (TKIP)** : TKIP は、WEP を実行するために構築された従来のハードウェア上で、利用可能な最善のセキュリティを達成するように設計された WEP 周辺の一組のアルゴリズムです。TKIP は WEP に対して、次の 4 つの点を改善しています。
  - weak-key (脆弱キー) 攻撃を阻止するための、パケットごとの暗号キー混合機能
  - リプレイ攻撃を検知するための、新しい IV キー作成ロジック
  - パケットの送信元と宛先の入れ替え (ビット フリップ 攻撃) や変更のような偽造を検出するための *Michael* と呼ばれる暗号メッセージ完全性チェック (MIC)
  - キー更新をほとんど不要にするための IV 長の拡張
- **Cisco Key Integrity Protocol (CKIP)** : IEEE 802.11i セキュリティ タスク グループによって提供された初期アルゴリズムに基づく、シスコの WEP キー置換技術です。
- **Cisco Message Integrity Check (CMIC)** : TKIP の *Michael* と同様、シスコのメッセージ完全性チェック メカニズムは、偽造攻撃を検出するように設計されています。
- **ブロードキャスト キー ローテーション (グループ キー更新とも呼ばれる)** : ブロードキャスト キー ローテーションにより、アクセス ポイントは最良のランダム グループ キーを生成でき、キー管理可能なクライアントすべてを定期的に更新できるようになります。Wi-Fi Protected Access (WPA) も、グループ キー更新の追加オプションを提供します。WPA の詳細は、「[WPA キー管理の使用](#)」(P.11-7) を参照してください。



(注) ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションは、キー管理 (動的 WEP (802.1x)、EAP を使用した WPA、または事前共有キーなど) を使用する場合のみサポートされます。

## 暗号スイートと WEP の設定

次の項では、暗号スイート、WEP、および MIC などの WEP 追加機能、TKIP、ブロードキャスト キー ローテーションの設定方法について説明します。

- 「[WEP キーの作成](#)」(P.10-4)
- 「[暗号スイートと WEP の有効化](#)」(P.10-6)
- 「[ブロードキャスト キー ローテーションの有効化と無効化](#)」(P.10-8)



(注) WEP、TKIP、MIC、およびブロードキャスト キー ローテーションは、デフォルトで無効に設定されています。

## WEP キーの作成



(注)

静的 WEP キーの設定は、静的 WEP を使用するクライアント デバイスをアクセス ポイントがサポートしなければならない場合にだけ必要となります。アクセス ポイントにアソシエートするすべてのクライアント デバイスがキー管理 (WPA、CCKM、または 802.1x 認証) を使用する場合は、静的 WEP キーを設定する必要はありません。

特権 EXEC モードから、次の手順に従って、WEP キーを作成し、キーのプロパティを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>encryption</code> <code>[vlan vlan-id]</code> <code>key 1-4</code> <code>size { 40   128 } encryption-key</code> <code>[ 0   7 ]</code> <code>[transmit-key]</code>	WEP キーを作成し、そのプロパティを設定します。 <ul style="list-style-type: none"> <li>• (任意) キーを作成する VLAN を選択します。</li> <li>• この WEP キーを配置するキー スロットの名前を指定します。VLAN ごとに最大 4 つの WEP キーを割り当てることができます。</li> <li>• キーを入力し、キーのサイズを 40 ビットか 128 ビットのいずれかに設定します。40 ビット キーには、10 の 16 進数が含まれ、128 ビット キーには、26 の 16 進数が含まれています。</li> <li>• (任意) このキーを暗号化するか (7)、または暗号化しないか (0) を指定します。</li> <li>• (任意) このキーを送信キーとして設定します。スロット 1 のキーは、デフォルトで送信キーとなります。</li> </ul> <p>(注) 静的 WEP を MIC (キーハッシュ) とともに設定する場合、アクセス ポイントおよびアソシエートされているクライアント デバイスは送信キーとして同じ WEP キーを使用する必要があり、そのキーは、アクセス ポイントとクライアントで同じキー スロットに設定されていなければなりません。</p> <p>(注) CMIC を使用した静的 WEP の設定はサポートされていません。</p> <p>(注) 認証済みキー管理などのセキュリティ機能を使用すると、WEP キーの設定を制限できます。WEP キーに影響を与える機能の一覧は、「<a href="#">WEP キーの制限</a>」(P.10-5) を参照してください。</p>

	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、VLAN 22 のスロット 3 に 128 ビット WEP キーを作成し、そのキーを送信キーとして設定する方法を示します。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456
transmit-key
ap1200(config-if)# end
```

## WEP キーの制限

表 10-1 は、それぞれのセキュリティ設定に基づいた WEP キーの制限の一覧を示しています。

表 10-1 WEP キーの制限

セキュリティ設定	WEP キーの制限
CCKM または WPA 認証済みキー管理	キー スロット 1 に WEP キーを設定できません。
LEAP または EAP 認証	キー スロット 4 に WEP キーを設定できません。
40 ビット WEP による暗号スイート	128 ビット キーを設定できません。
128 ビット WEP による暗号スイート	40 ビット キーを設定できません。
TKIP による暗号スイート	WEP キーを設定できません。
TKIP と 40 ビット WEP、または 128 ビット WEP による暗号スイート	WEP キーをキー スロット 1 と 4 に設定できません。
MIC による静的 WEP	アクセス ポイントとクライアント デバイスは、同じ WEP キーを送信キーとして使用する必要があります。また、このキーは、アクセス ポイントとクライアントの両方で同じキー スロットに設定されている必要があります。
ブロードキャスト キー ローテーション	ブロードキャスト キー ローテーションにより、スロット 2 と 3 のキーが上書きされます。  (注) ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションは、キー管理 (動的 WEP (802.1x)、EAP を使用した WPA、または事前共有キーなど) を使用する場合のみサポートされます。

## WEP キーの設定例

表 10-2 は、アクセス ポイントおよびアソシエートされるデバイスで機能する WEP キーの設定例を示しています。

表 10-2 WEP キーの設定例

キー スロット	アクセス ポイント		アソシエートされるデバイス	
	送信キー	キー値	送信キー	キー値
1	○	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	○	09876543210987654321fedcba
3	—	未設定	—	未設定
4	—	未設定	—	FEDCBA09876543211234567890

アクセス ポイントの WEP キー 1 は送信キーとして選択されているため、アソシエートされるデバイスの WEP キー 1 も同じ内容に設定する必要があります。アソシエートされるデバイスに設定されている WEP キー 4 は、送信キーとして選択されていないため、アクセス ポイントの WEP キー 4 を設定する必要はありません。



(注) MIC を有効にし、静的な WEP を使用する (いずれの EAP 認証も有効にしない) 場合は、アクセス ポイントと通信先のデバイスの両方で、データ送信用に同じ WEP キーを使用する必要があります。たとえば、MIC を有効にしたアクセス ポイントでスロット 1 のキーを送信キーとして使用する場合は、そのアクセス ポイントにアソシエートされるクライアント デバイスでも、同じキーをスロット 1 で使用し、これを送信キーとして選択する必要があります。

## 暗号スイートと WEP の有効化

特権 EXEC モードから、次の手順に従って暗号スイートを有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。



	コマンド	目的
ステップ 3	<pre> <b>encryption</b> [<b>vlan</b> <i>vlan-id</i>] <b>mode ciphers</b> {[<b>aes</b>   <b>aes-ccm</b>   <b>ckip</b>   <b>tkip</b>]} {[<b>wep128</b>   <b>wep40</b>]} </pre>	<p>必要な WEP 保護を含む暗号スイートを有効にします。表 10-3 は、設定する認証済みキー管理タイプと一致する暗号スイートを選択するためのガイドラインです。</p> <ul style="list-style-type: none"> <li>（任意）WEP および WEP 機能を有効にする VLAN を選択します。</li> <li>暗号オプションと WEP のレベルを設定します。TKIP は、128 ビットまたは 40 ビットの WEP と組み合わせることができます。</li> </ul> <p>(注) 2つの要素（TKIP と 128 ビット WEP など）からなる暗号スイートを有効にすると、2 番目の暗号はグループ暗号となります。</p> <p>(注) <b>ckip</b> を設定する場合は、Aironet 拡張機能も有効にする必要があります。Aironet 拡張機能を有効にするコマンドは、<b>dot11 extension aironet</b> です。</p> <p>(注) 静的 WEP は、<b>encryption mode wep</b> コマンドを使用して設定することもできます。ただし、<b>encryption mode wep</b> コマンドは、アクセス ポイントにアソシエートされているクライアントがキー管理に対応していない場合に限り使用してください。<b>encryption mode wep</b> コマンドの詳細は、『Cisco IOS Command Reference for Cisco Access Points and Bridges』を参照してください。</p> <p>(注) SSID に（TKIP + WEP 128 でも TKIP + WEP 40 でもない）暗号化 TKIP を設定する場合は、その SSID では WPA または CCKM キー管理を使用する必要があります。WPA または CCKM キー管理を有効にせずに暗号化 TKIP を使用した SSID では、クライアント認証が失敗します。</p> <p>(注) 暗号化モード <b>TKIP + WEP 128</b> または <b>TKIP + WEP 40</b> を設定するには、WPA キー管理をオプションとして設定する必要があります。</p>
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>copy running-config startup-config</b>	（任意）コンフィギュレーション ファイルに設定を保存します。

暗号スイートを無効にするには、**encryption** コマンドの **no** 形式を使用します。

## WPA または CCKM に一致する暗号スイート

WPA または CCKM 認証済みキー管理を使用するようにアクセス ポイントを設定する場合は、そのタイプの認証キー管理と互換性のある暗号スイートを選択する必要があります。表 10-3 は、WPA および CCKM と互換性のある暗号スイートを示しています。

表 10-3 WPA および CCKM と互換性のある暗号スイート

認証済みキー管理のタイプ	互換性のある暗号スイート
CCKM	<ul style="list-style-type: none"> <li>• encryption mode ciphers wep128</li> <li>• encryption mode ciphers wep40</li> <li>• encryption mode ciphers ckip</li> <li>• encryption mode ciphers cmic</li> <li>• encryption mode ciphers ckip-cmic</li> <li>• encryption mode ciphers tkip</li> <li>• encryption mode aes</li> </ul>
WPA	<ul style="list-style-type: none"> <li>• encryption mode ciphers tkip</li> <li>• encryption mode ciphers tkip wep128</li> <li>• encryption mode ciphers tkip wep40</li> <li>• encryption mode ciphers eas</li> </ul> <p>(注) WPA がオプションとして設定されている場合、encryption mode ciphers tkip wep128 および tkip wep-40 だけを使用できます。</p>



(注) キー管理として WPA および CCKM を使用している場合は、tkip および aes の暗号方式だけがサポートされます。キー管理として CCKM だけを使用している場合は、ckip、cmic、ckip-cmic、tkip、wep、および aes の各暗号方式がサポートされます。



(注) SSID に (TKIP + WEP 128 でも TKIP + WEP 40 でもない) 暗号化 TKIP を設定する場合は、その SSID では WPA または CCKM キー管理を使用する必要があります。WPA または CCKM キー管理を有効にせずに暗号化 TKIP を使用した SSID では、クライアント認証が失敗します。

WPA の詳細、および認証済みキー管理を設定する手順については、「[「WPA キー管理の使用」\(P.11-7\)](#)」を参照してください。

## ブロードキャスト キー ローテーションの有効化と無効化

ブロードキャスト キー ローテーションは、デフォルトでは無効になっています。



(注) ブロードキャスト キー ローテーションを有効にすると、静的 WEP を使用しているクライアント デバイスはアクセス ポイントを使用できなくなります。ブロードキャスト キー ローテーションは、キー管理 (動的 WEP (802.1x)、EAP を使用した WPA、または事前共有キーなど) を使用する場合のみサポートされます。

特権 EXEC モードから、次の手順に従ってブロードキャスト キー ローテーションを有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>broadcast-key change seconds [ vlan vlan-id ] [ membership-termination ] [ capability-change ]</code>	ブロードキャスト キー ローテーションを有効にします。 <ul style="list-style-type: none"> <li>ブロードキャスト キーのローテーションの間隔を秒単位で入力します。</li> <li>(任意) ブロードキャスト キー ローテーションを有効にする VLAN を入力します。</li> <li>(任意) WPA 認証済みキー管理を有効にすると、アクセス ポイントが WPA グループ キーを変更および配布するための条件を追加指定できます。 <ul style="list-style-type: none"> <li><b>Membership termination</b> : アクセス ポイントは、任意の認証済みクライアント デバイスがアクセス ポイントからアソシエーションを解除されたときに、新しいグループ キーを生成、配布します。この機能はアソシエートされたクライアントのグループ キーの機密性を保護します。しかし、ネットワーク上のクライアントが頻繁にローミングする場合、オーバーヘッドが生じる可能性があります。</li> <li><b>Capability change</b> : アクセス ポイントは、最後の非キー管理 (静的 WEP) クライアントがアソシエーションを解除されたときに、動的グループ キーを生成、配布します。また、最初の非キー管理 (静的 WEP) クライアントが認証するときに、静的に設定された WEP キーを配布します。WPA 移行モードでは、アクセス ポイントにアソシエートしている静的 WEP クライアントが存在しない場合は、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。</li> </ul> </li> </ul> <p>認証済みキー管理を有効にする方法の詳細については、<a href="#">第 11 章「認証タイプの設定」</a>を参照してください。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ブロードキャスト キー ローテーションを無効にするには、`encryption` コマンドの `no` 形式を使用します。

次の例は、VLAN 22 でブロードキャスト キー ローテーションを有効にし、ローテーション間隔を 300 秒に設定しています。

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# broadcast-key vlan 22 change 300
ap1200(config-if)# end
```



## 認証タイプの設定

---

この章では、アクセスポイントに認証タイプを設定する方法について説明します。この章の内容は、次のとおりです。

- 「[認証タイプの概要](#)」(P.11-2)
- 「[認証タイプの設定](#)」(P.11-10)
- 「[アクセスポイントとクライアントデバイスの認証タイプのマッチング](#)」(P.11-19)
- 「[ゲストアクセス管理](#)」(P.11-23)

## 認証タイプの概要

この項ではアクセスポイントに設定できる認証タイプについて説明します。認証タイプはアクセスポイントに設定する Service Set Identifier (SSID; サービスセット ID) に関連付けられます。同じアクセスポイントで異なるタイプのクライアントデバイスを使用する場合は、複数の SSID を設定します。複数の SSID の設定手順の詳細は、第7章「複数の SSID の設定」を参照してください。

無線クライアントデバイスがアクセスポイントを介してネットワークで通信を行うには、Open または Shared キー認証を使用してアクセスポイントから認証を得る必要があります。最大限のセキュリティを確保するために、クライアントデバイスは Media Access Control (MAC; メディアアクセスコントロール) アドレス認証または Extensible Authentication Protocol (EAP; 拡張認証プロトコル) 認証を使用してネットワークから認証を得る必要もあります。これらの認証タイプではネットワーク上の認証サーバが使用されます。



(注)

デフォルトでは、アクセスポイントは service-type 属性を `authenticate-only` に設定した状態で、再認証要求を認証サーバに送信します。ただし、Microsoft IAS サーバの中には、`authenticate-only` の service-type 属性をサポートしていないものがあります。ユーザの要件に応じて、service-type 属性を `dot11 aaa authentication attributes service-type login-user` または `dot11 aaa authentication attributes service-type framed-user` に設定してください。デフォルトでは、アクセス要求に応じてサービスタイプ「login」が送信されます。

アクセスポイントは、複数の認証メカニズム (タイプ) を同時に使用することができます。次の項でそれぞれの認証タイプについて説明します。

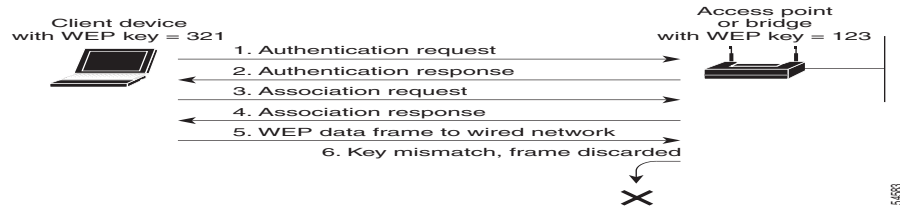
- 「アクセスポイントに対する Open 認証」(P.11-2)
- 「アクセスポイントに対する Shared Key 認証」(P.11-3)
- 「ネットワークに対する EAP 認証」(P.11-4)
- 「ネットワークに対する MAC アドレス認証」(P.11-5)
- 「MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ」(P.11-6)
- 「認証されたクライアントの CCKM の利用」(P.11-6)
- 「WPA キー管理の使用」(P.11-7)

## アクセスポイントに対する Open 認証

Open 認証では、すべてのデバイスに認証およびアクセスポイントとの通信の試みを許可します。Open 認証を使用すると、すべての無線デバイスがアクセスポイントから認証を受けられますが、デバイスが通信できるのは WEP キーがアクセスポイントの WEP キーに一致する場合だけです。WEP を使用しないデバイスは WEP を使用しているアクセスポイントに対して認証を試みません。Open 認証では、ネットワーク上の Remote Authentication Dial-In User Service (RADIUS) サーバは使用されません。

図 11-1 は、認証を試みるデバイスと、Open 認証を使用しているアクセスポイントとの認証シーケンスを示しています。この例では、デバイスの WEP キーがアクセスポイントのキーと一致しないため、認証はできても、データを転送できません。

図 11-1 Open 認証のシーケンス



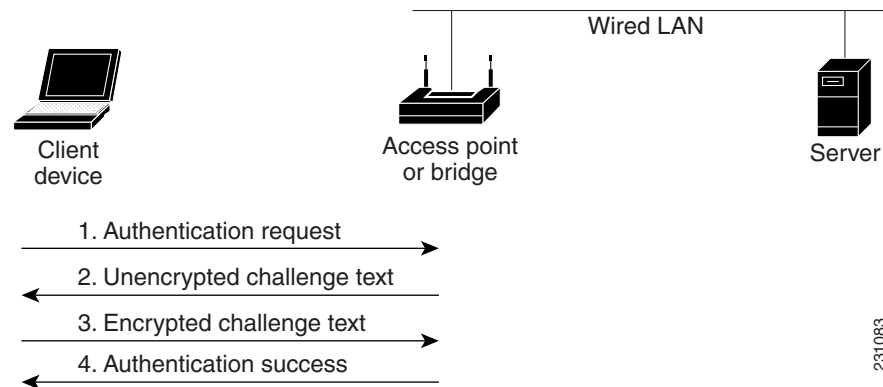
## アクセスポイントに対する Shared Key 認証

シスコでは、IEEE 802.11b 規格に準拠するために、Shared Key 認証も採用しています。ただし、Shared Key 認証にはセキュリティ上の弱点があるため、なるべく使用しないようにしてください。

Shared Key 認証では、アクセスポイントが、アクセスポイントとの通信を試みるすべてのデバイスに、暗号化されていない身元証明要求テキストストリングを送信します。認証を求めたデバイスは身元証明要求テキストを暗号化して、アクセスポイントに返送します。身元証明要求テキストが正しく暗号化されていれば、アクセスポイントはそのデバイスに認証を許可します。暗号化されていない身元証明要求も暗号化された身元証明要求もモニタできます。しかしそのために、アクセスポイントは、暗号化前のテキストと暗号化後のテキストを比較して WEP キーを計算する不正侵入者の攻撃に対し、無防備な状態になります。このような弱点により、Shared Key 認証は Open 認証よりも安全性が劣る場合があります。Open 認証と同様に、Shared Key 認証ではネットワーク上の RADIUS サーバは使用されません。

図 11-2 は、認証を試みるデバイスと、Shared Key 認証を使用しているアクセスポイントとの認証シーケンスを示しています。この例では、デバイスの WEP キーがアクセスポイントのキーと一致しているため、認証を受けて通信できます。

図 11-2 Shared Key 認証のシーケンス

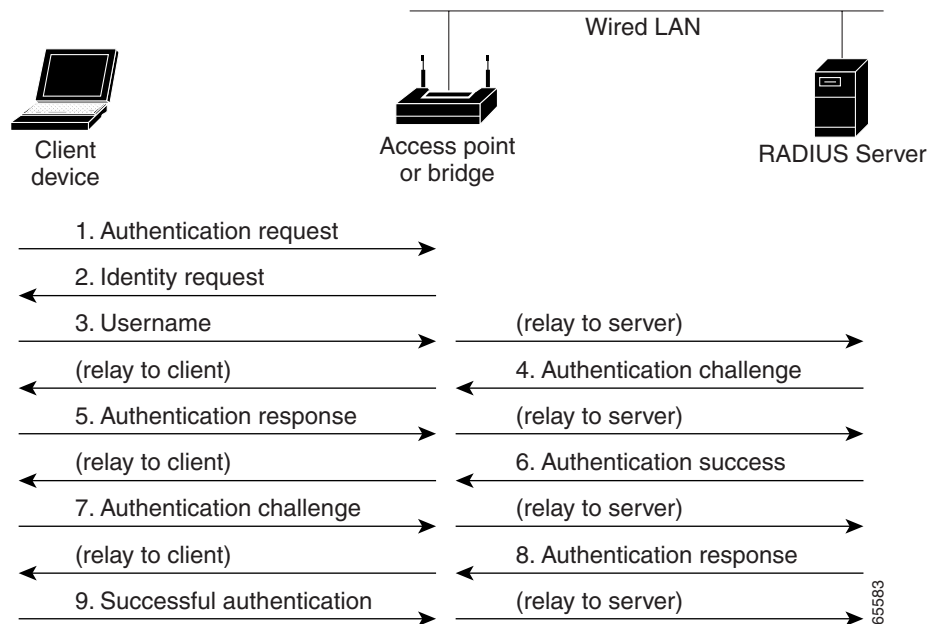


## ネットワークに対する EAP 認証

この認証タイプは、無線ネットワークに最高レベルのセキュリティを提供します。拡張認証プロトコル (EAP) を使用して EAP 互換の RADIUS サーバと対話することにより、アクセスポイントは、無線クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト WEP キーを引き出す補助をします。RADIUS サーバはアクセスポイントに WEP キーを送ります。アクセスポイントはこのキーを、クライアントに対して送受信するすべてのユニキャスト データ信号に使用します。さらに、アクセスポイントはブロードキャスト WEP キー (アクセスポイントの WEP キー スロット 1 に入力されたキー) をクライアントのユニキャストキーで暗号化して、クライアントに送信します。

アクセスポイントとクライアント デバイスで EAP を有効にすると、ネットワークに対する認証は、[図 11-3](#) に示す手順で実行されます。

図 11-3 EAP 認証のシーケンス



[図 11-3](#) の手順 1 ~ 9 では、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセスポイント経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザが入力したパスワードを一方方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、クライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、今度はクライアントが RADIUS サーバを認証します。

相互認証が終了すると、RADIUS サーバとクライアントは、クライアントに固有の、クライアントに適切なレベルのネットワーク アクセスを提供する WEP キーを決定します。これにより、有線のスイッチド セグメントのセキュリティレベルは、デスクトップのレベルに近づきます。クライアントはこのキーをロードして、ログインセッションでの使用に備えます。

ログインセッションでは、RADIUS サーバがセッションキーと呼ばれる WEP キーを暗号化して、有線 LAN 経由でアクセスポイントに送信します。アクセスポイントは、セッションキーを使用してブロードキャストキーを暗号化し、クライアントに送信します。クライアントは、



送信されてきたキーを、セッション キーを使用して復号化します。クライアントとアクセス ポイントは WEP を有効にし、セッション キーとブロードキャスト WEP キーを残りのセッションの間、すべての通信に対して使用します。

EAP 認証には複数のタイプがありますが、アクセス ポイントはどのタイプについても同じように機能します。つまり、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバ間の認証メッセージを中継します。アクセス ポイントで EAP を設定する方法の詳細は、「SSID への認証タイプの割り当て」(P.11-10) を参照してください。



(注) EAP 認証を使用する場合は、Open 認証または Shared Key 認証を選択できますが、この選択は必須ではありません。EAP 認証は、アクセス ポイントとネットワークの両方に対する認証を制御します。

## ネットワークに対する MAC アドレス認証

アクセス ポイントは、無線クライアント デバイスの MAC アドレスをネットワーク上の RADIUS サーバに中継します。サーバはそのアドレスを、許可される MAC アドレスのリストと照合します。MAC アドレスは不正侵入者でも偽造できるため、MAC ベースの認証は EAP 認証より安全性が劣ります。ただし、EAP 機能を持たないクライアント デバイスにとって、MAC ベースの認証は 1 つの代替認証方式となります。MAC ベースの認証の有効化の詳細は、「SSID への認証タイプの割り当て」(P.11-10) を参照してください。



ヒント

ネットワークに RADIUS サーバがない場合は、許可される MAC アドレスのリストをアクセス ポイントの [Advanced Security: MAC Address Authentication] ページで作成できます。このリストにない MAC アドレスを持つデバイスは、認証されません。

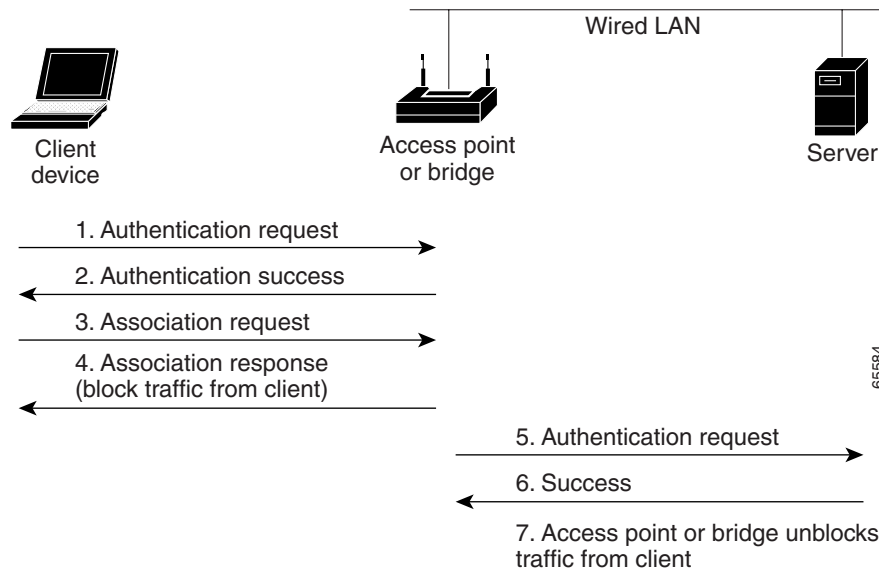


ヒント

無線 LAN 上の MAC 認証クライアントが頻繁にローミングする場合、アクセス ポイント上で MAC 認証キャッシュを有効にすることができます。MAC 認証キャッシングを使用すると、アクセス ポイントは認証サーバに要求を送信することなく MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが軽減されます。この機能を有効にする手順の詳細は、「MAC 認証キャッシングの設定」(P.11-15) を参照してください。

図 11-4 は、MAC ベースの認証のシーケンスを示しています。

図 11-4 MAC ベースの認証のシーケンス



## MAC ベースの認証、EAP 認証、および Open 認証の組み合わせ

MAC ベースの認証と EAP 認証を組み合わせることでクライアント デバイスを認証するように、アクセス ポイントを設定できます。この機能を有効にした場合、まず、802.11 Open 認証を使用してアクセス ポイントにアソシエートするクライアント デバイスが MAC 認証を行います。MAC 認証が成功すると、クライアント デバイスはネットワークに接続されます。MAC 認証が失敗した場合、EAP 認証を行います。このような認証の組み合わせを設定する方法の詳細は、「[SSID への認証タイプの割り当て](#)」(P.11-10) を参照してください。

## 認証されたクライアントの CCKM の利用

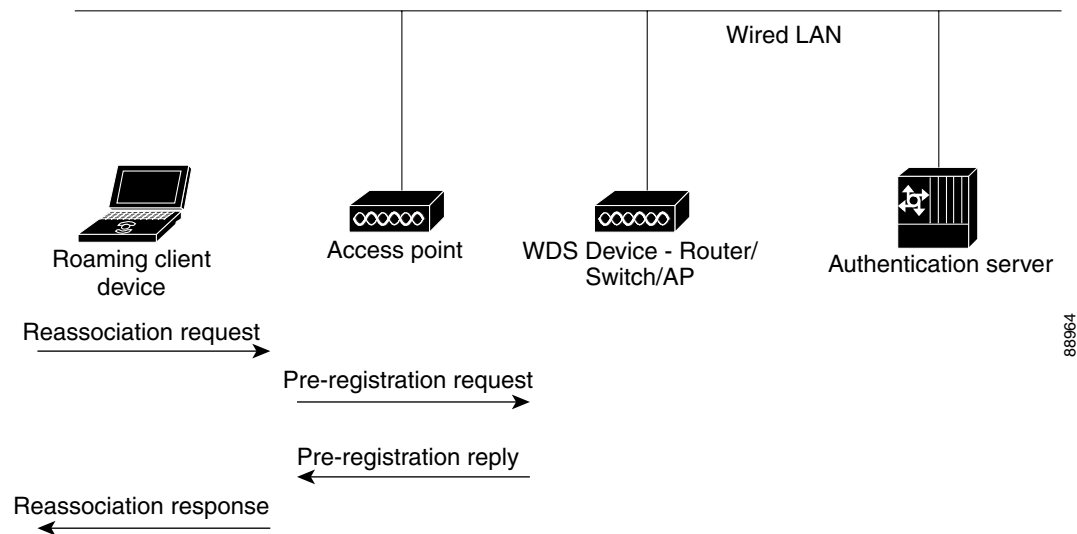
Cisco Centralized Key Management (CCKM) を使うと、認証されたクライアント デバイスは、1 つのアクセス ポイントから別のアクセス ポイントへ、再アソシエーションの際にほとんど遅延することなくローミングできます。ネットワーク上のアクセス ポイントは、Wireless Domain Service (WDS; 無線ドメイン サービス) を提供し、サブネット上の CCKM 対応クライアント デバイスに対してセキュリティ クレデンシャルのキャッシュを生成します。WDS アクセス ポイントのクレデンシャルのキャッシュは、CCKM 対応クライアント デバイスが新しいアクセス ポイントにローミングする際、再アソシエーションに必要な時間を大幅に短縮します。クライアント デバイスがローミングすると、WDS アクセス ポイントがクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送し、再アソシエーション プロセスが短縮されて、ローミングするクライアントと新しいアクセス ポイント間での 2 つの packets 交換だけになります。ローミングするクライアントは非常にすばやく再アソシエートするため、音声やその他の時間に敏感なアプリケーションで、知覚できるほどの遅延は生じません。アクセス ポイントで CCKM を有効にする方法の詳細は、「[SSID への認証タイプの割り当て](#)」(P.11-10) を参照してください。無線 LAN 上にある WDS アクセス ポイントの設定の詳細は、「[アクセス ポイントを潜在的な WDS デバイスとして設定する](#)」(P.12-10) を参照してください。



(注) RADIUS サーバによる VLAN 割り当て機能は、CCKM を利用した SSID グループのクライアントデバイスに対してはサポートされません。

図 11-5 は、CCKM を使用した再アソシエーションプロセスを示しています。

図 11-5 CCKM を使用したクライアント再アソシエーション



88964

## WPA キー管理の使用

Wi-Fi Protected Access (WPA) は、既存および将来の無線 LAN システムのデータ保護とアクセスコントロールの水準を大幅に向上させる、標準規格に基づく相互運用性の優れたセキュリティ拡張機能です。WPA は、現在策定中の IEEE 802.11i 規格のサブセットで、この規格と互換性があります。WPA では、データ保護に Temporal Key Integrity Protocol (TKIP) を使用し、認証済みキー管理に 802.1X を使用しています。

WPA キー管理は、2 つの相互排他的な管理タイプである WPA および WPA 事前共有キー (WPA-PSK) をサポートします。クライアントと認証サーバは、WPA を使用してキーを管理し、EAP 認証方式で相互認証を行い、Pairwise Master Key (PMK) を生成します。サーバは WPA を使用し、PMK を動的に生成してアクセスポイントに渡します。ただし、WPA-PSK を使用すると、クライアントとアクセスポイントの両方に事前共有キーが設定され、事前共有キーが PMK として使用されます。

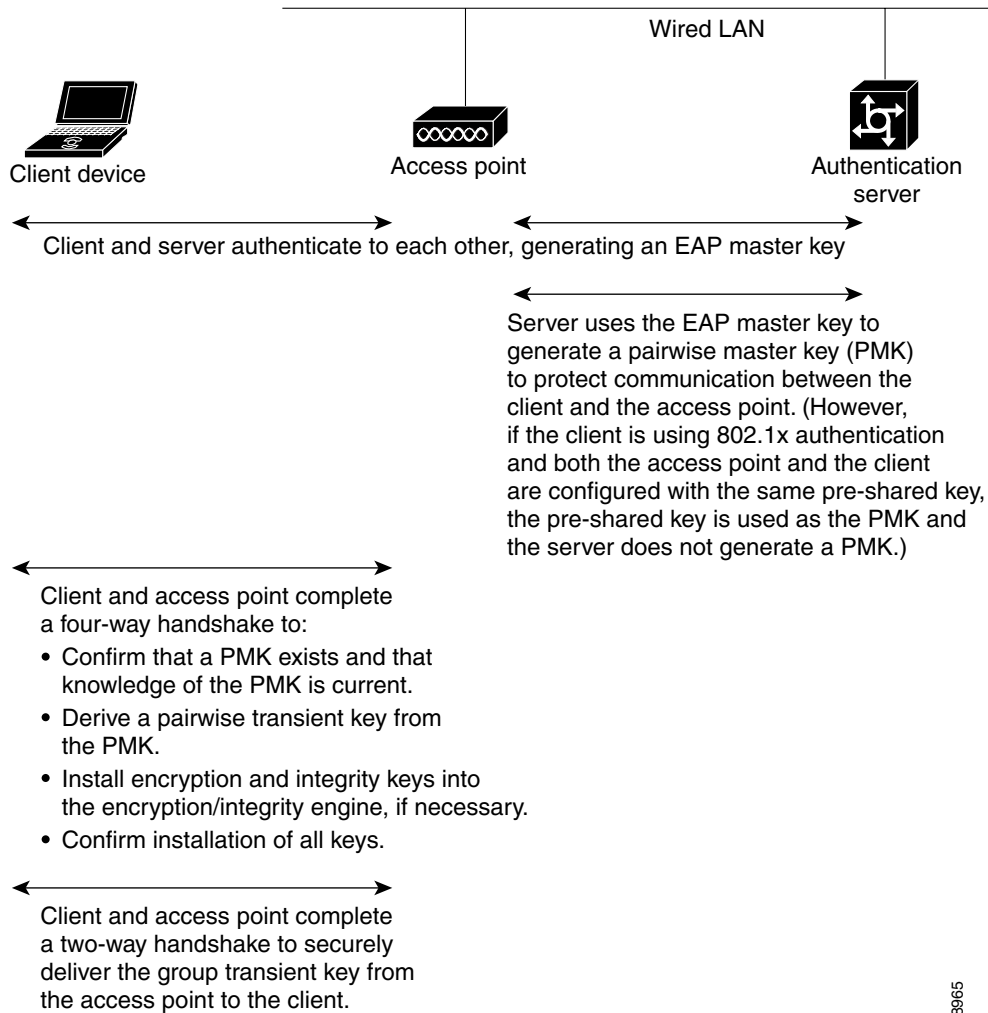


(注) WPA 情報エレメントでアドバタイズされる (さらに 802.11i でのアソシエーション中に決定される) ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、アクセスポイントとクライアントは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA プロトコルと CCKM プロトコルでは、最初の 802.11 暗号ネゴシエーションフェーズ以降での暗号スイートの変更は許可されていません。このような場合、クライアントデバイスと無線 LAN とのアソシエーションが解除されてしまいます。

WPA キー管理をアクセス ポイントで設定する方法の詳細は、「SSID への認証タイプの割り当て」(P.11-10) を参照してください。

図 11-6 は、WPA キー管理プロセスを示しています。

図 11-6 WPA キー管理プロセス



## WPA、CCKM、CKIP、および WPA-TKIP のソフトウェアおよびファームウェア要件

表 11-1 は、アクセス ポイントと Cisco Aironet クライアント デバイスが WPA および CCKM キー管理、Cisco Key Integrity Protocol (CKIP) および WPA-TKIP 暗号化プロトコルをサポートするために必要なファームウェアとソフトウェアの要件を示しています。

表 11-1 に挙げたセキュリティの組み合わせをサポートするには、Cisco Aironet アクセス ポイントおよび Cisco Aironet クライアント デバイスで、次のバージョンのソフトウェアとファームウェアを実行する必要があります。

- アクセス ポイント : Cisco IOS Release 12.2(13)JA 以降

- 340、350、および CB20A クライアント デバイス：次のコンポーネントを含むインストールウィザード バージョン 1.2
  - PC、LM、および PCI カード ドライバ バージョン 8.4
  - mini-PCI および CardBus PC カード ドライバ バージョン 3.7
  - Aironet Client Utility (ACU) バージョン 6.2
  - クライアント ファームウェア バージョン 5.30.13

表 11-1 WPA、CCKM、CKIP、WPA-TKIP のソフトウェアおよびファームウェア要件

キー管理 / 暗号化プロトコル	サードパーティ製ホスト サブリカント <sup>1</sup> の要 / 不要	サポートされているプラットフォーム オペレーティング システム
LEAP/CKIP (注) このセキュリティの組み合わせには 12.2(11)JA 以降が必要です。	No	Windows 95/98、Me、NT、2000、XP、Windows CE、Mac OS X、Linux、DOS
LEAP/CCKM + CKIP (注) このセキュリティの組み合わせには 12.2(11)JA 以降が必要です。	No	Windows 98、Me、NT、2000、XP、Windows CE
LEAP/CCKM + WPA-TKIP	No	Windows XP および 2000
LEAP/WPA (CCKM なし)	No	Windows XP および 2000
ホスト ベース EAP (PEAP、EAP-SIM、EAP-TLS など) / WPA (CCKM なし)	No <sup>2</sup>	Windows XP
ホスト ベース EAP (PEAP、EAP-SIM、EAP-TLS など) / WPA (CCKM なし)	Yes	Windows 2000
WPA-PSK モード	No <sup>2</sup>	Windows XP
WPA-PSK モード	Yes	Windows 2000

1. Funk Odyssey Client サブリカント バージョン 2.2、Meetinghouse Data Communications Aegis Client バージョン 2.1 など

2. Windows XP ではサードパーティ製のサブリカントは必要ありませんが、Windows XP Service Pack 1 および Microsoft サポート用修正プログラム 815485 をインストールする必要があります。

Cisco Aironet クライアント デバイスのセキュリティ設定の詳細については、『Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows』を参照してください。次の URL をクリックすると、『Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows』を参照できます。

[http://www.cisco.com/en/US/products/hw/wireless/ps4555/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html)



(注)

いずれかの無線インターフェイスまたは VLAN で、(TKIP + WEP 128 または TKIP + WEP 40 のような組み合わせではなく) TKIP だけの暗号スイートを設定する場合は、この無線または VLAN 上のすべての SSID を、WPA または CCKM のキー管理を使用するように設定する必要があります。無線または VLAN に対して TKIP を設定する場合、SSID にキー管理を設定しないと、SSID に対するクライアント認証が失敗します。

## 認証タイプの設定

この項では、認証タイプを設定する方法について説明します。設定タイプはアクセスポイントの SSID に割り当てます。複数の SSID の設定の詳細は、「複数の SSID の設定」(P.7-1) を参照してください。ここでは、次の内容について説明します。

- 「SSID への認証タイプの割り当て」(P.11-10)
- 「認証のホールドオフ、タイムアウト、間隔の設定」(P.11-16)
- 「802.1X サブリカントの EAP 方式プロファイルの作成と適用」(P.11-18)

## SSID への認証タイプの割り当て

特権 EXEC モードから、次の手順に従って SSID に認証タイプを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 ssid ssid-string</code>	<p>SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。</p> <p>SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。</p> <p>最初の文字に次の文字は使用できません。</p> <ul style="list-style-type: none"> <li>• 感嘆符 (!)</li> <li>• ポンド記号 (#)</li> <li>• セミコロン (;)</li> </ul> <p>次の文字は無効とされ、SSID には使用できません。</p> <ul style="list-style-type: none"> <li>• プラス記号 (+)</li> <li>• 閉じ大カッコ (])</li> <li>• スラッシュ (/)</li> <li>• 引用符 (")</li> <li>• タブ</li> <li>• 末尾のスペース</li> </ul>

コマンド	目的
<p>ステップ 3</p> <p><b>authentication open</b>  <code>[mac-address list-name [alternate]]</code>  <code>[[optional] eap list-name]</code></p>	<p>(任意) この SSID の認証タイプを Open に設定します。Open 認証では、すべてのデバイスに認証およびアクセスポイントとの通信の試みを許可します。</p> <ul style="list-style-type: none"> <li>(任意) SSID の認証タイプを MAC アドレス認証を使用する Open に設定します。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に MAC アドレス認証の実行を強制します。list-name には、認証方式リストを指定します。方式のリストの詳細は、次のリンクをクリックしてください。  <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2</a></li> </ul> <p>クライアント デバイスが MAC 認証か EAP 認証を使用してネットワークに接続するのを許可する場合は、<b>alternate</b> キーワードを使用します。いずれかの認証を得たクライアントはネットワークとの接続を許可されます。</p> <ul style="list-style-type: none"> <li>(任意) SSID の認証タイプを EAP 認証を使用する Open に設定します。アクセス ポイントは、すべてのクライアント デバイスに対して、ネットワーク接続を許可される前に EAP 認証の実行を強制します。list-name には、認証方式リストを指定します。</li> </ul> <p>クライアント デバイスが Open 認証か EAP 認証を使用してアソシエートおよび認証されるのを許可する場合は、<b>optional</b> キーワードを使用します。この設定は、特殊なクライアント アクセシビリティを必要とするサービスプロバイダーが主に使用します。</p> <p>(注) EAP 認証が設定されたアクセス ポイントは、アソシエートするすべてのクライアント デバイスに対して EAP 認証の実行を強制します。EAP を使用しないクライアント デバイスはアクセス ポイントを使用できません。</p>
<p>ステップ 4</p> <p><b>authentication shared</b>  <code>[mac-address list-name]</code>  <code>[eap list-name]</code></p>	<p>(任意) SSID の認証タイプを Shared Key に設定します。</p> <p>(注) 共有キーのセキュリティには欠陥があるため、使用しないことを推奨します。</p> <p>(注) Shared Key 認証を割り当てるのが可能な SSID は 1 つに限られます。</p> <ul style="list-style-type: none"> <li>(任意) SSID の認証タイプを MAC アドレス認証を使用する Shared Key に設定します。list-name には、認証方式リストを指定します。</li> <li>(任意) SSID の認証タイプを EAP 認証を使用する Shared Key に設定します。list-name には、認証方式リストを指定します。</li> </ul>



コマンド	目的
ステップ 5 <b>authentication network-eap</b> <i>list-name</i> <b>[mac-address list-name]</b>	<p>(任意) SSID の認証タイプを Network-EAP に設定します。拡張認証プロトコル (EAP) を使用して EAP 互換の RADIUS サーバと対話することにより、アクセスポイントは、無線クライアント デバイスと RADIUS サーバが相互認証を行って動的なユニキャスト WEP キーを引き出す補助をします。ただし、アクセスポイントはすべてのクライアント デバイスに対して EAP 認証を強制しません。</p> <ul style="list-style-type: none"> <li>• (任意) SSID の認証タイプを MAC アドレス認証を使用する Network-EAP に設定します。アクセスポイントにアソシエートするすべてのクライアント デバイスは、MAC アドレス認証の実行が要求されます。<i>list-name</i> には、認証方式リストを指定します。</li> </ul>
ステップ 6 <b>authentication key-management</b> <b>{ [wpa] [cckm] } [ optional ]</b>	<p>(任意) SSID の認証タイプを WPA または CCKM、あるいはその両方に設定します。 <b>optional</b> キーワードを指定すると、WPA または CCKM クライアント以外のクライアント デバイスもこの SSID を使用できます。 <b>optional</b> キーワードを指定しないと、この SSID を使用できるのは WPA または CCKM クライアント デバイスだけになります。</p> <p>SSID の CCKM 機能を有効にするには、Network-EAP 認証も有効にする必要があります。CCKM と Network EAP が SSID で有効な場合、クライアント デバイスが LEAP、EAP-FAST、PEAP/GTC、MSPEAP、EAP-TLS、および EAP-FAST を使用していれば SSID で認証できます。</p> <p>また、SSID の WPA 機能を有効にするには、Open 認証または Network-EAP 認証、あるいはその両方を有効にする必要があります。</p> <p>(注) 1 つの SSID で WPA と CCKM を両方とも有効にするには、<b>wpa</b> を先に入力し、次に <b>cckm</b> を入力します。WPA ではどのクライアントも認証を試行できますが、CCKM では音声クライアントだけが認証を試行できます。</p> <p>(注) CCKM または WPA を有効にするには、SSID の VLAN に対する暗号化モードを、いずれかの暗号スイート オプションに設定する必要があります。CCKM と WPA の両方を有効にするには、暗号化モードを、TKIP を含む暗号スイートに設定する必要があります。VLAN 暗号化モードの設定方法の詳細は、「暗号スイートと WEP の設定」(P.10-3) を参照してください。</p> <p>(注) 事前共有キーなしで SSID の WPA を有効にすると、キー管理タイプは WPA になります。事前共有キーを設定して WPA を有効にすると、キー管理タイプは WPA-PSK になります。事前共有キーの設定手順については、「追加の WPA の設定」(P.11-14) を参照してください。</p>



	コマンド	目的
ステップ 7	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

SSID を無効にする場合、または SSID 機能を無効にする場合は、SSID コマンドの **no** 形式を使用します。

次の例では、SSID *batman* の認証タイプを、CCKM 認証済みキー管理を使用した Network-EAP に設定します。batman SSID を使用するクライアント デバイスは、adam サーバリストを使って認証します。認証後、CCKM 対応クライアントは CCKM を使って迅速に再アソシエートできます。

```
ap1200# configure terminal
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

## WPA 移行モードの設定

WPA 移行モードにより、次に挙げるタイプのクライアント デバイスを、同じ SSID を使用してアクセス ポイントにアソシエートさせることができます。

- TKIP と認証済みキー管理に対応した WPA クライアント
- 認証済みキー管理には対応しているが TKIP には対応していない 802.1X-2001 クライアント (従来の LEAP クライアント、TLS を使うクライアントなど)
- TKIP にも認証済みキー管理にも対応してない静的 WEP クライアント

これら 3 つのタイプすべてのクライアントが同じ SSID を使用してアソシエートする場合、SSID 用のマルチキャスト暗号スイートは WEP でなければなりません。最初の 2 つのタイプのクライアントだけが同じ SSID を使用する場合、マルチキャスト キーは動的でもかまいませんが、静的 WEP クライアントが SSID を使用する場合、キーは静的でなければなりません。アクセス ポイントは自動的に静的グループ キーおよび動的グループ キー間を切り替えて、アソシエートされているクライアント デバイスに対応することができます。同じ SSID で 3 つのすべてのタイプのクライアントをサポートするには、キー スロット 2 または 3 に静的キーを設定する必要があります。

WPA 移行モードに SSID を設定するには、次の設定を行います。

- WPA (オプション)
- TKIP および 40 ビットまたは 128 ビット WEP を含む暗号スイート
- キー スロット 2 または 3 内の静的 WEP キー

次の例では、WPA 移行モードに移行するために SSID を設定します。

```
ap1200# configure terminal
ap1200(config-if)# ssid migrate
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config)# interface dot11radio 0
```

```
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# end
```

## 追加の WPA の設定

2つのオプションの設定を使ってアクセスポイントに事前共有キーを設定し、グループキーの更新頻度を調整します。

### 事前共有キーの設定

802.1X ベースの認証を使用できない無線 LAN 上の WPA をサポートするには、アクセスポイント上に事前共有キーを設定する必要があります。事前共有キーは ASCII 文字または 16 進数として入力できます。キーを ASCII 文字として入力する場合は、8 ～ 63 文字を入力します。アクセスポイントはこのキーを、『*Password-based Cryptography Standard (RFC2898)*』に記載されているプロセスを使用して展開します。キーを 16 進数として入力する場合は、64 桁の 16 進数を入力する必要があります。

### グループキー更新の設定

WPA プロセスの最後の段階で、アクセスポイントは認証されたクライアントデバイスにグループキーを配布します。次のオプションの設定を使って、クライアントのアソシエーションとアソシエーション解除をベースにして、グループキーを変更、配布するようにアクセスポイントを設定できます。

- **Membership-termination** : アクセスポイントは、任意の認証されたデバイスがアクセスポイントからアソシエーションを解除するときに、新しいグループキーを生成、配布します。この機能は、アソシエートされているデバイスに対してグループキーを秘匿しますが、ネットワーク上のクライアントがアクセスポイント間を頻繁にローミングする場合、オーバーヘッドトラフィックを生む可能性があります。
- **Capability change** : アクセスポイントは、最後の非キー管理（静的 WEP）クライアントがアソシエーションを解除されたときに、動的グループキーを生成、配布します。また、最初の非キー管理（静的 WEP）クライアントが認証するときに、静的に設定された WEP キーを配布します。WPA 移行モードでは、アクセスポイントにアソシエートしている静的 WEP クライアントが存在しない場合は、この機能により、キー管理が可能なクライアントのセキュリティが大幅に向上します。

特権 EXEC モードから、次の手順に従って、WPA 事前共有キーとグループキー更新オプションを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ssid ssid-string</code>	SSID の SSID コンフィギュレーション モードを開始します。
ステップ 3	<code>wpa-psk { hex   ascii } [ 0   7 ] encryption-key</code>	WPA を使用し、静的 WEP キーも使用するクライアントデバイス用の事前共有キーを入力します。  16 進数または ASCII 文字を使用して、キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合、アクセスポイントでキーが拡張されるように最低 8 文字の英数字または記号を入力する必要があります。ASCII 文字は 63 文字まで入力できます。

	コマンド	目的
ステップ 4	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。  5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 5	<code>ssid ssid-string</code>	ステップ 2 で定義した SSID を入力して、選択した無線インターフェイスに SSID を割り当てます。
ステップ 6	<code>exit</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>broadcast-key [ vlan vlan-id ] { change seconds } [ membership-termination ] [ capability-change ]</code>	<b>broadcast key rotation</b> コマンドを使用して、WPA グループ キーの追加の更新を設定します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、WPA および静的 WEP を使用するクライアント用の事前共有キーと、グループ キー更新オプションを設定する方法を示しています。

```
ap# configure terminal
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-termination capability-change
```

## MAC 認証キャッシングの設定

無線 LAN 上の MAC 認証クライアントが頻繁にローミングする場合、アクセス ポイント上で MAC 認証キャッシュを有効にすることができます。MAC 認証キャッシングを使用すると、アクセス ポイントは認証サーバに要求を送信することなく MAC アドレス キャッシュ内のデバイスを認証するため、オーバーヘッドが軽減されます。クライアント デバイスが認証サーバに対する MAC 認証を実行すると、アクセス ポイントがクライアントの MAC アドレスをキャッシュに追加します。

特権 EXEC モードから、次の手順に従って MAC 認証キャッシングを有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 aaa mac-authen filter-cache [timeout seconds]</code>	アクセス ポイントでの MAC 認証キャッシングを有効にします。  <b>timeout</b> オプションを使用して、キャッシュ内の MAC アドレスのタイムアウト値を設定します。値を 30 ~ 65555 秒の範囲で入力します。デフォルト値は 1800 (30 分) です。タイムアウト値を入力すると、MAC 認証キャッシングが自動的に有効になります。
ステップ 3	<code>exit</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 4	<b>show dot11 aaa mac-authen filter-cache [address]</b>	MAC 認証キャッシュ内のエントリを表示します。特定のクライアントのエントリを表示するには、クライアントの MAC アドレスを追加します。
ステップ 5	<b>clear dot11 aaa mac-authen filter-cache [address]</b>	キャッシュ内のすべてのエントリをクリアします。キャッシュから特定のクライアントをクリアするには、クライアントの MAC アドレスを追加します。
ステップ 6	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、タイムアウトを 1 時間に設定して MAC 認証キャッシングを有効にする方法を示しています。

```
ap# configure terminal
ap(config)# dot11 aaa mac-authen filter-cache timeout 3600
ap(config)# end
```

MAC 認証キャッシングを無効にするには、**dot11 aaa mac-authen filter-cache** コマンドの **no** 形式を使用します。次に例を示します。

```
no dot11 aaa authentication mac-authen filter-cache
```

または

```
no wlccp wds aaa authentication mac-authen filter-cache
```

## 認証のホールドオフ、タイムアウト、間隔の設定

特権 EXEC モードから、次の手順に従って、アクセス ポイントを介して認証を行うクライアント デバイスにホールドオフ時間、再認証間隔、認証タイムアウトを設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>dot11 holdoff-time seconds</b>	クライアント デバイスが認証失敗の後に次の認証を試みるまでに待機する時間を、秒数で入力します。ホールドオフ期間は、クライアントがログインに 3 回失敗したとき、つまりアクセス ポイントからの認証要求に 3 回応答できなかったときに開始されます。値を 1 ~ 65555 秒の範囲で入力します。

	コマンド	目的
ステップ 3	<code>dot1x timeout supp-response seconds [local]</code>	<p>認証に失敗するまでにアクセスポイントがクライアントの EAP/dot1x メッセージ返答を待つ時間を秒数で入力します。値を 1 ~ 120 秒の範囲で入力します。</p> <p>すでに設定されているタイムアウト値とは別のタイムアウト値を優先して送信するように RADIUS サーバを設定できます。アクセスポイントが RADIUS サーバの値を無視して、設定された値を使用するように設定するには、<b>local</b> キーワードを入力します。</p> <p>オプションの <b>no</b> キーワードを使用すると、タイムアウトが 30 秒のデフォルト状態にリセットされます。</p>
ステップ 4	<code>interface dot11radio { 0   1 }</code>	<p>無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。</p> <p>2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。</p> <p>5GHz 無線および 5GHz 802.11n 無線は 1 です。</p>
ステップ 5	<code>dot1x reauth-period { seconds   server }</code>	<p>認証されたクライアントに対して再認証するように強制する前に、アクセスポイントが待つ間隔を秒数で入力します。</p> <p>認証サーバが指定した再認証間隔を使用するようにアクセスポイントを設定する場合は、<b>server</b> キーワードを入力します。このオプションを使用する場合は、認証サーバを RADIUS 属性 27、Session-Timeout に設定します。この属性により、セッションまたはプロンプトが終了するまでにクライアントに提供されるサービスの最大秒数が設定されます。サーバは、クライアントデバイスが EAP 認証を実行するときにこの属性をアクセスポイントに送信します。</p> <p>(注) SSID に MAC アドレス認証と EAP 認証を両方設定した場合、サーバからクライアントデバイスの MAC 認証と EAP 認証両方の Session-Timeout 属性が送信されます。アクセスポイントでは、クライアントが最後に実行した認証の Session-Timeout 属性が使用されます。たとえば、クライアントが MAC アドレス認証を実行し、次に EAP 認証を実行した場合、アクセスポイントではサーバの EAP 認証の Session-Timeout 値が使用されます。いずれの Session-Timeout 属性を使用するのかという混乱を避けるため、認証サーバで MAC 認証と EAP 認証の両方に同じ Session-Timeout 値を設定します。</p>
ステップ 6	<code>countermeasure tkip hold-time seconds</code>	TKIP MIC 障害保持時間を設定します。アクセスポイントが 60 秒以内に 2 度の MIC 障害を検出した場合、そのインターフェイス上のすべての TKIP クライアントを保持期間の間ブロックします。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

値をデフォルトに戻すには、各コマンドの **no** 形式を使用します。

## 802.1X サブリカントの EAP 方式プロファイルの作成と適用

この項では、802.1X サブリカントに対応した EAP 方式リストのオプション設定について説明します。EAP 方式プロファイルを設定すると、サブリカントで利用可能な EAP 方式でも、サブリカントがその一部を確認応答しないようにできます。たとえば、RADIUS サーバが EAP-FAST と LEAP をサポートしている場合に、特定の設定下において、サーバは安全性の高い方式ではなく、LEAP を最初に使用する場合があります。優先される EAP 方式リストが定義されていない場合、サブリカントは LEAP をサポートしますが、EAP-FAST などの安全性の高い方式をサブリカントに強制するほうが有益です。



(注) 8021X サブリカントは、1130AG シリーズ、1240AG シリーズ、1250 シリーズ、および 1300 シリーズのアクセス ポイントで利用できます。1100 シリーズおよび 1200 シリーズのアクセス ポイントでは利用できません。

802.1X サブリカントの詳細については、「[クレデンシャル プロファイルの作成](#)」(P.4-28) を参照してください。

### EAP 方式プロファイルの作成

特権 EXEC モードから、次の手順に従って新しい EAP プロファイルを定義します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>eap profile profile name</code>	プロファイル名を入力します
ステップ 3	<code>description</code>	(任意) EAP プロファイルの説明を入力します
ステップ 4	<code>method fast</code>	許可する 1 つまたは複数の EAP 方式を入力します。  (注) EAP-GTC、EAP-MD5、および EAP-MSCHAPV2 は、サブパラメータとして表示されますが、トンネル型 EAP 認証の内部方式として使用され、プライマリ認証方式としては使用されません。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>copy running config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

コマンドを無効にする、またはデフォルトに設定するには、`no` コマンドを使用します。

現在利用可能な (登録済み) EAP 方式を表示するには、`show eap registrations method` コマンドを使用します。

既存の EAP セッションを表示するには、`show eap sessions` コマンドを使用します。

### ファスト イーサネット インターフェイスに対する EAP プロファイルの適用

この操作は一般にルート アクセス ポイントに適用されます。特権 EXEC モードから、次の手順に従って EAP プロファイルをファスト イーサネット インターフェイスに適用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface fastethernet 0</code>	アクセスポイントのファスト イーサネット ポートのインターフェイス コンフィギュレーション モードを開始します。  <code>interface fa0</code> を使用してファスト イーサネット コンフィギュレーション モードを開始することもできます。
ステップ 3	<code>dot1x eap profile profile</code>	プロファイルの事前設定プロファイル名を入力します。
ステップ 4	<code>end</code>	インターフェイス コンフィギュレーション モードを終了します。

## アップリンク SSID に対する EAP プロファイルの適用

この操作は一般的にリピータ アクセスポイントに適用されます。特権 EXEC モードから、次の手順に従って EAP プロファイルをアップリンク SSID に適用します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0 1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid</code>	アップリンク SSID を無線インターフェイスに割り当てます。
ステップ 4	<code>exit</code>	<code>configure terminal</code> モードに戻ります。
ステップ 5	<code>eap profile profile</code>	プロファイルの事前設定プロファイル名を入力します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>copy running config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## アクセスポイントとクライアント デバイスの認証タイプのマッチング

この項で説明する認証タイプを使用する場合は、アクセスポイントの認証設定がアクセスポイントにアソシエートするクライアント アダプタの認証設定に一致している必要があります。無線クライアント アダプタの認証タイプの設定手順の詳細は、『Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows』を参照してください。

表 11-2 は、各認証タイプに必要なクライアントとアクセスポイントの設定を示しています。



(注) Cisco Aironet 以外のクライアント アダプタの中には、**Open 認証 + EAP** を設定しないと、アクセスポイントに対して 802.1X 認証を実行しないものもあります。LEAP を使用する Cisco Aironet クライアントと LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP 認証** と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。

同様に、EAP-FAST を実行している Cisco Aironet 802.11a/b/g クライアント アダプタ (CB21AG および PI21AG) と EAP-FAST または LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP 認証** と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。



(注) 802.11n アクセスポイントを使用している場合、できるだけ 802.11n Wi-Fi カード ベンダーから使用中のカード向けの最新ドライバを入手してください。

表 11-2 クライアントとアクセスポイントのセキュリティ設定

セキュリティ機能	クライアントの設定	アクセスポイントの設定
静的 WEP キー (Open 認証)	WEP キーを作成し、Use Static WEP Keys と Open Authentication を有効化	WEP を設定して有効化し、SSID に対して Open 認証を有効化。
静的 WEP キー (Shared Key 認証)	WEP キーを作成し、Use Static WEP Keys と Shared Key Authentication を有効化	WEP を設定して有効化し、SSID に対して Shared Key 認証を有効化。
LEAP 認証	LEAP を有効化	WEP を設定して有効化し、SSID に対して Network-EAP を有効化。 <sup>1</sup>



表 11-2 クライアントとアクセスポイントのセキュリティ設定 (続き)

セキュリティ機能	クライアントの設定	アクセスポイントの設定
EAP-FAST 認証	EAP-FAST を有効化し、自動プロビジョニングを有効化または Protected Access Credential (PAC) ファイルをインポート	<p>WEP を設定して有効化し、SSID<sup>1</sup> に対して Network-EAP を有効化。</p> <p>ワイヤレスクライアントで EAP-FAST を使用する認証が設定されている場合は、Open 認証 + EAP も設定する必要があります。EAP を使用したオープン認証を設定しないと、次の GUI 警告メッセージが表示されます。</p> <p>「WARNING: Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」</p> <p>CLI を使用している場合は、次の警告メッセージが表示されます。</p> <p>「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」</p>
WPA による EAP-FAST 認証	<p>EAP-FAST および Wi-Fi Protected Access (WPA) を有効化し、自動プロビジョニングを有効化または PAC ファイルをインポート。</p> <p>WPA アクセスポイントと非 WPA アクセスポイントの両方にクライアントをアソシエートできるようにするには、両方のアクセスポイントに対して Allow Association を有効にします。</p>	<p>TKIP を含む暗号スイートの選択、WEP の設定および有効化、SSID に対する Network EAP および WPA の有効化。</p> <p>(注) WPA クライアントおよび非 WPA クライアントの両方で SSID を使用できるようにするには、オプションの WPA を有効にします。</p>
802.1X 認証と CCKM	LEAP を有効化	<p>暗号スイートを選択し、SSID に対して Network-EAP と CCKM を有効化。</p> <p>(注) 802.1X クライアントおよび非 802.1X クライアントの両方で SSID を使用できるようにするには、オプションの CCKM を有効にします。</p>

表 11-2 クライアントとアクセスポイントのセキュリティ設定 (続き)

セキュリティ機能	クライアントの設定	アクセスポイントの設定
802.1X 認証と WPA	いずれかの 802.1X 認証方式を有効化	暗号スイートを選択し、SSID に対して Open authentication と WPA を有効化 (Open 認証に加えて、または Open 認証の代わりに Network-EAP 認証を有効にすることもできます)。 <b>(注)</b> WPA クライアントと非 WPA クライアントの両方が SSID を利用できるようにするには、オプションの WPA を有効にします。
802.1X 認証と WPA-PSK	いずれかの 802.1X 認証方式を有効化	暗号スイートを選択し、SSID に対して Open authentication と WPA を有効化 (Open 認証に加えて、または Open 認証の代わりに Network-EAP 認証を有効にすることもできます)。WPA 事前共有キーを入力します。 <b>(注)</b> WPA クライアントと非 WPA クライアントの両方が SSID を利用できるようにするには、オプションの WPA を有効にします。
EAP-TLS 認証		
ACU を使用してカードを設定する場合	Host Based EAP と Use Dynamic WEP Keys を有効化 (ACU)、EAP タイプとして Enable network access control using IEEE 802.1X および Smart Card or other Certificate を選択 (Windows 2000 Service Pack 3 または Windows XP)	WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
Windows XP を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および Smart Card or other Certificate を選択	WEP を設定して有効化し、SSID に対して EAP と Open Authentication を有効化
EAP-MD5 認証		
ACU を使用してカードを設定する場合	WEP キーを作成し、Host Based EAP と Use Static WEP Keys を有効化 (ACU)、EAP タイプとして Enable network access control using IEEE 802.1X と MD5-Challenge を選択 (Windows 2000 Service Pack 3 または Windows XP)	WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化

表 11-2 クライアントとアクセスポイントのセキュリティ設定 (続き)

セキュリティ機能	クライアントの設定	アクセスポイントの設定
Windows XP を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および MD5-Challenge を選択	WEP を設定して有効化し、SSID に対して EAP と Open Authentication を有効化
PEAP 認証		
ACU を使用してカードを設定する場合	Host Based EAP と Use Dynamic WEP Keys を有効化 (ACU)、EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択 (Windows 2000 Service Pack 3 または Windows XP)	WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
Windows XP を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および PEAP を選択	WEP を設定して有効化し、SSID に対して Require EAP と Open authentication を有効化
EAP-SIM 認証		
ACU を使用してカードを設定する場合	Host Based EAP と Use Dynamic WEP Keys を有効化 (ACU)、EAP タイプとして Enable network access control using IEEE 802.1X および SIM Authentication を選択 (Windows 2000 Service Pack 3 または Windows XP)	安全な暗号化の WEP を設定して有効化し、SSID に対して EAP と Open authentication を有効化
Windows XP を使用してカードを設定する場合	EAP タイプとして Enable network access control using IEEE 802.1X および SIM 認証を選択	安全な暗号化の WEP を設定して有効化し、SSID に対して Require EAP と Open Authentication を有効化

1. Cisco Aironet 以外のクライアント アダプタの中には、**Open 認証 + EAP** を設定しないと、アクセスポイントに対して 802.1X 認証を実行しないものもあります。LEAP を使用する Cisco Aironet クライアントと LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP 認証** と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。同様に、EAP-FAST を実行している Cisco Aironet 802.11a/b/g クライアントアダプタ (CB21AG および PI21AG) と EAP-FAST または LEAP を使用する Cisco Aironet 以外のクライアントの両方が同じ SSID を使用してアソシエートできるようにするには、その SSID を **Network EAP 認証** と **Open 認証 + EAP** の両方に対応するように設定することが必要な場合があります。

## ゲスト アクセス管理

ゲスト アクセスでは、ゲストはインターネットと、ホスト エンタープライズのセキュリティを損なうことなくゲスト独自のエンタープライズにアクセスできます。

ゲスト アクセスは、次の方法で許可されます。

- [Web 認証 \(セキュア\)](#)
- [Web パススルー](#)

**Web 認証 (セキュア)**

Web 認証は、ゲストが有効なユーザ名とパスワードを入力するまで、自律 AP が IP トラフィック (DHCP および DNS 関連のパケット以外) をブロックできるようにするレイヤ 3 セキュリティ機能です。

Web 認証では、各ゲスト用に異なるユーザ名とパスワードを定義する必要があります。ユーザ名とパスワードを使用して、ゲストはローカル RADIUS サーバまたは外部 RADIUS サーバによって認証されます。

Web 認証を有効にするには、次の手順を実行します。

- 
- ステップ 1**    アクセス ポイントの GUI の [Security] ページを表示します。
  - ステップ 2**    [SSID Manager] を選択します。
  - ステップ 3**    [Web Authentication] チェックボックスをオンにします。
- 

特権 EXEC モードから、次のコマンドを使用して Web 認証を有効にします。

- Web 認証を SSID で有効にする場合は、次のようにします。Web 認証では Open 認証だけがサポートされるため、ネットワーク セキュリティのタイプは設定されません。
  - ap(config)# dot11 ssid guestssid
  - ap(config-ssid)# web-auth
  - ap(config-ssid)# authentication open
  - ap(config-ssid)# exit
- Web 認証を有効にする場合は、次のようにします。
  - ap(config)# ip admission name Web\_auth proxy http
  - ap(config)# interface dot11Radio 0
  - ap(config-if)# ip admission Web\_auth

**Web パススルー**

Web パススルーは、Web 認証と似ています。ただし、ゲストは認証情報を入力する必要はありません。

Web パススルーでは、ゲストがインターネットを初めて使用する時、使用ポリシー ページにゲストをリダイレクトします。ポリシーを受け入れると、アクセスが許可されます。アクセスポイントはゲストをポリシー ページにリダイレクトします。

Web 認証を有効にするには、次の手順を実行します。

- 
- ステップ 1**    アクセス ポイントの GUI の [Security] ページを表示します。
  - ステップ 2**    [SSID Manager] を選択します。
  - ステップ 3**    [Web Pass] チェックボックスをオンにします。
-

特権 EXEC モードから、次のコマンドを使用して、Web パススルーを有効にします。

- ap(config)# **ip admission name Web\_passthrough consent**
- ap(config)# **interface dot11Radio 0**
- ap(config-if)# **ip admission Web\_passthrough**



(注) VLAN がない場合に限り、Web 認証または Web パススルーがインターフェイスで動作します。SSID が VLAN にマップされている場合、IP admission Web\_auth または IP admission Web\_passthrough を VLAN に設定する必要があります。

## ゲスト アカウントの作成

新しいゲスト アカウントを作成するには、次の手順を実行します。

- 
- ステップ 1** アクセス ポイントの GUI の [Guest Management Services] ページを表示します。
  - ステップ 2** 新しいゲスト アカウントを作成するには、[New] を選択します。  
[Webauth Login] ページが表示されます。
  - ステップ 3** 次の値を入力してください。
    - Username
    - Password
    - Confirm Password
    - Lifetime
  - ステップ 4** [Generate Password] チェックボックスをオンにします。
  - ステップ 5** [Apply] をクリックします。

既存のユーザを削除するには、次の手順を実行します。

- 
- ステップ 1** アクセス ポイントの GUI の [Guest Management Services] ページを表示します。
  - ステップ 2** 削除するユーザ名を選択します。
  - ステップ 3** [Delete] をクリックします。  
確認メッセージが表示されます。
  - ステップ 4** [OK] をクリックしてユーザを削除するか、[Cancel] をクリックして変更をキャンセルします。

特権 EXEC モードから、CLI コマンドを使用してゲスト アカウントを作成するには、次のコマンドを使用します。

- ap(config)# **dot11 guest**
- ap(config-guest-mode)# **username Gues-1 lifetime 40 password t\_ksdgon**
- ap(config-guest-mode)# **username Gues-2 lifetime 35 password gp2**
- ap(config)# **exit**

ゲスト アクセスは最大で 24 日、最小で 5 分許可されます。

特権 EXEC モードから、ゲスト ユーザを削除するには、次のコマンドを使用します。

```
ap# clear dot11 guest-user Gues-1
```

特権 EXEC モードから、ゲスト ユーザを表示するには、次のコマンドを使用します。

```
ap# show dot11 guest-users
```

### ゲスト アクセス ページのカスタマイズ

ゲスト アクセス ページをカスタマイズして、カスタム ロゴやその他のイメージを表示できます。ゲスト ログイン ページは、編集してフラッシュにロードできます。カスタマイズされた WebAuth を選択する場合、ログイン ページ、成功ページ、期限切れと失敗のページをロードする必要があります。

ログイン ページ、成功ページ、期限切れと失敗のページをカスタマイズするには、次の手順を実行します。

- 
- ステップ 1**    アクセス ポイントの GUI の [Guest Management Services] ページを表示します。
  - ステップ 2**    [Webauth Login] を選択します。
  - ステップ 3**    ローカル サーバから、次のページを参照してアップロードします。
    - 成功ページ
    - 失敗ページ
    - 期限切れのページ
  - ステップ 4**    ファイル転送方式として FTP または TFTP を選択します。
  - ステップ 5**    [Username] を入力します。
  - ステップ 6**    [Password] を入力します。
  - ステップ 7**    [Allowed-In ACL Name] と [Allowed-Out ACL Name] を入力します。
  - ステップ 8**    変更を保存するには、[Close Window] をクリックします。
- 

特権 EXEC モードから、すべての編集済みファイルをフラッシュにロードするには、次のコマンドを使用します。

- ap(config)# ip auth-proxy proxy http login page file flash:web\_login.html
- ap(config)# ip auth-proxy proxy http success page file flash:web\_success.html
- ap(config)# ip auth-proxy proxy http failure page file flash:web\_fail.html
- ap(config)# ip auth-proxy proxy http login expired page file flash:web\_logout.html

ゲスト アクセス ページをカスタマイズするには、いくつかの ACL コマンドも実行する必要があります。特権 EXEC モードから、次の ACL コマンドを使用します。

- ap(config)# dot11 webauth allowed incoming webauth\_acl\_in outgoing webauth\_acl\_out
- ap(config)# ip access-list extended webauth\_acl\_in
- ap(config-ext-nacl)# permit tcp any host 40.40.5.10 eq www
- ap(config-ext-nacl)# permit tcp any host 40.40.5.10 eq 443
- ap(config-ext-nacl)# permit tcp any host 40.40.5.10 eq 443
- ap(config-ext-nacl)# exit

- ap(config)# **ip access-list extended webauth\_acl\_out**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**



(注)

acl-in および acl-out は、アクセス リストの名前です。これらの ACL を使用すると、マシンに保存されたイメージ ファイルをダウンロードして Web ページのカスタマイズに使用できます。

デフォルト ページには、ユーザ名、パスワード、[OK] ページだけが表示されます。

ゲスト アクセスは、次をサポートしていません。

- IPv6
- SNMP
- ローミング







## WDS、高速安全ローミング、無線管理、 および Wireless Intrusion Detection Service の設定

この章では、Wireless Domain Service (WDS; 無線ドメイン サービス)、クライアント デバイスの高速安全ローミング、無線管理、および Wireless Intrusion Detection Service (WIDS) のためにアクセス ポイントを設定する方法について説明します。この章の内容は、次のとおりです。

- 「WDS の概要」 (P.12-2)
- 「高速安全ローミングの概要」 (P.12-3)
- 「無線管理の概要」 (P.12-5)
- 「レイヤ 3 モビリティの概要」 (P.12-5)
- 「Wireless Intrusion Detection Service の概要」 (P.12-7)
- 「WDS の設定」 (P.12-8)
- 「高速安全ローミングの設定」 (P.12-21)
- 「管理フレーム保護の設定」 (P.12-25)
- 「無線管理の設定」 (P.12-30)
- 「WIDS に参加するようにアクセス ポイントを設定する」 (P.12-32)

スイッチの Wireless LAN Services Module (WLSM) に WDS を設定する方法は、『*Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*』を参照してください。

## WDS の概要

ネットワークに無線ドメイン サービスを設定すると、無線 LAN 上のアクセス ポイントは WDS デバイス (WDS デバイスとして設定されたアクセス ポイント、Integrated Services Router、またはスイッチ) を使用してクライアント デバイスに高速安全ローミングを提供し、無線管理に参加します。スイッチを WDS デバイスとして使用する場合、そのスイッチは Wireless LAN Services Module (WLSM) を備えている必要があります。WDS デバイスとして設定したアクセス ポイントは、最大 60 個のアクセス ポイントの参加をサポートします。WDS デバイスとして設定したサービス統合型ルータ (ISR) は、最大 100 個のアクセス ポイントの参加をサポートします。WLSM を備えたスイッチは、最大 600 個のアクセス ポイントの参加および最大 240 個のモビリティグループをサポートします。



(注) 単一のアクセス ポイントは、最大 16 個までのモビリティ グループをサポートします。

高速安全ローミングによって、クライアント デバイスがアクセス ポイント間をローミングするときにはすみやかに再認証でき、音声やその他の時間に敏感なアプリケーションにおける遅延を回避できます。

無線管理に参加しているアクセス ポイントは、無線環境に関する情報 (潜在的な不正アクセス ポイント、クライアント アソシエーション、アソシエーション解除など) を WDS デバイスに転送します。WDS デバイスはこの情報を集約し、ネットワーク上の Wireless LAN Solution Engine (WLSE; 無線 LAN ソリューション エンジン) デバイスに転送します。

## WDS デバイスの役割

WDS デバイスは無線 LAN 上で次のようないくつかの作業を実行します。

- WDS 機能をアドバタイズして、無線 LAN に最適な WDS デバイスの選択に参加します。WDS 用に無線 LAN を設定する場合は、1 つのデバイスをメインの WDS 候補として設定し、1 つ以上の追加デバイスをバックアップの WDS 候補として設定します。メインの WDS デバイスがオフラインになったら、バックアップの WDS デバイスの 1 つがその役割を引き継ぎます。
- サブネット中の全アクセス ポイントを認証して、それぞれと安全な通信チャネルを設定します。
- サブネット中のアクセス ポイントから無線データを収集して、データを集約し、これをネットワーク上の WLSE デバイスに転送します。
- 参加しているアクセス ポイントにアソシエートされているすべての 802.1X 認証クライアント デバイスに対するパススルーとして機能します。
- 動的キーを使用するサブネット中の全クライアント デバイスを登録して、それらに対してセッション キーを設定し、セキュリティ クレデンシャルをキャッシュします。クライアントが別のアクセス ポイントにローミングすると、WDS デバイスはクライアントのセキュリティ クレデンシャルを新しいアクセス ポイントに転送します。

表 12-1 は、WDS デバイスとして設定できるプラットフォーム (アクセス ポイント、ISR、または WLSM 装備スイッチ) でサポートされる参加アクセス ポイント数を示しています。

表 12-1 WDS デバイスでサポートされる参加アクセス ポイント数

WDS デバイスとして設定されたユニット	サポートされる参加アクセス ポイント数
クライアント デバイスからも接続できる アクセス ポイント	30
無線インターフェイスが無効になっている アクセス ポイント	60
サービス統合型ルータ (ISR)	100 (ISR プラットフォームに応じて異なる)
WLSM を備えたスイッチ	600

## WDS デバイスを使用したアクセス ポイントの役割

無線 LAN 上のアクセス ポイントは、次の動作において WDS デバイスと対話します。

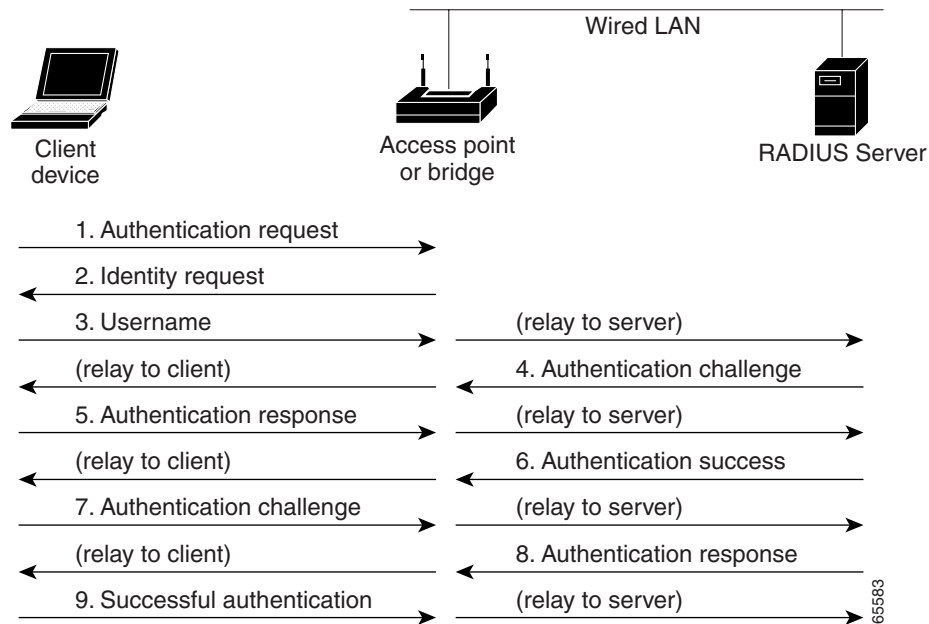
- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。
- 無線データを WDS デバイスに報告します。

## 高速安全ローミングの概要

多くの無線 LAN 内のアクセス ポイントは、システム全体においてアクセス ポイントからアクセス ポイントへローミングするモバイル クライアント デバイスに対応します。クライアント デバイスで稼働するアプリケーションの中には、異なるアクセス ポイントにローミングする場合に高速な再アソシエーションを必要とするものがあります。たとえば、音声アプリケーションでは、会話の遅延やギャップを防ぐために、シームレスなローミングが必要です。

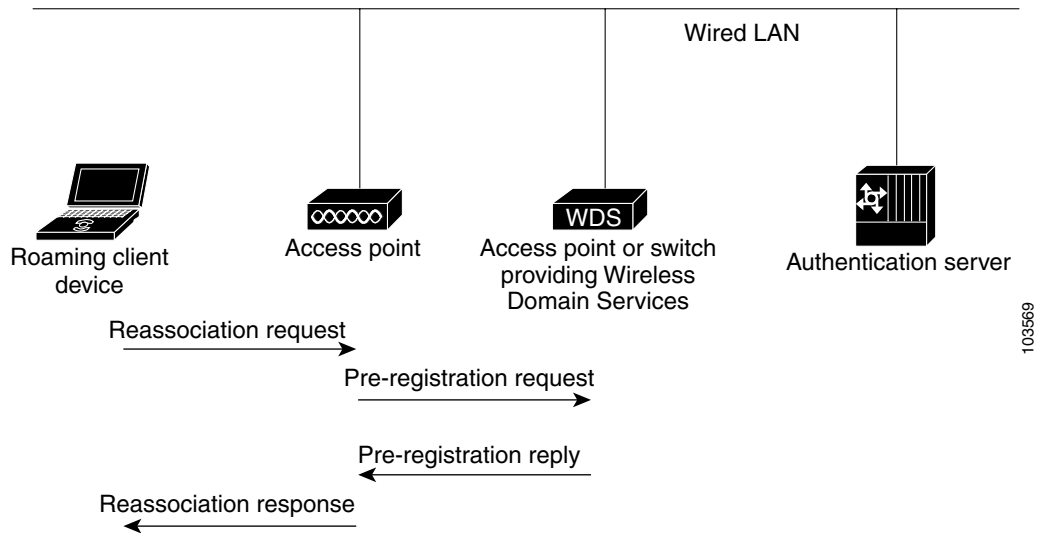
通常稼働時、LEAP 対応クライアント デバイスは、[図 12-1](#) に示すように、メイン RADIUS サーバとの通信を含む完全な LEAP 認証を実行することによって、新しいアクセス ポイントとの間で相互に認証を実行します。

図 12-1 RADIUS サーバを使ったクライアント認証



無線 LAN に高速安全ローミングを設定すれば、LEAP 使用可能クライアント デバイスはメイン RADIUS サーバを利用することなく、あるアクセス ポイントから別のアクセス ポイントへのローミングを行うことが可能です。Cisco Centralized Key Management (CCKM) を使用すると、無線ドメイン サービス (WDS) を提供するように設定されているデバイスは、RADIUS サーバの代わりにクライアントを短時間で認証するため、音声などの時間が重要なアプリケーションでは知覚できるほどの遅延は発生しません。図 12-2 は、CCKM を使用したクライアント認証を示しています。

図 12-2 CCKM と WDS アクセス ポイントを使用するクライアント再アソシエーション



WDS デバイスは、無線 LAN 上の CCKM 利用可能クライアント デバイスに対するクレデンシャルのキャッシュを維持します。CCKM 利用可能クライアントが、1つのアクセスポイントから別のアクセスポイントへローミングする場合、クライアントが新しいアクセスポイントへ再アソシエーションの要求を送信し、新しいアクセスポイントはその要求を WDS デバイスへ中継します。WDS デバイスはクライアントのクレデンシャルを新しいアクセスポイントに転送し、新しいアクセスポイントは再アソシエーション応答をクライアントに送信します。クライアントと新しいアクセスポイントとの間で渡されるパケットは2つだけであるため、再アソシエーションの時間が大幅に短縮されます。クライアントは再アソシエーション応答をユニキャストキーの生成にも使用します。高速安全ローミングをサポートするアクセスポイントを設定する方法の詳細は、「[高速安全ローミングの設定](#)」(P.12-21)を参照してください。

## 無線管理の概要

無線管理に参加しているアクセスポイントは、無線環境をスキャンし、潜在的な不正アクセスポイント、アソシエートされたクライアント、クライアントの信号強度、他のアクセスポイントからの無線信号などの無線情報に関するレポートを WDS デバイスに送信します。WDS デバイスは集約した無線データを、ネットワーク上の WLSE デバイスに転送します。無線管理に参加しているアクセスポイントは、近くのアクセスポイントに障害が発生した場合のカバレッジを提供するための無線 LAN の自己修復や自動設定調整についてもサポートしています。無線管理の設定手順の詳細は、「[無線管理の設定](#)」(P.12-30)を参照してください。

WLSE に関する資料を参照するには、次の URL をクリックします。

[http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/cscowork/ps3915/tsd_products_support_series_home.html)

このリンクをクリックすると、[Tools and Resources Downloads] ページが表示されます。WLSE の資料を参照するには、[Wireless LAN Management] を選択します。

## レイヤ3 モビリティの概要

WLSM をネットワーク上の WDS デバイスとして使用すると、特定のサブネットを1つ設定したり、有線スイッチ インフラストラクチャ全体に VLAN を設定したりしなくても、大規模なレイヤ3 ネットワークの任意の場所にアクセスポイントを設置できます。クライアント デバイスは、Multipoint GRE (mGRE; マルチポイント GRE) トンネルを使用して、異なるレイヤ3 サブネットに存在するアクセスポイントにローミングします。ローミングしているクライアントは、IP アドレスを変更しなくてもネットワークに接続されたままとなっています。

Wireless LAN Services Module (WLSM) を備えたスイッチに WDS を設定する方法については、『*Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide*』を参照してください。

レイヤ3 モビリティ無線 LAN ソリューションは、次のハードウェア コンポーネントおよびソフトウェア コンポーネントで構成されています。

- WDS に参加している 1040、1100、1130、1200、1240、および 1260 シリーズのアクセスポイント
- スーパーバイザ モジュールおよび WDS デバイスとして設定されている WLSM を備えた Catalyst 6500 スイッチ

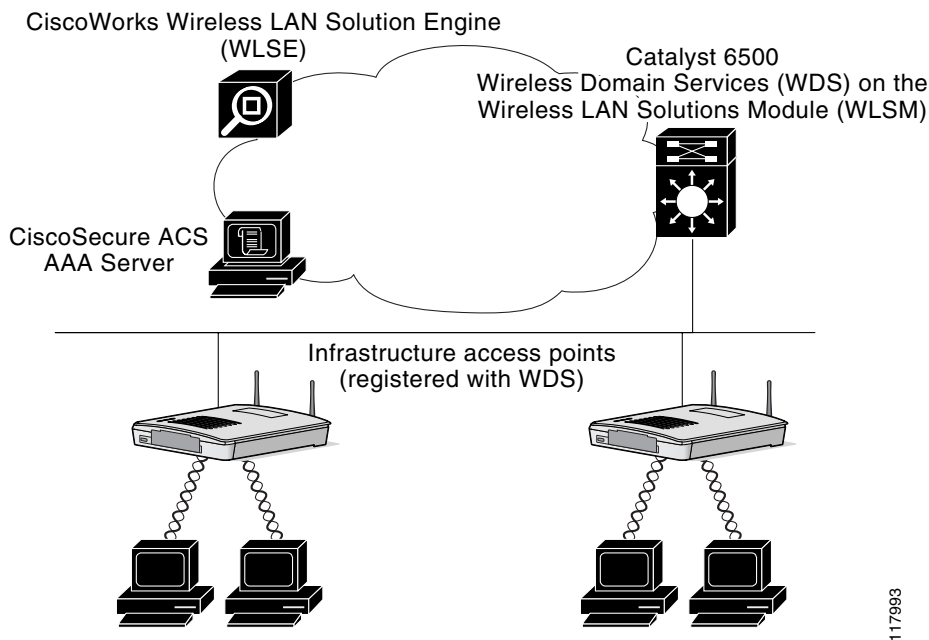


(注) レイヤ3 モビリティを適切に設定するには、WLSM を WDS デバイスとして使用する必要があります。アクセス ポイントを WDS デバイスとして使用すると、レイヤ3 モビリティはサポートされません。

- クライアント デバイス

図 12-3 は、互いに対話してレイヤ3 モビリティを実行するコンポーネントを示しています。

図 12-3 レイヤ3 モビリティに必要なコンポーネント



117993

Cisco Structured Wireless-Aware Network (SWAN) に関する情報ページを表示するには、次のリンクをクリックしてください。

[http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html)



(注) ある Service Set Identifier (SSID; サービス セット ID) にレイヤ3 モビリティを有効化していて、WDS デバイスでレイヤ3 モビリティがサポートされていない場合、クライアント デバイスはその SSID を使用してもアソシエートできません。



(注) リピータ アクセス ポイント、およびワークグループブリッジモードのアクセス ポイントは、レイヤ3 モビリティが設定された SSID にはアソシエートできません。



## Wireless Intrusion Detection Service の概要

無線 LAN 上に Wireless Intrusion Detection Service (WIDS) を実装すると、アクセス ポイント、WLSE、およびオプションの (シスコ製品ではない) WIDS エンジンが同時に動作して、無線 LAN インフラストラクチャ、およびアソシエートされたクライアント デバイスに対する攻撃を感知および防止します。

WLSE と同時に動作する場合、アクセス ポイントは侵入を感知し、無線 LAN を防御するアクションを実行します。WIDS の機能は次のとおりです。

- スイッチ ポートのトレースと不正抑制：スイッチ ポートのトレースと抑制では、未知の無線 (潜在的な不正デバイス) の無線 MAC アドレスを生成する RF 検出方法を使用します。WLSE は、無線 MAC アドレスから有線側 MAC アドレスを取り出し、これを使用してスイッチの BRIDGE MIB を検索します。1 つまたは複数の検索可能な MAC アドレスが利用できる場合、WLSE は Cisco Discovery Protocol (CDP) を使用して、検出元のアクセス ポイントから最大 2 ホップ離れて接続しているすべてのスイッチを発見します。WLSE は CDP で発見された各スイッチの BRIDGE MIB を調べて、ターゲット MAC アドレスが含まれているかどうかを判断します。CDP でいずれかの MAC アドレスが見つかったら、WLSE は対応するスイッチ ポート番号を抑制します。
- 過剰管理フレーム検出：過剰管理フレームは、無線 LAN が攻撃されたことを示します。攻撃者は、無線上で大量の管理フレームを注入し、そのフレームを処理する必要があるアクセス ポイントに大きな負荷を加えることにより、サービス拒絶攻撃を実行する場合があります。スキャン モードのアクセス ポイントとルート アクセス ポイントは、WIDS のフィッチャセットの一部として無線信号をモニタして、過剰管理フレームを検出します。アクセス ポイントが過剰管理フレームを検出すると、障害を生成し、WDS を介して WLSE にこれを送信します。
- 認証/保護失敗検出：認証/保護失敗検出は、無線 LAN 上での最初の認証フェーズを回避するかまたは、進行中のリンク保護を侵害しようとする攻撃者を探します。これらの検出メカニズムは、次の特定の認証攻撃に対応します。
  - EAPOL フラッド検出
  - MIC/暗号化失敗検出
  - MAC スプーフィング検出
- フレーム キャプチャ モード：フレーム キャプチャ モードでは、スキャナ アクセス ポイントが 802.11 フレームを収集し、ネットワーク上の WIDS エンジンのアドレスに転送します。



(注) アクセス ポイントの WIDS への参加の設定方法については、「[WIDS に参加するようにアクセス ポイントを設定する](#)」(P.12-32) を、アクセス ポイントに対する Management Frame Protection (MFP; 管理フレーム保護) の設定方法については、「[管理フレーム保護の設定](#)」(P.12-25) を参照してください。

- 802.11 管理フレーム保護 (MFP)：本質的に、無線は正規のデバイスか、不法デバイスであるかを問わず、あらゆるデバイスで傍受および参加が可能なブロードキャスト メディアです。制御/管理フレームは、クライアント ステーションが AP とのセッションを選択および開始するために使用するため、これらのフレームはオープンである必要があります。管理フレームは暗号化できませんが、偽造から保護する必要があります。MFP は、802.11 管理フレームを完全に保護できる手段です。



(注) MFP で侵入イベントを報告するには WLSE が必要です。



(注) MFP は、1040、1130、1140、1240、1250、および 1260 シリーズのアクセス ポイント、および AP モードの 1300 シリーズのアクセス ポイントなどの 32Mb プラットフォームだけで利用できます。

## WDS の設定

この項では、ネットワーク上で WDS を設定する方法について説明します。この項の構成は、次のとおりです。

- 「WDS のガイドライン」 (P.12-8)
- 「WDS の要件」 (P.12-8)
- 「コンフィギュレーションの概要」 (P.12-9)
- 「アクセス ポイントを潜在的な WDS デバイスとして設定する」 (P.12-10)
- 「アクセス ポイントを WDS デバイスを使用するように設定する」 (P.12-14)
- 「認証サーバが WDS をサポートするように設定する」 (P.12-15)
- 「WDS 専用モードの設定」 (P.12-19)
- 「WDS 情報の表示」 (P.12-20)
- 「デバッグ メッセージの使用」 (P.12-21)

## WDS のガイドライン

WDS を設定する場合は、次のガイドラインに従います。

- クライアント デバイスも収容している WDS アクセス ポイントでは最大 30 個のアクセス ポイントの参加がサポートされますが、無線を無効にした WDS アクセス ポイントでは、最大 60 個までサポートされます。
- WDS 専用モードの場合、WDS では最大 60 個までのインフラストラクチャ アクセス ポイントと 1200 個のクライアントがサポートされます。
- リピータ アクセス ポイントは、WDS をサポートしません。リピータ アクセス ポイントを WDS 候補として設定しないでください。また WDS アクセス ポイントを、イーサネット障害時にリピータ モードに戻る（フォールバックする）設定はしないでください。
- 350 シリーズ アクセス ポイントはメインの WDS デバイスとして設定できません。ただし、350 シリーズ アクセス ポイントを WDS に参加するように設定できます。

## WDS の要件

WDS を設定するには、無線 LAN 上に次の項目を含める必要があります。

- WDS デバイスとして設定可能なアクセス ポイント、サービス統合型ルータ (ISR)、またはスイッチ (Wireless LAN Services Module を装備) が 1 つ以上
- 認証サーバ (またはローカル認証サーバとして設定されたアクセス ポイントまたは ISR)





(注) 1300 アクセス ポイントまたはブリッジは、WDS マスターとして設定できませんが、WDS ネットワークに参加できます。この機能は、1300 アクセス ポイントまたはブリッジではサポートされていません。

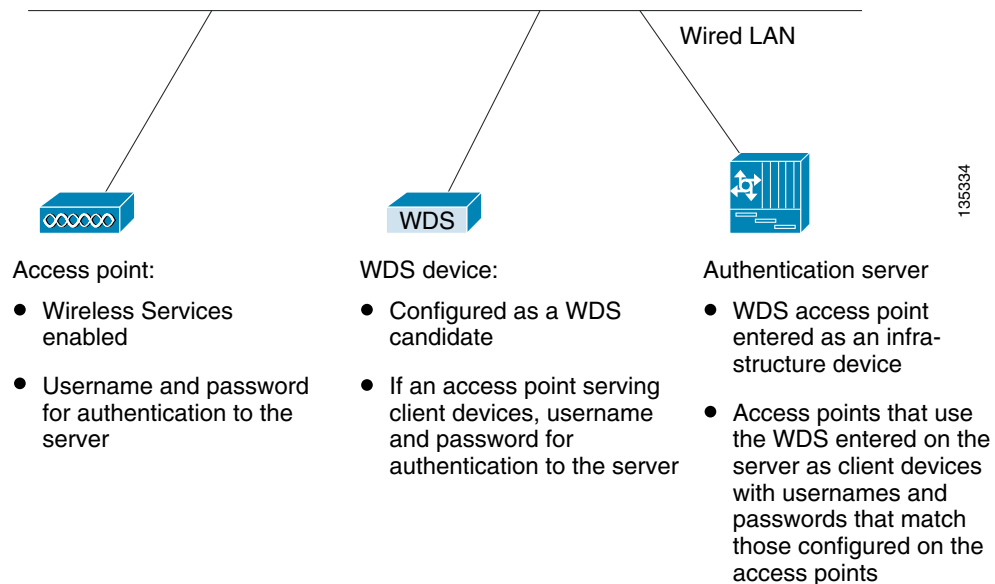
## コンフィギュレーションの概要

WDS および高速安全ローミングの設定には、次の 3 つの主要手順を完了する必要があります。

1. アクセス ポイント、ISR、またはスイッチを潜在的な WDS デバイスとして設定します。この項では、アクセス ポイントを WDS デバイスとして設定する方法について説明します。Wireless LAN Services Module (WLSM) を備えたスイッチに WDS を設定する方法については、『Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide』を参照してください。
2. 他のアクセス ポイントが、この WDS デバイスを使用するように設定します。
3. ネットワーク上の認証サーバが WDS デバイスと、WDS デバイスを使用するアクセス ポイントを認証するように設定します。

図 12-4 は、WDS に参加する各デバイスに必要な設定を示しています。

図 12-4 WDS に参加するデバイスの設定



## アクセスポイントを潜在的な WDS デバイスとして設定する



(注) メインの WDS 候補用に、多数のクライアント デバイスを収容する必要のないアクセスポイントを設定します。クライアント デバイスが WDS アクセスポイントの起動時にアソシエートした場合、そのクライアントは認証のために数分待たされる可能性があります。



(注) リピータ アクセスポイントは、WDS をサポートしません。リピータ アクセスポイントを WDS 候補として設定しないでください。また、WDS アクセスポイントを、イーサネット障害時にリピータ モードに戻るように設定しないでください。



(注) WDS が有効な場合、WDS アクセスポイントはすべての認証を実行、トラッキングします。したがって、WDS アクセスポイントでは EAP セキュリティ設定を行う必要があります。アクセスポイント上での EAP 設定の詳細は、第 11 章「認証タイプの設定」を参照してください。



(注) 350 シリーズ アクセスポイントはメインの WDS デバイスとして設定できません。ただし、350 シリーズ アクセスポイントを WDS に参加するように設定できます。

プライマリ WDS アクセスポイントとして設定するアクセスポイント上で、次の手順に従ってメインの WDS 候補としてアクセスポイントを設定します。

**ステップ 1** [Wireless Services Summary] ページを表示します。図 12-5 は、[Wireless Services Summary] ページを示しています。

図 12-5 [Wireless Services Summary] ページ

HOME	Hostname ap	ap uptime is 1 day, 21 hours, 26 minutes			
EXPRESS SET-UP					
EXPRESS SECURITY					
NETWORK MAP +	Wireless Services Summary				
ASSOCIATION +	AP				
NETWORK INTERFACES +	WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State
SECURITY +					
SERVICES +	Wireless Domain Services				
WIRELESS SERVICES	MAC Address	IP Address	Priority	State	
AP					
WDS					
SYSTEM SOFTWARE +					
EVENT LOG +					
				Refresh	

111873

**ステップ 2** [WDS] をクリックして [WDS/WNM Summary] ページを表示します。

**ステップ 3** [WDS/WNM Summary] ページで、[General Setup] をクリックして [WDS/WNM General Setup] ページを表示します。図 12-6 は、[General Setup] ページを示しています。

図 12-6 [WDS/WNM General Setup] ページ

- ステップ 4** [Use this AP as Wireless Domain Services] チェックボックスをオンにします。
- ステップ 5** [Wireless Domain Services Priority] フィールドに 1 ~ 255 の優先順位数を入力して、WDS 候補の優先順位を設定します。[Wireless Domain Services Priority] フィールド内の数字が最も大きい WDS アクセス ポイント候補が、WDS アクセス ポイントとして機能します。たとえば、1 つの WDS 候補には優先順位に 255 が割り当てられており、もう 1 つの候補には優先順位に 100 が割り当てられている場合は、優先順位が 255 の候補が WDS アクセス ポイントとして機能します。
- ステップ 6** (任意) [Use Local MAC List for Client Authentication] チェックボックスをオンにして、WDS デバイス上で設定されたアドレスのローカル リストにある MAC アドレスを使用してクライアント デバイスを認証します。このチェックボックスをオンにしない場合、WDS デバイスは [Server Groups] ページで MAC アドレス認証用に指定したサーバを使用して、MAC アドレスに基づくクライアント認証を行います。



(注) [Use Local MAC List for Client Authentication] チェックボックスをオンにしても、クライアント デバイスに対して MAC ベースの認証が強制されるわけではありません。サーバベースの MAC アドレス認証に対するローカルの代替方法が提供されるだけです。

- ステップ 7** (任意) ネットワーク上で無線 LAN ソリューション エンジン (WLSE) を使用している場合、[Configure Wireless Network Manager] チェックボックスをオンにして、[Wireless Network Manager IP Address] フィールドに WLSE デバイスの IP アドレスを入力します。WDS アクセス ポイントは、アクセス ポイントとクライアント デバイスから無線計測情報を収集し、集約したデータを WLSE デバイスに送信します。
- ステップ 8** [Apply] をクリックします。
- ステップ 9** [Server Groups] をクリックして、[WDS Server Groups] ページを表示します。図 12-7 は、[WDS Server Groups] ページを示しています。

図 12-7 [WDS Server Groups] ページ

- ステップ 10** WDS アクセス ポイントを使用するインフラストラクチャ デバイス (アクセス ポイント) の 802.1x 認証に使用するサーバ グループを作成します。[Server Group Name] フィールドにグループ名を入力します。
- ステップ 11** [Priority 1] ドロップダウン リストからプライマリ サーバを選択します (グループに追加する必要のあるサーバが [Priority] ドロップダウン リストに表示されない場合は、[Define Servers] をクリックして、[Server Manager] ページを表示します。そのページでサーバを設定してから、[WDS Server Groups] ページに戻ります)。



(注) ネットワーク上に認証サーバが存在しない場合、アクセス ポイントまたは ISR をローカル認証サーバとして設定できます。設定方法の詳細は、第 9 章「ローカル認証サーバ アクセス ポイントの設定」を参照してください。

- ステップ 12** (任意) [Priority 2] ドロップダウン リストおよび [Priority 3] ドロップダウン リストからバックアップ サーバを選択します。

**ステップ 13** [Apply] をクリックします。

**ステップ 14** クライアント デバイス用の 802.1x 認証に使用するサーバのリストを設定します。EAP、LEAP、PEAP、または MAC ベースのような特定タイプの認証を使ってクライアント用の別のリストを指定したり、任意のタイプの認証を使ってクライアント デバイス用のリストを指定したりできます。[Server Group Name] フィールドに、サーバのグループ名を入力します。

[LEAP Authentication] チェックボックスは、特に次に示すシスコ製クライアント向けに用意されています。

- LEAP および EAP-FAST を使用する Cisco Aironet 350 シリーズ カード
- LEAP、EAP-FAST、PEAP、および EAP-TLS を使用する、Cisco Phone 7920、7921、および 7925
- LEAP を使用する ADU

[LEAP Authentication] チェックボックスをオフにすると、これらのクライアント デバイスは無線ネットワークに接続できなくなります。しかし、他のクライアント カードまたはサブリカントの組み合わせの場合、クライアントは先に示した各種 EAP タイプの下で Network-EAP を使用して接続し認証できます。Open 認証に 802.1X 規格を使用するその他すべてのクライアント。先に示した情報は、シスコ以外のクライアントには適用されません。

**ステップ 15** [Priority 1] ドロップダウン リストからプライマリ サーバを選択します (グループに追加する必要のあるサーバが [Priority] ドロップダウン リストに表示されない場合は、[Define Servers] をクリックして、[Server Manager] ページを表示します。そのページでサーバを設定してから、[WDS Server Groups] ページに戻ります)。

**ステップ 16** (任意) [Priority 2] ドロップダウン リストおよび [Priority 3] ドロップダウン リストからバックアップ サーバを選択します。

**ステップ 17** (任意) [Restrict SSIDs] を選択すると、使用するサーバグループを、特定の SSID を使用するクライアント デバイスに制限できます。[SSID] フィールドに SSID を入力して、[Add] をクリックします。SSID を削除するには、削除する SSID を [SSID] リスト内で選択して [Remove] をクリックします。

**ステップ 18** [Apply] をクリックします。

**ステップ 19** LEAP 認証用に WDS アクセス ポイントを設定します。LEAP の設定方法の詳細は、第 11 章「[認証タイプの設定](#)」を参照してください。



(注)

WDS アクセス ポイントでクライアント デバイスを使用する場合は、「[アクセス ポイントを WDS デバイスを使用するように設定する](#)」(P.12-14) の手順に従って、WDS アクセス ポイントが WDS を使用するように設定します。

## CLI の設定例

次の例は、「[アクセス ポイントを潜在的な WDS デバイスとして設定する](#)」(P.12-10) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
AP(config-wlccp-auth)# ssid fred
```

```
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

次の例では、サーバグループ *infra\_devices* を使用してインフラストラクチャ デバイスを認証しています。SSID *fred* または *ginger* を使用するクライアント デバイスは、サーバグループ *client\_devices* を使用して認証されます。

この例で使用されているコマンドの詳細については、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。

## アクセスポイントを WDS デバイスを使用するように設定する

WDS デバイスを通じて認証し、WDS 内に参加するようにアクセスポイントを設定する手順は、次のとおりです。



(注)

インフラストラクチャ アクセスポイントが WDS に参加するには、WDS が実行している IOS と同じバージョンを実行する必要があります。

**ステップ 1** [Wireless Services Summary] ページを表示します。

**ステップ 2** [AP] をクリックして [Wireless Services AP] ページを表示します。図 12-8 は、[Wireless Services AP] ページを示しています。

図 12-8 [Wireless Services AP] ページ

Hostname AP1100 15:45:46 Thu Dec 16 2004

Wireless Services: AP

Participate in SWAN Infrastructure:  Enable  Disable

WDS Discovery:  Auto Discovery  Specified Discovery:  (IP Address)

Username:

Password:

Confirm Password:

Apply Cancel

**ステップ 3** [Participate in SWAN Infrastructure] 設定で [Enable] をクリックします。

- ステップ 4** (任意) ネットワーク上で WDS デバイスとして WLSM スイッチ モジュールを使用する場合は、[Specified Discovery] を選択して、入力フィールドに WLSM の IP アドレスを入力します。[Specified Discovery] を有効にすると、アクセス ポイントは WDS アドバタイズメントを待たずに、WDS デバイスを使用して即座に認証します。指定した WDS デバイスが応答しない場合、アクセス ポイントは WDS アドバタイズメントを待ちます。
- ステップ 5** [Username] フィールドにアクセス ポイントのユーザ名を入力します。このユーザ名は、認証サーバ上でアクセス ポイント用に作成したユーザ名と一致していなければなりません。
- ステップ 6** [Password] フィールドにアクセス ポイントのパスワードを入力し、[Confirm Password] フィールドに同じパスワードをもう一度入力します。このパスワード名は、認証サーバ上でアクセス ポイント用に作成したパスワードと一致していなければなりません。
- ステップ 7** [Apply] をクリックします。

WDS と対話するように設定したアクセス ポイントは、自動的に次の手順を実行します。

- 現在の WDS デバイスを検出、トラッキングし、WDS アドバタイズメントを無線 LAN に中継します。
- WDS デバイスを認証して、認証した WDS デバイスと安全な通信チャネルを確立します。
- WDS デバイスとアソシエートしたクライアント デバイスを登録します。

## CLI の設定例

次の例は、「[アクセス ポイントを WDS デバイスを使用するように設定する](#)」(P.12-14) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7 wes7win8
AP(config)# end
```

この例では、アクセス ポイントは WDS デバイスと対話できるように設定されており、ユーザ名に *APWestWing*、パスワードに *wes7win8* を使用して認証サーバに対する認証を行います。認証サーバ上でクライアントとしてアクセス ポイントを設定するときには、同じユーザ名とパスワードの組み合わせで設定する必要があります。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

## 認証サーバが WDS をサポートするように設定する

WDS デバイスと WDS に参加している全アクセス ポイントは、認証サーバに対する認証を行う必要があります。サーバ上で、アクセス ポイント用のユーザ名とパスワードと、WDS デバイス用のユーザ名とパスワードを設定します。

サーバが Cisco ACS を実行している場合は、次の手順に従ってサーバ上でアクセス ポイントを設定します。

- ステップ 1** Cisco Secure ACS にログインし、[Network Configuration] をクリックして [Network Configuration] ページを表示します。WDS デバイス用のエントリを作成するには、[Network Configuration] ページを使用する必要があります。[図 12-9](#) は、[Network Configuration] ページを示しています。

図 12-9 [Network Configuration] ページ

The screenshot shows the Cisco Network Configuration page. On the left is a navigation menu with options like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' and contains two tables: 'AAA Clients' and 'AAA Servers'. Below each table are 'Add Entry' and 'Search' buttons.

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">DD 3600</a>	10.10.0.2	TACACS+ (Cisco IOS)
<a href="#">DD TME 1200 1</a>	10.10.0.24	RADIUS (Cisco Aironet)
<a href="#">DD TME 1200 2</a>	10.10.0.25	RADIUS (Cisco Aironet)

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
<a href="#">proliant</a>	10.91.104.76	CiscoSecure ACS

**ステップ 2** [AAA Clients] テーブルで、[Add Entry] をクリックします。[Add AAA Client] ページが表示されます。図 12-10 は、[Add AAA Client] ページを示しています。



図 12-10 [Add AAA Client] ページ

The screenshot shows the Cisco Network Configuration interface for adding an AAA client. The sidebar on the left contains the following menu items: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled 'Add AAA Client' and contains the following fields and options:

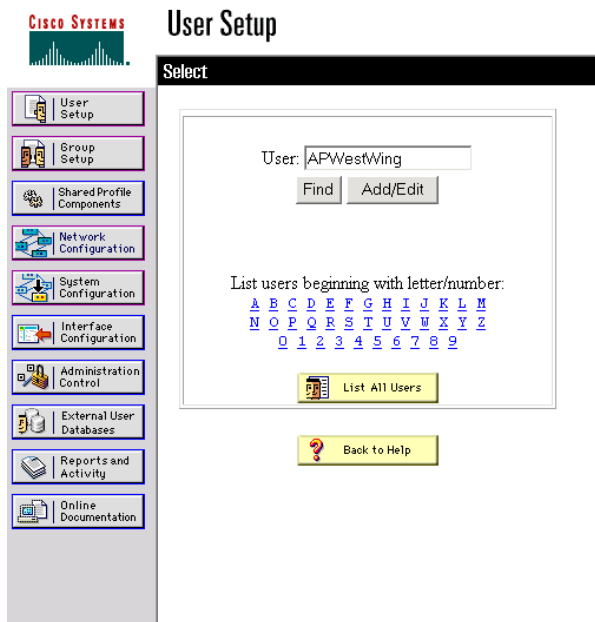
- AAA Client Hostname:
- AAA Client IP Address:
- Key:
- Authenticate Using:
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

At the bottom of the form are three buttons: Submit, Submit + Restart, and Cancel.

- ステップ 3** [AAA Client Hostname] フィールドに、WDS デバイスの名前を入力します。
- ステップ 4** [AAA Client IP Address] フィールドに、WDS デバイスの IP アドレスを入力します。
- ステップ 5** [Key] フィールドに、WDS デバイスで設定したのとまったく同じパスワードを入力します。
- ステップ 6** [Authenticate Using] ドロップダウン リストから [RADIUS (Cisco Aironet)] を選択します。
- ステップ 7** [Submit] をクリックします。
- ステップ 8** WDS デバイス候補それぞれに対して、[ステップ 2](#) から [ステップ 7](#) の手順を繰り返します。

- ステップ 9** [User Setup] をクリックして [User Setup] ページを表示します。WDS デバイスを使用するアクセスポイント用のエントリを作成するには、[User Setup] ページを使用する必要があります。  
 図 12-11 は、[User Setup] ページを示しています。

図 12-11 [User Setup] ページ

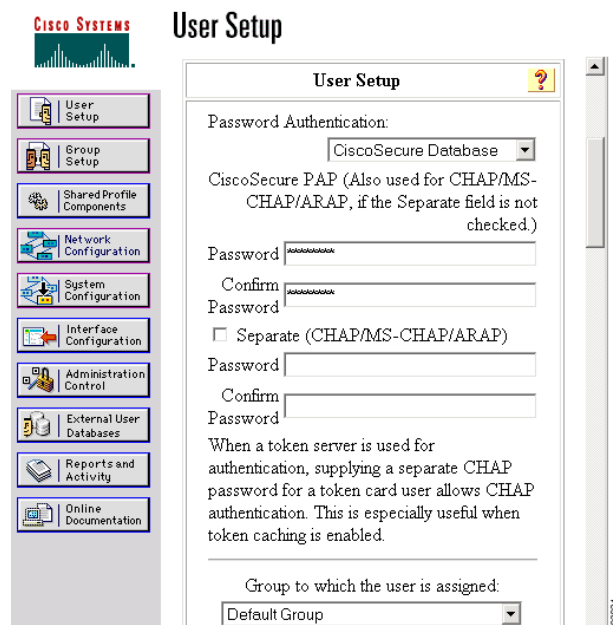


- ステップ 10** [User] フィールドに、アクセスポイントの名前を入力します。

- ステップ 11** [Add/Edit] をクリックします。

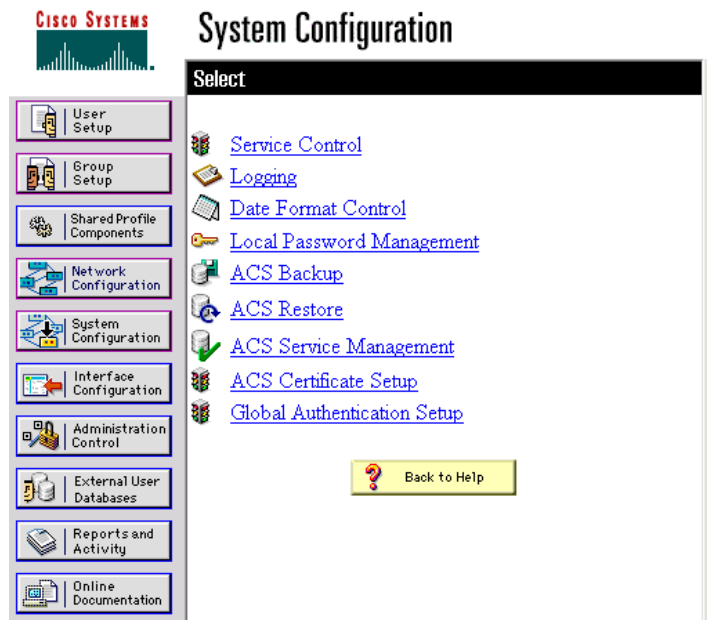
- ステップ 12** [User Setup] ボックスが表示されるまで、画面を下にスクロールします。図 12-12 は、[User Setup] ボックスを示しています。

図 12-12 [ACS User Setup] ボックス



- ステップ 13** [Password Authentication] ドロップダウン リストから [CiscoSecure Database] を選択します。
- ステップ 14** [Password] フィールドと [Confirm Password] フィールドに、[Wireless Services AP] ページでアクセスポイントに対して入力したのとまったく同じパスワードを入力します。
- ステップ 15** [Submit] をクリックします。
- ステップ 16** WDS デバイスを使用するアクセスポイントそれぞれに対して、[ステップ 10](#) から [ステップ 15](#) の手順を繰り返します。
- ステップ 17** [System Configuration] ページを表示して [Service Control] をクリックし、ACS を再始動してエントリ内容を適用します。[図 12-13](#) は、[System Configuration] ページを示しています。

**図 12-13** [ACS System Configuration] ページ



## WDS 専用モードの設定

WDS アクセスポイントは、**wlccp wds mode wds-only** コマンドを使用すれば、WDS 専用モードで稼働できます。このコマンドを発行してリロードすると、アクセスポイントは WDS 専用モードで機能を開始します。WDS 専用モードでは、dot11 サブシステムが初期化されず、dot11 インターフェイス関連のコマンドが設定できません。WDS 専用モードの場合、WDS では最大 60 個までのインフラストラクチャアクセスポイントと最大 1200 個のクライアントがサポートされます。このコマンドの **no** 形式を使用して、WDS 専用モードをオフにします。WDS アクセスポイントの実行中モードを表示するには、**show wlccp wds** コマンドを使用します。

WDS アクセスポイントが AP および WDS の両モードで稼働するように設定するには、**no wlccp wds mode wds-only** コマンドを使用し、さらに **write erase** コマンドを使用してアクセスポイントをただちにリロードします。アクセスポイントをリロードすると、dot11 無線サブシステムが初期化されます。アクセスポイントと WDS は、無線クライアントに直接アソシエートします。このモードの場合、WDS では 20 個の無線クライアントの直接アソシエートに加え、30 個のインフラストラクチャアクセスポイントと 600 個のクライアントがサポートされます。

## WDS 情報の表示

Web ブラウザのインターフェイスでは、[Wireless Services Summary] ページを使って WDS ステータスの概要を表示します。

特権 EXEC モードの CLI では、次のコマンドを使って、現在の WDS デバイスと CCKM に参加している他のアクセス ポイントについての情報を表示します。

コマンド	説明
<code>show wlccp ap</code>	CCKM に参加する任意のアクセス ポイント上で、このコマンドを使用して、WDS デバイスの MAC アドレス、WDS デバイスの IP アドレス、アクセス ポイントのステータス（認証中、認証済み、登録済み）、インフラストラクチャ認証サーバの IP アドレス、クライアント デバイス（MN）認証サーバの IP アドレスを表示できます。
<code>show wlccp wds { ap   mn } [ detail ] [ mac-addr mac-address ]</code>	<p>WDS デバイスに限り、このコマンドを使って、アクセス ポイントとクライアント デバイスに関するキャッシュ情報を表示できます。</p> <ul style="list-style-type: none"> <li> <b>ap</b> : このオプションを使用して、CCKM に参加するアクセス ポイントを表示します。このコマンドは、各アクセス ポイントの MAC アドレス、IP アドレス、状態（認証中、認証済み、または登録済み）、有効期間（アクセス ポイントが再認証を必要とするまでの秒数）を表示します。<b>mac-addr</b> オプションを使用して、特定のアクセス ポイントに関する情報を表示します。         </li> <li> <b>mn</b> : このオプションを使用して、クライアント デバイスや呼び出されたモバイル ノードに関するキャッシュ情報を表示します。このコマンドは、各クライアントの MAC アドレス、IP アドレス、クライアントがアソシエートされているアクセス ポイント（cur-AP）、および状態（認証中、認証済み、または登録済み）を表示します。<b>detail</b> オプションを使用して、クライアントの有効期間（クライアントが再認証を必要とするまでの残りの秒数）、SSID、および VLAN ID を表示します。<b>mac-addr</b> オプションを使用して、特定のクライアント デバイスに関する情報を表示します。         </li> </ul> <p><code>show wlccp wds</code> だけを入力すると、アクセス ポイントの IP アドレス、MAC アドレス、優先順位、インターフェイスの状態（管理上スタンダアロン、アクティブ、バックアップ、候補、または WDS 専用）を表示します。</p> <p>状態がバックアップの場合、コマンドは現在の WDS デバイスの IP アドレス、MAC アドレス、および優先順位も表示します。</p> <p>状態が WDS 専用の場合、コマンドはデバイスの MAC アドレス、IP アドレス、インターフェイスの状態、アクセス ポイント数、およびモバイル ノード数を表示します。</p>

## デバッグ メッセージの使用

特権 EXEC モードでは、デバッグ コマンドを使用して、WDS デバイスと対話するデバイス用のデバッグ メッセージの表示を制御します。

コマンド	説明
<code>debug wlccp ap</code> {mn   wds-discovery   state}	このコマンドを使用して、クライアント デバイス (mn)、WDS 検出プロセス、WDS デバイス (state) に対するアクセス ポイントの認証に関連するデバッグ メッセージの表示をオンにします。
<code>debug wlccp dump</code>	このコマンドを使用して、バイナリ形式で送受信された WLCCP パケットのダンプを実行します。
<code>debug wlccp packet</code>	このコマンドを使用して、WDS デバイスとやり取りするパケットの表示をオンにします。
<code>debug wlccp wds [aggregator   authenticator   nm   state   statistics]</code>	このコマンドとそのオプションを使用して、WDS デバック メッセージの表示をオンにします。statistics オプションを使用して、障害統計情報の表示をオンにします。
<code>debug wlccp wds authenticator</code> {all   dispatcher   mac-authen   process   rxdata   state-machine   txdata}	このコマンドとそのオプションを使用して、認証に関連する WDS デバック メッセージの表示をオンにします。

## 高速安全ローミングの設定

WDS を設定すると、CCKM 用に設定したアクセス ポイントは、アソシエートされたクライアント デバイスに高速安全ローミングを提供できます。この項では、高速で安全なローミングを無線 LAN 上で設定する方法を説明します。この項の構成は、次のとおりです。

- [高速安全ローミングの要件](#)
- [高速安全ローミングをサポートするアクセス ポイントの設定](#)

## 高速安全ローミングの要件

高速安全ローミングを設定するには、無線 LAN で次の項目が必要となります。

- WDS デバイスとして設定される 1 つ以上のアクセス ポイント、ISR、または WLSM を備えたスイッチ
- WDS に参加するように設定されたアクセス ポイント
- 高速安全ローミング用に設定されたアクセス ポイント
- 認証サーバ (またはローカル認証サーバとして設定されたアクセス ポイント、ISR、またはスイッチ)
- Cisco Aironet クライアント デバイス、または Cisco Compatible Extensions (CCX) バージョン 2 以降と互換性のあるシスコ互換のクライアント デバイス

WDS の設定方法については、「[WDS の設定](#)」(P.12-8) を参照してください。

## 高速安全ローミングをサポートするアクセスポイントの設定

高速安全ローミングをサポートするには、WDS に参加するように無線 LAN 上のアクセスポイントを設定し、アクセスポイントで少なくとも 1 つの SSID に対して CCKM 認証済みキー管理を許可する必要があります。SSID に CCKM を設定する手順は、次のとおりです。

- ステップ 1** アクセスポイント GUI で [Encryption Manager] ページを表示します。図 12-14 は、[Encryption Manager] ページの上部を示しています。

図 12-14 [Encryption Manager] ページ

- ステップ 2** [Cipher] ボタンをクリックします。
- ステップ 3** [Cipher] ドロップダウン リストから、[CKIP + CMIC] を選択します。
- ステップ 4** [Apply] をクリックします。
- ステップ 5** [Global SSID Manager] ページを表示します。図 12-15 は、[Global SSID Manager] ページの上部を示しています。

図 12-15 [Global SSID Manager] ページ

HOME	Hostname AP1230	08:05:20 Thu May 19 2005
EXPRESS SET-UP	<b>Security: Global SSID Manager</b>	
EXPRESS SECURITY	<b>SSID Properties</b>	
NETWORK MAP +	<b>Current SSID List</b>	
ASSOCIATION +	<input type="text" value="fastroam"/>	SSID: <input type="text" value="fastroam"/>
NETWORK INTERFACES +	<input type="text" value="UC"/> <input type="text" value="fastroam"/>	VLAN: <input type="text" value="&lt; NONE &gt;"/> <a href="#">Define VLANs</a>
<b>SECURITY</b>		Interface: <input checked="" type="checkbox"/> Radio0-802.11G <input type="checkbox"/> Radio1-802.11A
Admin Access		Network ID: <input type="text" value=""/> (0-4096)
Encryption Manager		<input type="button" value="Delete"/>
<b>SSID Manager</b>	<b>Authentication Settings</b>	
Server Manager	<b>Methods Accepted:</b>	
Local RADIUS Server	<input type="checkbox"/> Open Authentication: <input type="text" value="&lt; NO ADDITION &gt;"/>	
Advanced Security	<input type="checkbox"/> Shared Authentication: <input type="text" value="&lt; NO ADDITION &gt;"/>	
<b>SERVICES</b> +	<input checked="" type="checkbox"/> Network EAP: <input type="text" value="&lt; NO ADDITION &gt;"/>	
WIRELESS SERVICES +	<b>Server Priorities:</b>	
SYSTEM SOFTWARE +	<b>EAP Authentication Servers</b>	
EVENT LOG +	<input checked="" type="radio"/> Use Defaults <a href="#">Define Defaults</a>	
	<input type="radio"/> Customize	
	Priority 1: <input type="text" value="&lt; NONE &gt;"/>	<b>MAC Authentication Servers</b>
	Priority 2: <input type="text" value="&lt; NONE &gt;"/>	<input checked="" type="radio"/> Use Defaults <a href="#">Define Defaults</a>
	Priority 3: <input type="text" value="&lt; NONE &gt;"/>	<input type="radio"/> Customize
		Priority 1: <input type="text" value="&lt; NONE &gt;"/>
		Priority 2: <input type="text" value="&lt; NONE &gt;"/>
		Priority 3: <input type="text" value="&lt; NONE &gt;"/>
	<b>Authenticated Key Management</b>	
	Key Management: <input type="text" value="Mandatory"/>	<input checked="" type="checkbox"/> CCKM <input type="checkbox"/> WPA
	WPA Pre-shared Key: <input type="text"/>	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal

**ステップ 6** CCKM をサポートする SSID で、次の設定を選択します。

- アクセス ポイントに複数の無線インターフェイスが含まれている場合は、SSID が適用されるインターフェイスを選択します。
- [Authentication Settings] で、[Network EAP] を選択します。CCKM を有効にする際は、認証タイプとして Network EAP を有効にする必要があります。

- c. [Authenticated Key Management] で、[Mandatory] または [Optional] を選択します。  
[Mandatory] を選択した場合、CCKM をサポートするクライアントだけが、SSID を使用してアソシエートできます。[Optional] を選択した場合、CCKM クライアントと CCKM をサポートしないクライアントの両方が、SSID を使用してアソシエートできます。
- d. [CCKM] チェックボックスをオンにします。

**ステップ 7** [Apply] をクリックします。

## CLI の設定例

次の例は、「[高速安全ローミングをサポートするアクセスポイントの設定](#)」(P.12-22) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers ckip-cmic
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

次の例では、SSID *fastroam* は Network EAP と CCKM をサポートするように設定されています。2.4GHz 無線インターフェイス上で CKIP-CMIC 暗号スイートが有効になっています。また、2.4GHz 無線インターフェイス上で、SSID *fastroam* が有効になっています。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

## 802.11r のサポート

自律ルートアクセスポイントでは 802.11r のサポートを提供します。無線ドメイン サービスでは、次のタイプのローミングをサポートします。

- 分散システム (DS) 上の Fast Transition
- 無線経由の Fast Transition

802.11r は、Cisco Centralized Key Management (CCKM) および Pairwise Master Key Identifier (PMKID) のローミングとは次のように異なります。

- ローミングする前に最初の認証が行われる
- 無線経由または DS を使用したターゲット AP との認証に既存アクセスポイントの通信チャネルを使用する

### 802.11r の有効化

802.11r を有効にするには、次の手順を実行します。

**ステップ 1** [Network] > [Network interface] を選択します。

**ステップ 2** [Radio0-802.11n 2G.Hz] または [Radio0-802.11n 5G.Hz] を選択します。



- ステップ 3** 11r 設定の [enable] オプション ボタンをクリックします。
- ステップ 4** [over-air] または [over-ds] オプション ボタンをクリックします。
- ステップ 5** 再アソシエーションの時間を入力します。  
値の範囲は 20 ~ 1200 です。
- ステップ 6** [Apply] をクリックします。

特権 EXEC モードから、アクセス ポイントの CLI で SSH を設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 ssid &lt;ssid&gt;</code>	SSID を設定します。
ステップ 3	<code>authentication key-management wpa version 2 dot11r</code>	アクセス ポイントに 802.11r を設定します。
ステップ 4	<code>interface dot11radio {0 / 1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。2.4GHz 無線は Radio 0、5GHz 無線は Radio 1 です。
ステップ 5	<code>dot11 dot11r pre-authentication</code>	[over-air] または [over-ds] の移行を有効または無効にします。
ステップ 6	<code>dot11 dot11r re-association timer &lt;value&gt;</code>	再アソシエーション タイマーを設定します。
ステップ 7	<code>debug dot11 ft</code>	802.11r の高速 BSS 移行をデバッグします。
ステップ 8	<code>debug dot11 ft-scan</code>	802.11r の高速 BSS 移行のスキャンをデバッグします。

## 管理フレーム保護の設定

管理フレーム保護の稼働には WDS が必要で、この保護は 32Mb プラットフォーム (s : 1130、1240 シリーズ アクセス ポイント、および AP モードの 1300 シリーズ アクセス ポイント) だけで利用できます。MFP は WLSE で設定されますが、アクセス ポイントおよび WDS では MFP を手動で設定できます。



- (注) WLSE が存在しない場合は、MFP では検出した侵入をレポートできないため、有効性が限定されます。WLSE が存在する場合は、WLSE から設定を実行します。

完全に保護するには、MFP アクセス ポイントで Simple Network Transfer Protocol (SNTP) も設定します。

## Management Frame Protection

管理フレーム保護は、アクセスポイントとクライアントステーション間で転送される管理メッセージにセキュリティ機能を提供します。MFPは、インフラストラクチャMFPとクライアントMFPの2つの機能コンポーネントで構成されます。

インフラストラクチャMFPは、インフラストラクチャサポートを提供します。インフラストラクチャMFPは、不正デバイスおよびサービス拒絶攻撃の検出に有益なブロードキャストおよび誘導された管理フレームに対するMessage Integrity Check (MIC; メッセージ完全性チェック)を利用します。クライアントMFPはクライアントをサポートします。クライアントMFPは、WLANに対する一般的な攻撃の多くを無力化することによって、認証されたクライアントをスプーフィングされたフレームから保護します。

管理フレーム保護の稼働にはWDSが必要で、この保護は32Mbプラットフォーム(1130、1140、1240、1250シリーズアクセスポイント、およびAPモードの1300シリーズアクセスポイント)だけで利用できます。MFPはWLSEで設定されますが、アクセスポイントおよびWDSではMFPを手動で設定できます。



(注)

WLSEが存在しない場合は、MFPでは検出した侵入をレポートできないため、有効性が限定されます。WLSEが存在する場合は、WLSEから設定を実行します。

完全に保護するには、MFPアクセスポイントでSimple Network Transfer Protocol (SNTP)も設定します。

## 概要

クライアントMFPは、アクセスポイントとCCXv5対応クライアントステーション間で送信されるクラス3管理フレームを暗号化し、スプーフィングされたクラス3管理フレーム(APと認証およびアソシエートされたクライアントステーション間で送信される管理フレーム)をドロップすることによってAPとクライアントの両方が予防措置を実行できるようにします。クライアントMFPは、IEEE 802.11iに規定されたセキュリティメカニズムを使用して、クラス3ユニキャスト管理フレームを保護します。再アソシエーション要求のRSNIEでSTAによって決定されたユニキャスト暗号スイートによって、ユニキャストデータとクラス3管理フレームの両方が保護されます。ワークグループブリッジ、リピータ、または非ルートブリッジモードのアクセスポイントでクライアントMFPを使用するには、TKIPまたはAES-CCMPのいずれかのネゴシエーションが必要です。

## ユニキャスト管理フレームの保護

ユニキャストクラス3管理フレームは、すでにデータフレームに使用されている方法と同様にしてAES-CCMPまたはTKIPのいずれかを適用することによって保護されます。クライアントMFPは、暗号化がAES-CCMPまたはTKIPで、キー管理WPAバージョン2の場合に限り、自律アクセスポイントで有効化されます。

## ブロードキャスト管理フレームの保護

ブロードキャスト フレームを使用した攻撃を防ぐため、CCXv5 をサポートするアクセス ポイントではブロードキャスト クラス 3 管理フレームをいっさい送信しません。クライアント MFP が有効化されている場合、ワークグループブリッジ、リピータ、または非ルートブリッジモードのアクセス ポイントでは、ブロードキャスト クラス 3 の管理フレームが廃棄されます。

クライアント MFP は、暗号化が AES-CCMP または TKIP で、キー管理 WPA バージョン 2 の場合に限り、自律アクセス ポイントで有効化されます。

## ルート モードのアクセス ポイントのクライアント MFP

ルート モードの自律アクセス ポイントでは、混合モードのクライアントがサポートされます。CCXv5 に対応し、WPAv2 の暗号スイート AES または TKIP が決定されているクライアントでは、クライアント MFP は有効です。CCXv5 に対応していないクライアントでは、クライアント MFP は無効です。デフォルトでは、クライアント MFP はアクセス ポイント上の特定の SSID に対するオプションで、SSID コンフィギュレーション モードで CLI を使用して有効と無効を切り替えることができます。

特定の SSID に、クライアント MFP を必須とするか、オプションとするかを設定できます。クライアント MFP を必須に設定するには、SSID でキー管理 WPA バージョン 2 を必須に設定します。キー管理が WPAv2 必須に設定されていない場合、エラー メッセージが表示され、CLI コマンドが拒否されます。クライアント MFP を必須として設定したキー管理およびキー管理 WPAv2 を変更しようとする、エラー メッセージが表示され、CLI コマンドが拒否されます。オプションとして設定されている場合、クライアント MFP は SSID で WPAv2 に対応している場合に限り有効化され、対応していない場合にはクライアント MFP は無効化されます。

## クライアント MFP の設定

次の CLI コマンドは、ルート モードのアクセス ポイントでクライアント MFP を設定する際に使用されます。

### **ids mfp client required**

この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP を必須として有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。また、このコマンドでは、SSID で WPA バージョン 2 が必須として設定されていることが要求されます。SSID で WPAv2 が必須として設定されていない場合、エラーメッセージが表示され、コマンドが拒否されます。

### **no ids mfp client**

この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP を無効にします。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。

### **ids mfp client optional**

この SSID コンフィギュレーション コマンドは、特定の SSID でクライアント MFP をオプションとして有効化します。このコマンドの実行時に SSID が Dot11Radio インターフェイスにバインドされている場合は、Dot11Radio インターフェイスがリセットされます。クライアント MFP は SSID で WPAv2 に対応している場合に限り、特定の SSID に対して有効化され、対応していない場合にはクライアント MFP は無効化されます。

**show dot11 ids mfp client statistics**

このコマンドを使用すると、Dot11Radio インターフェイスのアクセス ポイント コンソールにクライアント MFP 統計が表示されます。

**clear dot11 ids mfp client statistics**

このコマンドを使用すると、クライアント MFP 統計がクリアされます。

**authentication key management wpa version {1|2}**

このコマンドを使用すると、特定の SSID の WPA キー管理に使用される WPA バージョンが明示的に指定されます。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>dot11 ids mfp generator</b>	アクセス ポイントを MFP ジェネレータとして設定します。有効にすると、アクセス ポイントは Message Integrity Check Information Element (MIC IE; メッセージ完全性チェック情報エレメント) を各フレームに追加して、送信する管理フレームを保護します。フレームのコピー、改変、またはリプレイなどの攻撃が仕掛けられた場合、フレームは MIC を無効にし、MFP フレームを検出 (検証) するように設定された受信アクセス ポイントのすべてで不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。
ステップ 3	<b>dot11 ids mfp detector</b>	アクセス ポイントを MFP ディテクタとして設定します。有効にすると、アクセス ポイントで他のアクセス ポイントから受信した管理フレームが検証されます。有効および予測された MIC IE が含まれないフレームを受信すると、WDS に不一致がレポートされます。アクセス ポイントは、WDS のメンバーである必要があります。
ステップ 4	<b>sntp server <i>server IP address</i></b>	SNTP サーバの名前または IP アドレスを入力します。
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

特権 EXEC モードから、次の手順に従って WDS を設定します。

	コマンド	説明
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>dot11 ids mfp distributor</b>	WDS を MFP ディストリビュータとして設定します。有効にすると、WDS では署名キーが管理されます。このキーは MIC IE の作成に使用され、ジェネレータとディストリビュータ間で安全に転送されます。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## 802.11w による管理フレーム保護

現在の 802.11 標準は、無線リンクの管理および制御に使用するフレーム タイプを定義します。802.11 プロトコルに含まれる管理フレームは、WLAN に最高レベルのセキュリティが使用されている場合でも、認証も暗号化もされません。802.11w は、IEEE 802.11 標準ファミリの管理フレーム保護標準です。

802.11w は 3 種類の新しいセキュリティを提供することにより、管理フレームのセキュリティを向上します。

- データ送信元の信頼性
- リプレイ検出
- 堅牢な管理フレーム保護。

保護できる管理フレームは次のとおりです。

- ディスアソシエーション
- 認証解除
- パブリック アクション フレームを除くロバスト アクション フレーム

802.11w を使用して、アソシエーション要求のリプレイ攻撃を防ぐこともできます。

802.11w を有効にするには、次の手順を実行します。

- 
- ステップ 1** アクセス ポイントの GUI の [Security] ページを表示します。
  - ステップ 2** [SSID Manager] を選択します。
  - ステップ 3** [Client Authenticated Key Management] ページで、[11w Configuration Required] オプション ボタンをクリックします。
  - ステップ 4** [11w Association-comeback] の時間を入力します。
  - ステップ 5** [11w Saquery-retry] の時間を入力します。
- 

次の CLI コマンドは、アクセス ポイントの 802.11w を有効にするために使用されます。

```
ap(config-ssid)# 11w-pmf client required/optional
```

次の CLI コマンドは、アソシエーションのタイムアウトと saquery の再試行間隔を設定するために使用されます。

```
ap(config-ssid)# 11w-pmf association-comeback 1000-20000ms
```

```
ap(config-ssid)# 11w-pmf saquery-retry 100-500ms
```

これらのコマンドは任意です。これらのコマンドを使用しない場合、デフォルトの間隔が設定されます。アクセス ポイントに 802.11w を設定するには、MFP クライアントを無効にする必要があります。



(注) WPAv2/AES は 802.11w では必須です。

---

次のコマンドは、WGB デバイスで 802.11w を設定するために使用されます。

```
- ap(config-ssid)# 11w-pmf client required/optional
```



(注) 次のコマンドは、AP の設定と同じである必要があります。

- ap(config-ssid)# no ids mfp client



(注) CCKM、11r 高速ローミング、DLS、無線計測、公共の処理用の保護されたデュアル、の各アクションフレームはサポートされません。

デバッグを有効にするには、次のコマンドを使用します。

- ap(config-ssid)# debug dot11 mgmt 11w
- ap(config-ssid)# debug dot11 mgmt interface
- ap(config-ssid)# debug dot11 wpa-cckm-km-dot1x

## 無線管理の設定

WDS を使用するように無線 LAN 上のアクセス ポイントを設定すると、アクセス ポイントは WDS デバイスと対話するときに自動的に無線管理における役割を果たします。無線管理の設定を行うには、ネットワーク上の WLSE デバイスと対話するように WDS デバイスを設定します。

WDS デバイスとして設定されたアクセス ポイント上の無線管理を有効にする手順は、次のとおりです。

- ステップ 1** [Wireless Services Summary] ページを表示します。図 12-16 は、[Wireless Services Summary] ページを示しています。

図 12-16 [Wireless Services Summary] ページ

HOME	Hostname ap	ap uptime is 1 day, 21 hours, 26 minutes																					
EXPRESS SET-UP	<b>Wireless Services Summary</b> <a href="#">AP</a> <table border="1"> <thead> <tr> <th>WDS MAC Address</th> <th>WDS IP Address</th> <th>IN Authenticator</th> <th>MN Authenticator</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> <a href="#">Wireless Domain Services</a> <table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Priority</th> <th>State</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table>					WDS MAC Address	WDS IP Address	IN Authenticator	MN Authenticator	State						MAC Address	IP Address	Priority	State				
WDS MAC Address						WDS IP Address	IN Authenticator	MN Authenticator	State														
MAC Address						IP Address	Priority	State															
EXPRESS SECURITY																							
NETWORK MAP +																							
ASSOCIATION +																							
NETWORK INTERFACES +																							
SECURITY +																							
SERVICES +																							
<b>WIRELESS SERVICES</b>																							
AP																							
WDS																							
SYSTEM SOFTWARE +																							
EVENT LOG +																							
Refresh																							

111873

- ステップ 2** [WDS] をクリックして [General Setup] ページを表示します。
- ステップ 3** [WDS/WNM Summary] ページで [Settings] をクリックして [General Setup] ページを表示します。図 12-17 は、[General Setup] ページを示しています。

図 12-17 [WDS/WNM General Setup] ページ

WDS STATUS SERVER GROUPS GENERAL SET-UP

HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION + NETWORK INTERFACES + SECURITY + SERVICES +

WIRELESS SERVICES AP WDS SYSTEM SOFTWARE + EVENT LOG +

Hostname ap ap uptime is 1 day, 21 hours, 33 minutes

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

Use this AP as Wireless Domain Services

Wireless Domain Services Priority: DISABLED (1-255)

Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

Configure Wireless Network Manager

Wireless Network Manager IP Address: DISABLED (IP Address)

Apply Cancel 111871

**ステップ 4** [Configure Wireless Network Manager] チェックボックスをオンにします。

**ステップ 5** [Wireless Network Manager IP Address] フィールドに、ネットワーク上の WLSE デバイスの IP アドレスを入力します。

**ステップ 6** [Apply] をクリックします。WDS アクセス ポイントが WLSE デバイスと対話するように設定されます。

## CLI の設定例

次の例は、「無線管理の設定」(P.12-30) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

この例では、WDS アクセス ポイントは、IP アドレスが 192.250.0.5 の WLSE デバイスと対話できるようになります。

この例で使用されているコマンドの詳細については、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。

## WIDSに参加するようにアクセスポイントを設定する

WIDSに参加するには、WDSと無線管理に参加するようにアクセスポイントを設定する必要があります。WDSと無線管理に参加するようにアクセスポイントを設定するには、「[アクセスポイント](#)をWDSデバイスを使用するように設定する」(P.12-14)と「[無線管理の設定](#)」(P.12-30)の手順を実行します。

### アクセスポイントをスキャナモードに設定する

スキャナモードの場合、アクセスポイントは無線活動のチャンネルをすべてスキャンし、その活動をネットワーク上のWDSデバイスに報告します。スキャナアクセスポイントは、クライアントアソシエーションを受け付けません。

特権EXECモードから、次の手順に従ってアクセスポイントに無線ネットワークの役割をスキャナに設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイスコンフィギュレーションモードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。  5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>station role scanner</code>	アクセスポイントの役割をスキャナに設定します。
ステップ 4	<code>end</code>	特権EXECモードに戻ります。

### アクセスポイントをモニタモードに設定する

アクセスポイントをスキャナとして設定すると、モニタモードでフレームのキャプチャも可能になります。モニタモードでは、アクセスポイントは802.11フレームをキャプチャし、これをネットワーク上でWIDSエンジンに転送します。アクセスポイントは、転送するすべての802.11フレームに28バイトのキャプチャヘッダーを追加します。ネットワーク上のWIDSエンジンは、このヘッダー情報を分析に使用します。アクセスポイントは、キャプチャしたフレームの転送にUDPパケットを使用します。ネットワーク帯域幅を節約するため、複数のキャプチャしたフレームを1つのUDPパケットに結合できます。

スキャナモードでは、アクセスポイントは無線活動のすべてのチャンネルをスキャンします。ただし、モニタモードの場合、アクセスポイントは、アクセスポイント無線が設定されているチャンネルだけをモニタします。



(注)

アクセスポイントに2つ無線が含まれている場合、インターフェイス上でモニタモードを設定するには、無線が両方ともスキャナモードに設定されている必要があります。



特権 EXEC モードから、次の手順に従って 802.11 フレームをキャプチャして転送するようにアクセスポイントを設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface dot11radio {0   1}</b>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<b>monitor frames endpoint ip address IP-address port UDP-port [truncate truncation-length]</b>	モニタ モードに無線を設定します。ネットワーク上の WIDS エンジン上で、IP アドレスと UDP ポートを入力します。  <ul style="list-style-type: none"> <li>(任意) 転送したフレームごとに、バイト単位で最大長を設定します。アクセスポイントは、この値より長いフレームを切り捨てます。デフォルトの長さは 128 バイトです。</li> </ul>
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。

## モニタ モード統計の表示

**show wlccp ap rm monitor statistics** グローバル コンフィギュレーション コマンドを使用して、キャプチャしたフレームの統計を表示します。

次に、コマンドの出力例を示します。

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
=====
WLAN Monitoring           : Enabled
Endpoint IP address      : 10.91.107.19
Endpoint port            : 2000
Frame Truncation Length  : 535 bytes

Dot11Radio 1
=====
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
=====
Total No.of frames rx by DOT11 driver      : 58475
Total No.of Dot11 no buffers                : 361
Total No.of Frames Q Failed                : 0
Current No.of frames in SCAN Q             : 0

Total No.of frames captured                 : 0
Total No.of data frames captured           : 425
Total No.of control frames captured        : 1957
Total No.of Mgmt frames captured           : 20287
Total No.of CRC errored frames captured: 0

Total No.of captured frames forwarded      : 23179
Total No.of captured frames forward failed : 0
```

**clear wlccp ap rm statistics** コマンドを使用して、モニタ モード統計を消去します。

## モニタ モード制限の設定

モニタ モードでアクセスポイントが使用するしきい値を設定できます。しきい値を超えると、アクセスポイントは、情報をログに記録するかまたは警告を送信します。

### 認証失敗制限の設定

認証失敗制限を設定すると、*EAPOL* フラッディングと呼ばれるサービス拒絶攻撃からネットワークを保護できます。クライアントとアクセスポイントとの間で発生する **802.1X** 認証により、アクセスポイント、オーセンティケータ、および *EAPOL* メッセージングを使用する認証サーバの間に、一連のメッセージが表示されます。通常、*RADIUS* サーバである認証サーバは、過度に認証が試みられるとすぐに負荷に耐えられなくなります。規制されていない場合、1台のクライアントからネットワークに影響を与えるほどの認証要求が発生する可能性があります。

モニタ モードでは、アクセスポイントは **802.1X** クライアントがアクセスポイントを通じて認証を試みる割合をトラッキングします。過度な認証の試みによってネットワークが攻撃される場合、アクセスポイントは、認証しきい値を超えると警告を發します。

これらの制限はアクセスポイント上で設定できます。

- アクセスポイントからの **802.1X** の試みの回数
- アクセスポイント上の秒単位での *EAPOL* フラッドの期間

アクセスポイントは、過度の認証の試みを検出すると、この情報を示すための *MIB* 変数を設定します。

- *EAPOL* フラッドが検出されました
- 認証の試みの回数
- 認証の試みの回数が最も多いクライアントの *MAC* アドレス

特権 EXEC モードから、次の手順に従って、アクセスポイント上の失敗をトリガーする認証制限を設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>dot11 ids eap attempts number period seconds</b>	認証の試みの回数と、アクセスポイント上で失敗をトリガーする <i>EAPOL</i> フラッドの秒数を設定します。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。



## RADIUS サーバと TACACS+ サーバの設定

この章では、Remote Authentication Dial-In User Service (RADIUS) と Terminal Access Controller Access Control System Plus (TACACS+) を有効にして設定する方法について説明します。これは、認証プロセスと許可プロセスに詳細なアカウント情報と柔軟な管理制御を提供します。RADIUS と TACACS+ は AAA を通じて効率化され、AAA コマンド以外では有効に設定できません。



(注) アクセス ポイントをローカル認証サーバとして設定し、メインサーバのバックアップとして使用したり、RADIUS サーバの存在しないネットワークで認証サービスを提供したりできます。アクセス ポイントをローカル認証サーバとして設定する方法の詳細については、[第 11 章「認証タイプの設定」](#)を参照してください。



(注) この章で使用されるコマンドの構文と使用方法の詳細については、リリース 12.2 の『*Cisco IOS Security Command Reference*』を参照してください。

この章の内容は、次のとおりです。

- 「RADIUS の設定と有効化」 (P.13-1)
- 「TACACS+ の設定と有効化」 (P.13-22)

### RADIUS の設定と有効化

この項では、RADIUS を設定して有効にする方法について説明します。次の各項で RADIUS の設定について説明します。

- 「RADIUS の概要」 (P.13-2)
- 「RADIUS の動作」 (P.13-2)
- 「RADIUS の設定」 (P.13-3)
- 「RADIUS の設定の表示」 (P.13-19)
- 「アクセス ポイントが送信する RADIUS 属性」 (P.13-19)

## RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは RADIUS をサポートするシスコ デバイス上で動作し、中央 RADIUS サーバに認証要求を送信します。RADIUS サーバには、ユーザ認証情報とネットワーク サービス アクセス情報がすべて格納されます。RADIUS ホストは、通常、シスコ (Cisco Secure Access Control Server バージョン 3.0)、Livingston、Merit、Microsoft、または他のソフトウェアプロバイダーの RADIUS サーバソフトウェアが稼働しているマルチユーザシステムです。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS は、次のようなアクセス セキュリティを必要とするネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。マルチベンダーのアクセス サーバを使用する IP ベースのネットワークでは、ダイヤルイン ユーザは Kerberos セキュリティ システムと連携するようにカスタマイズされた RADIUS サーバを通じて認証されます。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。これは、スマート カードアクセス コントロール システムを使用するようなアクセス環境です。その例として、ユーザの検証とネットワーク リソースへのアクセス許可に、RADIUS が Enigma のセキュリティ カードとともに使用されています。
- すでに RADIUS を使用中のネットワーク。ネットワークには、RADIUS クライアントを含むシスコ アクセス ポイントを追加できます。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース (時間、パケット、バイトなど) の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP)、NetWare Asynchronous Services Interface (NASI)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

## RADIUS の動作

無線ユーザが、RADIUS サーバによってアクセス コントロールされるアクセス ポイントにログインして認証を試行する場合、ネットワークの認証は [図 13-1](#) に示す手順で実行されます。

図 13-1 EAP 認証のシーケンス

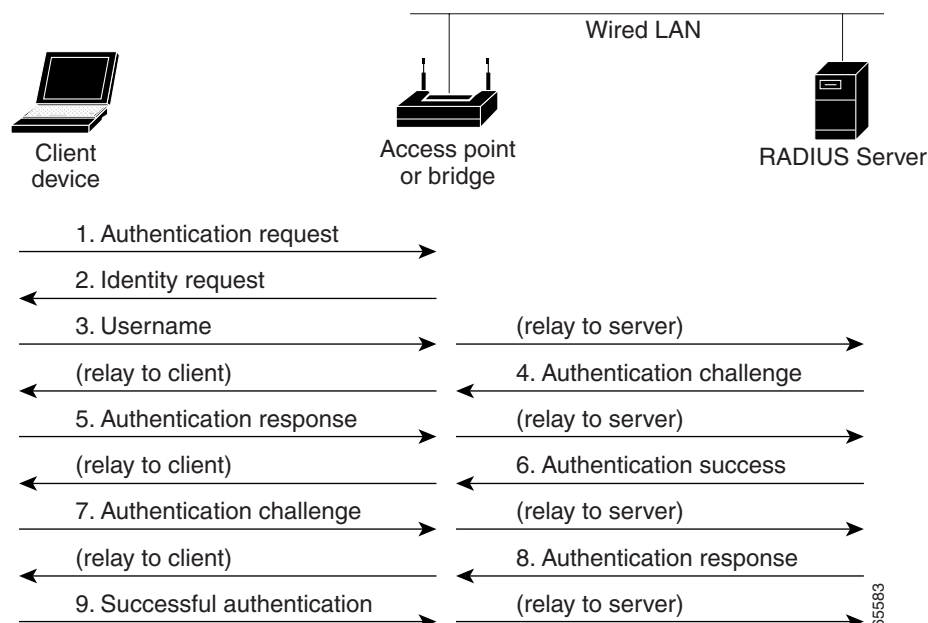


図 13-1 の手順 1 ～ 9 では、無線クライアント デバイスと有線 LAN 上の RADIUS サーバが 802.1x および EAP を使用して、アクセス ポイント経由で相互認証を実行します。RADIUS サーバは、認証身元証明要求をクライアントに送信します。クライアントはユーザが入力したパスワードを一方向暗号化し、認証身元証明要求に対する応答を生成して RADIUS サーバに送信します。RADIUS サーバは、サーバ自体のユーザ データベースの情報から独自の応答を生成し、クライアントからの応答と比較します。RADIUS サーバがクライアントを認証すると、同じ処理が逆方向から繰り返され、今度はクライアントが RADIUS サーバを認証します。

相互認証が終了すると、RADIUS サーバとクライアントは、クライアントに固有の、クライアントに適切なレベルのネットワーク アクセスを提供する WEP キーを決定します。これにより、有線のスイッチド セグメントのセキュリティ レベルは、デスクトップのレベルに近づきます。クライアントはこのキーをロードして、ログインセッションでの使用に備えます。

ログインセッションでは、RADIUS サーバがセッション キーと呼ばれる WEP キーを暗号化して、有線 LAN 経由でアクセス ポイントに送信します。アクセス ポイントは、セッション キーを使用してブロードキャスト キーを暗号化し、クライアントに送信します。クライアントは、送信されてきたキーを、セッション キーを使用して復号化します。クライアントとアクセス ポイントは WEP を有効にし、セッション キーとブロードキャスト WEP キーを残りのセッションの間、すべての通信に対して使用します。

EAP 認証には複数のタイプがありますが、アクセス ポイントはどのタイプについても同じように機能します。つまり、アクセス ポイントは、無線クライアント デバイスと RADIUS サーバ間の認証メッセージを中継します。RADIUS サーバを使用したクライアント認証の設定方法の詳細は、「SSID への認証タイプの割り当て」(P.11-10) を参照してください。

## RADIUS の設定

この項では、RADIUS をサポートするアクセス ポイントの設定方法について説明します。最低限、RADIUS サーバソフトウェアが稼働するホスト (1 つまたは複数) を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウントイングの方式リストを定義できます。

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティプロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

アクセス ポイントに RADIUS 機能を設定する前に、RADIUS サーバにアクセスして設定する必要があります。

ここでは、次の設定情報について説明します。

- 「RADIUS のデフォルト設定」 (P.13-4)
- 「RADIUS サーバ ホストの識別」 (P.13-4) (必須)
- 「RADIUS ログイン認証の設定」 (P.13-7) (必須)
- 「AAA サーバグループの定義」 (P.13-9) (任意)
- 「ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定」 (P.13-11) (任意)
- 「パケット オブ ディスコネクトの設定」 (P.13-12) (任意)
- 「RADIUS アカウンティングの開始」 (P.13-13) (任意)
- 「CSID 形式の選択」 (P.13-14) (任意)
- 「すべての RADIUS サーバの設定」 (P.13-15) (任意)
- 「ベンダー固有の RADIUS 属性を使用するアクセス ポイントの設定」 (P.13-16) (任意)
- 「ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定」 (P.13-17) (任意)
- 「WISPr RADIUS 属性の設定」 (P.13-18) (任意)



(注) RADIUS サーバの CLI コマンドは、**aaa new-model** コマンドを入力するまで無効になっています。

## RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS を有効にすると、CLI を通じてアクセス ポイントにアクセスするユーザを認証できます。

## RADIUS サーバホストの識別

アクセス ポイントと RADIUS サーバ間の通信には、次のいくつかのコンポーネントを使用します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定のユーザ データグラム プロトコル (UDP) ポート番号、または IP アドレスと特定の UDP ポート番号により識別されます。IP アドレスと UDP ポート番号の組み合わせから一意の識別子が作成され、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。



(注) Cisco IOS Release 12.2(8)JA 以降では、RADIUS サーバとアクセス ポイントとの通信に、21645 ~ 21844 の範囲で無作為に選択された UDP ソース ポート番号が使用されます。

同一の RADIUS サーバにアカウントリングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリのフェールオーバー時のバックアップとして機能します。この例では、最初に設定されたホスト エントリがアカウントリング サービスに失敗すると、アクセス ポイントは同じデバイスに設定された 2 番目のホスト エントリにアカウントリング サービスの提供を求めます (RADIUS ホスト エントリは、設定した順序に従って試行されます)。

RADIUS サーバとアクセス ポイントは、共有の身元証明要求テキスト ストリングを使用して、パスワードを暗号化して応答を交換します。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバ デモンを実行しているホストと、アクセス ポイントと共有する身元証明要求テキスト (キー) ストリングを指定する必要があります。

タイムアウト、再送信、暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することも、またはグローバル設定とサーバ単位の設定を組み合わせることも可能です。アクセス ポイントと通信するすべての RADIUS サーバにこれらの設定をグローバルに適用するには、3 つの一意なグローバル コンフィギュレーション コマンド (**radius-server timeout**、**radius-server retransmit**、**radius-server key**) を使用します。これらの設定を特定の RADIUS サーバに適用するには、**radius-server host** グローバル コンフィギュレーション コマンドを使用します。




(注) アクセス ポイントにグローバル機能とサーバ単位の機能 (タイムアウト、再送信、キー コマンド) を同時に設定する場合、サーバ単位のタイマー、再送信、キー値のコマンドがグローバルなタイマー、再送信、キー値のコマンドに優先します。すべての RADIUS サーバに対してこれらの値を設定するには、「すべての RADIUS サーバの設定」(P.13-15) を参照してください。

認証時用に AAA サーバ グループを使用して既存のサーバ ホストをグループ化するようアクセス ポイントを設定できます。詳細については、「AAA サーバ グループの定義」(P.13-9) を参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>aaa new-model</b>	AAA をイネーブルにします。



コマンド	目的
<p><b>ステップ 3</b> <code>radius server {hostname   ip-address}[auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code></p> <p> <b>(注)</b> このコマンドは、以前のリリースでサポートされています。新しいコマンドを使用することを推奨します。</p> <p>次の一連の新しいコマンドがこのリリースで以前のコマンドを置き換える目的で導入されました:</p> <p><code>radius server name</code></p> <p><code>address [IP address ip-address] [auth-port port-number] [acct-port port-number]</code></p>	<p>リモート RADIUS サーバ ホストのサーバ名を指定します。</p> <ul style="list-style-type: none"> <li>• (任意) <code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。(任意) <code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>timeoutseconds</code> には、アクセス ポイントが再送信する前に RADIUS サーバの応答を待つ時間を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドによる設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。</li> <li>• (任意) <code>retransmit retries</code> には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信回数を指定しない場合、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。</li> <li>• (任意) <code>key string</code> には、アクセス ポイントと RADIUS サーバで稼働中の RADIUS デーモンの間で使用される認証と暗号キーを指定します。</li> </ul> <p><b>(注)</b> キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト スtring でなければなりません。キーは常に <code>radius-server host</code> コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。</p> <p>アクセス ポイントが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイントのソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。</p>
<p><b>ステップ 4</b> <code>dot11 ssid ssid-string</code></p>	<p>アカウントを有効にする必要がある、Service Set Identifier (SSID; サービスセット ID) の SSID コンフィギュレーション モードを開始します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。</p>



	コマンド	目的
ステップ 5	<code>accounting list-name</code>	この SSID の RADIUS アカウンティングを有効にします。 <i>list-name</i> には、アカウンティング方式のリストを指定します。 方式のリストの詳細は、次の URL をクリックしてください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2</a>  (注) SSID のアカウンティングを有効にするには、SSID 設定に <code>accounting</code> コマンドを含める必要があります。URL をクリックすると、SSID コンフィギュレーション モード <code>accounting</code> コマンドの詳細が表示されます。  <a href="http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_command_reference_chapter09186a008041757f.html#wp2449819">http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_command_reference_chapter09186a008041757f.html#wp2449819</a>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定の RADIUS サーバを削除するには、`no radius-server host {hostname | ip-address}` グローバル コンフィギュレーション コマンドを使用します。

次に、1 つの RADIUS サーバを認証用に、もう 1 つの RADIUS サーバをアカウンティング用に設定する例を示します。

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例は、RADIUS アカウンティング用に SSID を設定する方法を示しています。

```
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
```

次に、`host1` を RADIUS サーバとして設定し、認証およびアカウンティングの両方にデフォルトのポートを使用するように設定する例を示します。

```
AP(config)# radius-server host host1
```



(注) RADIUS サーバ上でも、いくつかの値を設定する必要があります。その設定には、アクセス ポイントの IP アドレスおよびサーバとアクセス ポイントで共有するキー ストリングが含まれます。詳細については、RADIUS サーバのマニュアルを参照してください。

## RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リスト（偶然に `default` と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login {default   list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li><b>login authentication</b> コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。リスト名の詳細は、次のリンクをクリックしてください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios12/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2">http://www.cisco.com/univercd/cc/td/doc/product/software/ios12/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2</a></li> <li><b>method1...</b> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li><b>line</b> : 回線パスワードを認証に使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。<b>password password</b> ライン コンフィギュレーション コマンドを使用します。</li> <li><b>local</b> : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。<b>username password</b> グローバル コンフィギュレーション コマンドを使用します。</li> <li><b>radius</b> : RADIUS 認証を使用します。この認証方式を使用するには、事前に RADIUS サーバを設定しておく必要があります。詳細については、「<a href="#">RADIUS サーバ ホストの識別</a>」(P.13-4) を参照してください。</li> </ul>
ステップ 4	<code>line [console   tty   vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。

	コマンド	目的
ステップ 5	<code>login authentication {default   list-name}</code>	回線または回線セットに対して、認証リストを適用します。 <ul style="list-style-type: none"> <li><code>default</code> を指定する場合は、<code>aaa authentication login</code> コマンドで作成したデフォルトのリストを使用します。</li> <li><code>list-name</code> には、<code>aaa authentication login</code> コマンドで作成したリストを指定します。</li> </ul>
ステップ 6	<code>radius-server attribute 32 include-in-access-req format %h</code>	認証時に NAS_ID 属性でシステム名を送信するようにアクセスポイントを設定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	入力内容を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、`no aaa authentication login {default | list-name} method1 [method2...]` グローバル コンフィギュレーション コマンドを使用します。ログインに関する RADIUS 認証をディセーブルにする、あるいはデフォルト値に戻すには、`no login authentication {default | list-name}` ライン コンフィギュレーション コマンドを使用します。

## AAA サーバグループの定義

認証時に AAA サーバグループを使用して既存のサーバホストをグループ化するようアクセスポイントを設定できます。設定済みのサーバホストのサブセットを選択して、それを特定のサービスに使用します。サーバグループは、選択されたサーバホストの IP アドレスのリストを含むグローバルなサーバホスト リストとともに使用されます。

サーバグループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意的 ID (IP アドレスと UDP ポート番号の組み合わせ) を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。同一の RADIUS サーバにアカウントリングなど同じサービスを実行する 2 つのホスト エントリを設定すると、2 番目に設定されたホスト エントリは最初のホスト エントリのフェールオーバー時のバックアップとして機能します。

定義したグループサーバに特定のサーバを対応付けるには、`server` グループサーバ コンフィギュレーション コマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の `auth-port` および `acct-port` キーワードを使用して複数のホスト インスタンスまたはエントリを特定することもできます。

AAA サーバグループを定義し、そのグループに特定の RADIUS サーバを対応付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
<b>ステップ 3</b> <code>radius-server host {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> <li>（任意）<code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。</li> <li>（任意）<code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。</li> <li>（任意）<code>timeoutseconds</code> には、アクセス ポイントが再送信する前に RADIUS サーバの応答を待つ時間を指定します。指定できる範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドによる設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。</li> <li>（任意）<code>retransmit retries</code> には、サーバが応答しない場合、または応答が遅い場合に、RADIUS 要求をサーバに再送信する回数を指定します。指定できる範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信回数を指定しない場合、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。</li> <li>（任意）<code>key string</code> には、アクセス ポイントと RADIUS サーバで稼働中の RADIUS デーモンの間で使用される認証と暗号キーを指定します。</li> </ul> <p><b>(注)</b> キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。キーは常に <code>radius-server host</code> コマンドの最後のアイテムとして設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないとください。</p> <p>アクセス ポイントが単一の IP アドレスと関連付けられた複数のホスト エントリを認識するように設定するには、このコマンドを必要な数だけ入力します。その際、各 UDP ポート番号が異なっていることを確認してください。アクセス ポイントのソフトウェアは、指定された順序でホストを検索します。各 RADIUS ホストで使用するタイムアウト、再送信回数、および暗号キーの値をそれぞれ設定してください。</p>
<b>ステップ 4</b> <code>aaa group server radius group-name</code>	<p>AAA サーバ グループを、特定のグループ名で定義します。</p> <p>このコマンドを実行すると、アクセス ポイントはサーバ グループ コンフィギュレーション モードへ移行します。</p>
<b>ステップ 5</b> <code>server ip-address</code>	<p>特定の RADIUS サーバを定義済みのサーバグループに対応付けます。AAA サーバグループの RADIUS サーバごとに、このステップを繰り返します。</p> <p>グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。</p>
<b>ステップ 6</b> <code>end</code>	<p>特権 EXEC モードに戻ります。</p>

	コマンド	目的
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「 <a href="#">RADIUS ログイン認証の設定</a> 」(P.13-7) を参照してください。

特定の RADIUS サーバを削除するには、`no radius-server host {hostname | ip-address}` グローバル コンフィギュレーション コマンドを使用します。サーバ グループをコンフィギュレーション リストから削除するには、`no aaa group server radius group-name` グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、`no server ip-address` サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、アクセス ポイントは異なる 2 つの RADIUS グループ サーバ (`group1` と `group2`) を認識するように設定されます。`group1` では、同じ RADIUS サーバ上の異なる 2 つのホスト エントリを、同じサービス用に設定しています。2 番目のホスト エントリが、最初のエントリのフェールオーバー バックアップとして動作します。

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

## ユーザ イネーブル アクセスおよびネットワーク サービスに関する RADIUS 許可の設定

AAA 認証によってユーザが使用できるサービスが制限されます。AAA 許可が有効の場合、アクセス ポイントはユーザのプロファイルから取得した情報を使用してユーザのセッションを設定します。ユーザのプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。



(注) この項では、アクセス ポイント管理者向けの許可の設定について説明します。無線クライアント デバイス向けの許可の設定は説明しません。

グローバル コンフィギュレーション コマンド `aaa authorization` と `radius` キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

`aaa authorization exec radius local` コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network radius</code>	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるようにアクセス ポイントを設定します。
ステップ 3	<code>aaa authorization exec radius</code>	ユーザの RADIUS 許可でユーザの特権 EXEC アクセス権の有無を判断するように、アクセス ポイントを設定します。  <b>exec</b> キーワードを指定すると、ユーザ プロファイル情報 ( <b>autocommand</b> 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

## パケット オブ ディスコネクトの設定

Packet of Disconnect (PoD; パケット オブ ディスコネクト) は、ディスコネクト メッセージとも呼ばれています。PoD の詳細は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) Internet Standard RFC 3576 で参照できます。

パケット オブ ディスコネクトは、検出されたセッションを終了させる方式で構成されています。PoD は RADIUS Disconnect\_Request パケットであり、RADIUS access\_accept パケットによりセッションが承認された後、認証するエージェント サーバがユーザを接続解除するときに使用されるようになっています。これが必要な場合としては、少なくとも次の 2 つの状況が考えられます。

- 不正使用の検出。これは、コールを承認後でなければ実行できません。
- プリペイド アクセス時間が切れたホット スポット ユーザの切断。

セッションが終了すると、RADIUS サーバは Network Access Server (NAS; ネットワーク アクセス サーバ) (WDS またはアクセス ポイント) に切断メッセージを送信します。802.11 セッションには、Pod 要求で Calling-Station-ID [31] RADIUS 属性 (クライアントの MAC アドレス) を指定する必要があります。アクセス ポイントまたは WDS は、関連するセッションのアソシエーションを解除しようとし、次に接続解除応答メッセージを RADIUS サーバに返送します。メッセージ タイプは次のとおりです。

- 40 : 切断要求
- 41 : 切断 : ACK
- 42 : 切断 : NAK



(注) PoD 要求の設定法については、ご使用の RADIUS サーバ アプリケーションの資料を参照してください。



(注) アクセス ポイントは、再アソシエーションしようとするクライアントの次の試みを妨害しません。PoD 要求を発行する前にクライアントのアカウントを無効にするのは、セキュリティ管理者の責任です。



(注) WDS を設定すると、PoD 要求は WDS に対して発行されます。WDS はアソシエーション解除の要求を親アクセス ポイントに転送してから、そのセッションを自身の内部テーブルから削除します。



(注) PoD は Cisco CNS Access Registrar (CAR) RADIUS サーバでサポートされていますが、Cisco Secure ACS Server v4.0 以前ではサポートされていません。

特権 EXEC モードから、次の手順に従って PoD を設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa pod server [port port number] [auth-type {any   all   session-key}] [clients client 1...] [ignore {server-key string...   session-key }   server-key string...]</code>	<p>特定のセッション属性が提供されると、RADIUS サーバからの要求により切断されるユーザセッションを有効にします。</p> <p><b>port port number</b> : (任意) アクセス ポイントが PoD 要求をリスンする UDP ポート。デフォルト値は 1700 です。</p> <p><b>auth-type</b> : このパラメータは、802.11 セッションに対してはサポートされません。</p> <p><b>clients</b> (任意) : 4 台までの RADIUS サーバをクライアントとして指名できます。この設定が存在し、リストにないデバイスからの PoD 要求が発信される場合、拒否されます。</p> <p><b>ignore</b> (任意) : <code>server_key</code> に設定すると、PoD 要求を受信したときに共有の身元証明要求は検証されません。</p> <p><b>session-key</b> : 802.11 セッションに対してはサポートされません。</p> <p><b>server-key</b> : 共有秘密テキスト スtring を設定します。 <b>string</b> : ネットワーク アクセス サーバとクライアント ワークステーション間で共有される事前共有キー。この共有身元証明要求は両方のシステムで同一である必要があります。</p> <p>(注) このパラメータ以降に入力されたデータは、共有の身元証明要求 String として扱われます。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## RADIUS アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングが有効の場合、アクセス ポイントはアカウンティングの記録の形式でユーザ アクティビティを RADIUS セキュリティ サーバに報

告します。各アカウントングレコードにはアカウントングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アクセスポイントに送信される属性の詳細なリストについては、「[アクセスポイントが送信する RADIUS 属性](#)」(P.13-19) を参照してください。

Cisco IOS の権限レベルおよびネットワークサービスに関する RADIUS アカウントングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa accounting network start-stop radius</code>	ネットワーク関連のすべてのサービス要求について、RADIUS アカウントングをイネーブルにします。
ステップ 3	<code>ip radius source-interface bvi1</code>	アカウントングの記録として BVI IP アドレスを NAS_IP_ADDRESS 属性で送信するようにアクセスポイントを設定します。
ステップ 4	<code>aaa accounting update periodic minutes</code>	アカウントングの更新間隔を分で入力します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウントングをディセーブルにするには、`no aaa accounting {network | exec} {start-stop} method1...` グローバル コンフィギュレーション コマンドを使用します。

## CSID 形式の選択

RADIUS パケット内の Called-Station-ID (CSID) および Calling-Station-ID 属性に対する MAC アドレスの形式を選択できます。`dot11 aaa csid` グローバル コンフィギュレーション コマンドを使用して CSID 形式を選択します。表 13-1 は、対応する MAC アドレスの例付きで示した形式のオプションです。

表 13-1 CSID 形式オプション

オプション	MAC アドレスの例
デフォルト	0007.85b3.5f4a
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

デフォルトの CSID 形式に戻すには、`dot11 aaa csid` コマンドで `no` を指定するか、`dot11 aaa csid default` と入力します。



(注) また `wlccp wds aaa csid` コマンドを使用しても CSID 形式を選択できます。



## すべての RADIUS サーバの設定

特権 EXEC モードから、次の手順に従ってアクセス ポイントとすべての RADIUS サーバ間のグローバル通信設定を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server key string</code>	アクセス ポイントとすべての RADIUS サーバ間で使用する共有の身元証明要求テキスト ストリングを指定します。  (注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 3	<code>radius-server retransmit retries</code>	アクセス ポイントが RADIUS 要求をサーバに送信して、中止するまでの回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ~ 1000 です。
ステップ 4	<code>radius-server timeout seconds</code>	アクセス ポイントが RADIUS 要求を再送する前に、要求への応答を待機する時間を秒数で指定します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 です。
ステップ 5	<code>radius-server deadtime minutes</code>	このコマンドは、Cisco IOS ソフトウェアで認証要求に応答しない RADIUS サーバを「dead」とマークして、要求の待機がタイムアウトになる前に、設定された次のサーバを試行する場合に使用します。dead とマークされている RADIUS サーバでは、指定する時間の間（最大 1440 分、24 時間）、追加の要求はスキップされます。  (注) このコマンドは、複数の RADIUS サーバを定義するときに必要な設定です。設定しない場合、クライアントの認証が行われません。定義される RADIUS サーバが 1 台の場合、このコマンドはオプションです。
ステップ 6	<code>radius-server attribute 32 include-in-access-req format %h</code>	認証時に NAS_ID 属性でシステム名を送信するようにアクセス ポイントを設定します。
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>show running-config</code>	設定値を確認します。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例では、2 つのメイン サーバとローカル認証サーバについて、サーバのデッド タイムを 10 分間に設定する方法を示します。

```
AP(config)# aaa new-model
```

```
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
```

```
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
```

```
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
```

```
AP(config)# radius-server deadtime 10
```

再送信、タイムアウト、デッドタイムをデフォルトの設定に戻すには、それぞれのコマンドで **no** 形式を使用します。

## ベンダー固有の RADIUS 属性を使用するアクセスポイントの設定

Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) のドラフト規格では、アクセスポイントと RADIUS サーバ間で、ベンダー固有の属性 (属性 26) を使用してベンダー固有の情報をやり取りする方法を指定しています。各ベンダーは、Vendor-Specific Attribute (VSA) を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9 で、サポートされるオプションはベンダータイプ 1、名前は *cisco-avpair* です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

*protocol* は、特定の許可タイプに使用するシスコのプロトコル属性の値です。*attribute* と *value* は、Cisco TACACS+ 仕様で定義された該当 AV ペアです。*sep* には、必須属性の場合は = を、オプション属性の場合はアスタリスク (\*) を指定します。このコマンドにより、TACACS+ 許可で使用できる全機能が RADIUS でも使用できます。

たとえば、次の AV ペアは IP 許可の際 (PPP の IPCP アドレス割り当ての際)、シスコの *multiple named ip address pools* 機能を有効にします。

```
cisco-avpair= "ip:addr-pool=first"
```

次の例は、特権 EXEC コマンドへの即時アクセスを使用して、ユーザがアクセスポイントからログインする方法を示しています。

```
cisco-avpair= "shell:priv-lvl=15"
```

他のベンダーには、そのベンダー固有の ID、オプション、関連 VSA があります。ベンダーの ID と VSA についての詳細は、RFC 2138 「Remote Authentication Dial-In User Service (RADIUS)」を参照してください。

特権 EXEC モードから、次の手順に従って、VSA を認識して使用するようアクセスポイントを設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>radius-server vsa send [accounting   authentication]</b>	アクセスポイントが RADIUS IETF 属性 26 で定義された VSA を認識して使用できるようにします。 <ul style="list-style-type: none"> <li>• (任意) 認識されるベンダー固有属性の集合をアカウントング属性だけに限定するには、<b>accounting</b> キーワードを使用します。</li> <li>• (任意) 認識されるベンダー固有属性の集合を認証属性だけに限定するには、<b>authentication</b> キーワードを使用します。</li> </ul> キーワードを指定せずにこのコマンドを入力すると、アカウントングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	設定値を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

RADIUS 属性の詳細なリスト、または VSA 26 の詳細は、リリース 12.2 の『Cisco IOS Security Configuration Guide』の付録「RADIUS Attributes」を参照してください。

## ベンダー専用の RADIUS サーバ通信用アクセス ポイントの設定

IETF の RADIUS ドラフト規格では、アクセス ポイントと RADIUS サーバの間でベンダー専用の情報を通信する方法を指定していますが、一部のベンダーは RADIUS 属性セットを独自の方法で拡張しています。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

すでに説明したように、ベンダー専用または IETF ドラフト準拠の RADIUS を設定するには、RADIUS サーバ デーモンを実行しているホストと、そのホストがアクセス ポイントを共有する身元証明要求テキストを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** グローバル コンフィギュレーション コマンドを使用します。

ベンダー独自仕様の RADIUS サーバ ホスト、および共有されるシークレット テキスト ストリングを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>radius-server host {hostname   ip-address} non-standard</b>	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ホストがベンダー専用の RADIUS 実装を使用していることを識別します。
ステップ 3	<b>radius-server key string</b>	アクセス ポイントとベンダー専用の RADIUS サーバ間で使用する共有の身元証明要求テキスト ストリングを指定します。アクセス ポイントと RADIUS サーバは、このテキスト ストリングを使用して、パスワードを暗号化し応答を交換します。  (注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されません。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	設定値を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

ベンダー独自仕様の RADIUS ホストを削除するには、**no radius-server host {hostname | ip-address} non-standard** グローバル コンフィギュレーション コマンドを使用します。キーをディセーブルにするには、**no radius-server key** グローバル コンフィギュレーション コマンドを使用します。

次の例は、ベンダー専用の RADIUS ホストを指定して、アクセス ポイントとサーバ間で秘密キー `rad124` を使用する方法を示しています。

```
AP(config)# radius-server host 172.20.30.15 nonstandard
AP(config)# radius-server key rad124
```

## WISPr RADIUS 属性の設定

Wi-Fi アライアンスの資料である『*WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming*』には、アクセス ポイントが RADIUS アカウンティングおよび認証要求とともに送信しなければならない RADIUS 属性が示されています。現在アクセス ポイントは、WISPr ロケーション名、ISO と International Telecommunications Union (ITU; 国際電気通信連合) の国番号とエリア コード属性だけをサポートしています。`snmp-server location` コマンドと `dot11 location isocc` コマンドを使用して、アクセス ポイントでこれらの属性を設定します。

また、『*WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming*』には、RADIUS 認証応答とアカウンティング要求でクラス属性をアクセス ポイントに加えることも指示されています。アクセス ポイントは自動的にクラス属性を加えるため、設定する必要はありません。

ISO と ITU の国番号とエリア コードのリストは、ISO と ITU の Web サイトにあります。Cisco IOS ソフトウェアは、アクセス ポイントで設定された国番号とエリア コードの有効性を確認しません。

特権 EXEC モードから、次の手順に従ってアクセス ポイントに WISPr RADIUS 属性を指定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server location location</code>	WISPr の場所名属性を指定します。『 <i>WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming</i> 』では、次の形式で場所名を入力することを推奨しています。 <code>hotspot_operator_name,location</code>
ステップ 3	<code>dot11 location isocc ISO-country-code cc country-code ac area-code</code>	アクセス ポイントがアカウンティング要求と認証要求に加える ISO と ITU の国番号とエリア コードを指定します。 <ul style="list-style-type: none"> <li>• <code>isocc ISO-country-code</code> : アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ISO 国番号を指定します。</li> <li>• <code>cc country-code</code> : アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ITU 国番号を指定します。</li> <li>• <code>ac area-code</code> : アクセス ポイントが RADIUS 認証とアカウンティング要求に加える ITU エリア コードを指定します。</li> </ul>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show running-config</code>	設定値を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、WISPr の場所名属性を設定する方法を示しています。

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

次の例は、アクセス ポイントで ISO と ITU のロケーション コードを設定する方法を示しています。

```
ap# dot11 location isocc us cc 1 ac 408
```

次の例は、アクセス ポイントがクライアント デバイスの使用する SSID を追加して場所 ID ストリングをフォーマットする方法を示しています。

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

## RADIUS の設定の表示

RADIUS の設定を表示するには、`show running-config` 特権 EXEC コマンドを使用します。



(注)

アクセス ポイントで DNS が設定されている場合、`show running-config` コマンドはサーバの名前の代わりに IP アドレスを表示することがあります。

## アクセス ポイントが送信する RADIUS 属性

表 13-2 から 表 13-6 は、アクセス ポイントがクライアントに送信するアクセス要求、アクセス許可、アカウント要求パケット中の属性を示しています。



(注)

Wi-Fi アライアンスの資料『*WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming*』で推奨されているように、RADIUS アカウント要求と認証要求の属性に加えるように、アクセス ポイントを設定できます。詳細は、「[WISPr RADIUS 属性の設定](#)」(P.13-18) を参照してください。

表 13-2 アクセス要求パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID (MAC アドレス)
31	Calling-Station-ID (MAC アドレス)

表 13-2 アクセス要求パケットで送信される属性

属性 ID	説明
32	NAS-Identifier <sup>1</sup>
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

1. 属性 32 (include-in-access-req) が設定されている場合、アクセス ポイントは NAS-Identifier を送信します。

表 13-3 アクセス許可パケットで送信される属性

属性 ID	説明
25	Class
27	Session-Timeout
64	Tunnel-Type <sup>1</sup>
65	Tunnel-Medium-Type <sup>1</sup>
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID <sup>1</sup>
VSA (属性 26)	LEAP session-key
VSA (属性 26)	auth-algo-type
VSA (属性 26)	SSID

1. RFC2868、VLAN オーバーライド番号を定義

表 13-4 アカウンティング要求 (開始) パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type
VSA (属性 26)	SSID
VSA (属性 26)	NAS-Location
VSA (属性 26)	Cisco-NAS-Port
VSA (属性 26)	Interface

表 13-5 アカウンティング要求 (更新) パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA (属性 26)	SSID
VSA (属性 26)	NAS-Location
VSA (属性 26)	VLAN-ID
VSA (属性 26)	Connect-Progress
VSA (属性 26)	Cisco-NAS-Port
VSA (属性 26)	Interface

表 13-6 アカウンティング要求 (終了) パケットで送信される属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause

表 13-6 アカウンティング要求 (終了) パケットで送信される属性 (続き)

属性 ID	説明
61	NAS-Port-Type
VSA (属性 26)	SSID
VSA (属性 26)	NAS-Location
VSA (属性 26)	Disc-Cause-Ext
VSA (属性 26)	VLAN-ID
VSA (属性 26)	Connect-Progress
VSA (属性 26)	Cisco-NAS-Port
VSA (属性 26)	Interface
VSA (属性 26)	auth-algo-type



(注)

デフォルトでは、アクセス ポイントは `service-type` 属性を `authenticate-only` に設定した状態で、再認証要求を認証サーバに送信します。ただし、Microsoft IAS サーバの中には、`authenticate-only` の `service-type` 属性をサポートしていないものがあります。ユーザの要件に応じて、`service-type` 属性を `dot11 aaa authentication attributes service-type login-user` または `dot11 aaa authentication attributes service-type framed-user` に設定してください。デフォルトでは、アクセス要求に応じてサービス タイプ「login」が送信されます。

## TACACS+ の設定と有効化

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」 (P.13-22)
- 「TACACS+ の動作」 (P.13-23)
- 「[Configuring TACACS+]」 (P.13-24)
- 「TACACS+ 設定の表示」 (P.13-28)

## TACACS+ の概要

TACACS+ は、アクセス ポイントにアクセスしようとするユーザを集中的に検証するセキュリティアプリケーションです。RADIUS とは異なり、TACACS+ はアクセス ポイントにアソシエートされたクライアント デバイスを認証しません。

TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デモンのデータベースで管理されます。アクセス ポイントに TACACS+ 機能を設定する前に、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ (TACACS+ デモン) が各サービス (認証、許可、およびアカウンティング) を別個に提供します。各サービスを固有のデータベースに結合し、デモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインとパスワードのダイアログ、身元証明要求と応答、メッセージのサポートを通じて管理者の認証を完全に制御します。

認証機能は、管理者との対話を実行できます（たとえば、ユーザ名とパスワードが入力された後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号など、複数の質問でユーザの身元を確認します）。また TACACS+ 認証サービスは、管理者の画面にメッセージを送信できます。たとえば、会社のパスワード エージング ポリシーに従い、パスワードを変更する必要があることをメッセージで管理者に通知することができます。

- 許可：管理者のセッション期間中の管理機能を詳細に制御します。これには自動コマンドの設定、アクセス コントロール、セッション期間、またはプロトコル サポートなどが含まれますが、それに限定されません。また、管理者が TACACS+ 許可機能で実行できるコマンドを強制的に制限できます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワーク マネージャはアカウンティング機能を使用して、セキュリティ監査時に管理者アクティビティを追跡したり、またはユーザの課金時に情報を提供できます。アカウンティング レコードには、管理者 ID、開始時間と終了時間、実行されたコマンド（PPP など）、パケット数、バイト数が含まれます。

TACACS+ プロトコルは、アクセス ポイントと TACACS+ デーモンの間で認証を実行します。アクセス ポイントと TACACS+ デーモンの間で実行されるすべてのプロトコル交換が暗号化されるため、認証の機密性を保証します。

アクセス ポイントで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアを実行するシステムが必要です。

## TACACS+ の動作

管理者が TACACS+ を使用してアクセス ポイントの認証を受け、簡単な ASCII ログインを試行した場合、次のプロセスが発生します。

1. 接続が確立されると、アクセス ポイントは TACACS+ デーモンに連絡してユーザ名プロンプトを取得し、このプロンプトが管理者に表示されます。管理者がユーザ名を入力すると、アクセス ポイントは TACACS+ デーモンにアクセスしてパスワード プロンプトを取得します。アクセス ポイントは管理者にパスワード プロンプトを表示し、管理者がパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

TACACS+ を使用してデーモンと管理者との間で会話が続けられ、デーモンは管理者の認証に必要な情報を取得します。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう求めますが、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. アクセス ポイントは最終的に、TACACS+ デーモンから次に示す応答のいずれかを受信します。
  - ACCEPT：管理者が認証され、サービスが開始します。許可を要求するようにアクセス ポイントが設定されている場合、この時点で許可が開始します。
  - REJECT：管理者は認証されません。管理者は TACACS+ デーモンに従ってアクセスが拒否されるか、ログイン シーケンスを再試行するように要求されます。
  - ERROR：デーモンによる認証のある時点、またはデーモンとアクセス ポイント間のネットワーク接続のある時点で、エラーが発生しています。ERROR 応答を受信した場合、通常、アクセス ポイントは、別の方法で管理者の認証を試行します。
  - CONTINUE：管理者は追加の認証情報を要求されます。

認証の後、アクセス ポイントで許可が有効になっている場合、管理者はさらに許可フェーズに進みます。管理者は TACACS+ 許可に進む前に、まず TACACS+ 認証を完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。ACCEPT 応答が返された場合、この応答には属性の形でその管理者に EXEC または NETWORK セッションを指示するデータが含まれており、管理者がアクセスできる下記のサービスを決定できます。
  - Telnet、rlogin、または特権 EXEC サービス
  - 接続パラメータ。ホストまたはクライアントの IP アドレス、アクセス リスト、管理者のタイムアウトが含まれます。

## 「Configuring TACACS+」

この項では、TACACS+ をサポートするアクセス ポイントの設定方法について説明します。最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウントिंगの方式リストを定義できます。方式リストは管理者アカウントの認証、許可、管理に使用される手順と方法を定義します。方式リストを使用して、使用するセキュリティプロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップ システムが確保されます。このソフトウェアは、リストの先頭の方式を使用して管理者のアカウントを認証、許可、または管理します。その方式が応答しない場合には、リストの次の方式が選択されます。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

ここでは、次の設定情報について説明します。

- 「TACACS+ のデフォルト設定」 (P.13-24)
- 「TACACS+ サーバ ホストの特定および認証キーの設定」 (P.13-24)
- 「TACACS+ ログイン認証の設定」 (P.13-25)
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」 (P.13-27)
- 「TACACS+ アカウントिंगの起動」 (P.13-28)

## TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ を有効にすると、CLI を通じてアクセス ポイントにアクセスする管理者を認証できます。

## TACACS+ サーバホストの特定および認証キーの設定

認証時に単一サーバまたは AAA サーバグループを使用して既存のサーバ ホストをグループ化するようにアクセス ポイントを設定できます。サーバをグループ化して設定済みサーバ ホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバグループは、グローバル サーバ ホスト リストとともに使用され、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ サーバを維持する IP ホストを特定し、任意で暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>tacacs-server host hostname [port integer] [timeout integer] [key string]</code>	TACACS+ サーバを維持する IP ホスト (1 つまたは複数) を特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 <ul style="list-style-type: none"> <li>• <code>hostname</code> には、ホストの名前または IP アドレスを指定します。</li> <li>• (任意) <code>port integer</code> には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ~ 65535 です。</li> <li>• (任意) <code>timeout integer</code> には、タイムアウトになってアクセスポイントがエラーを宣言するまでにデーモンからの応答を待機する時間を秒数で指定します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 秒です。</li> <li>• (任意) <code>key string</code> には、アクセスポイントと TACACS+ デーモンの間の全トラフィックを暗号化および復号化するための暗号キーを指定します。暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。</li> </ul>
ステップ 3	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa group server tacacs+ group-name</code>	(任意) AAA サーバグループを、特定のグループ名で定義します。このコマンドは、アクセスポイントをサーバグループサブコンフィギュレーションモードに移行します。
ステップ 5	<code>server ip-address</code>	(任意) 特定の TACACS+ サーバを定義済みのサーバグループに対応付けます。AAA サーバグループの TACACS+ サーバごとに、このステップを繰り返します。  グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show tacacs</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host hostname** グローバル コンフィギュレーション コマンドを使用します。サーバグループをコンフィギュレーション リストから削除するには、**no aaa group server tacacs+ group-name** グローバル コンフィギュレーション コマンドを使用します。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバグループ サブコンフィギュレーション コマンドを使用します。

## TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義し、そのリストを各種のインターフェイスに適用します。この方式リストは、実行される認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式が実行されるようにするには、この方式リストを特定のインターフェイスに適用しておく必要があります。唯一の例外はデフォルトの方式リス

ト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストには、管理者を認証するクエリのシーケンスと認証方式が記述されています。認証に使用する 1 つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのどの認証にも失敗する場合、つまりセキュリティサーバまたはローカルユーザ名データベースが管理者アクセス権の拒否を応答した場合、認証プロセスは停止して、他の認証方式は試行されません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login {default   list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li>• <b>login authentication</b> コマンドに名前付きリストが指定されなかった場合に使用されるデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。</li> <li>• <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。</li> <li>• <i>method1...</i> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li>• <b>line</b> : 回線パスワードを認証に使用します。この認証方式を使用する前に、回線パスワードを定義する必要があります。 <b>password password</b> ライン コンフィギュレーション コマンドを使用します。</li> <li>• <b>local</b> : ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。 <b>username password</b> グローバル コンフィギュレーション コマンドを使用します。</li> <li>• <b>tacacs+</b> : TACACS+ 認証を使用します。この認証方式を使用するには、事前に TACACS+ サーバを設定しておく必要があります。</li> </ul>
ステップ 4	<code>line [console   tty   vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。

	コマンド	目的
ステップ 5	<code>login authentication {default   list-name}</code>	回線または回線セットに対して、認証リストを適用します。 <ul style="list-style-type: none"> <li><code>default</code> を指定する場合は、<code>aaa authentication login</code> コマンドで作成したデフォルトのリストを使用します。</li> <li><code>list-name</code> には、<code>aaa authentication login</code> コマンドで作成したリストを指定します。</li> </ul>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	入力内容を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、`no aaa authentication login {default | list-name} method1 [method2...]` グローバル コンフィギュレーション コマンドを使用します。ログインに関する TACACS+ 認証をディセーブルにする、あるいはデフォルト値に戻すには、`no login authentication {default | list-name}` ライン コンフィギュレーション コマンドを使用します。

## 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可は、管理者が使用できるサービスを制限します。AAA 許可が有効の場合、アクセスポイントは管理者のプロファイルから取得した情報を使用して管理者のセッションを設定します。管理者のプロファイルは、ローカル ユーザ データベースかセキュリティ サーバにあります。管理者が要求したサービスへのアクセスが許可されるのは、管理者プロファイル内の情報により許可された場合だけです。

`tacacs+` キーワードを指定してグローバル コンフィギュレーション コマンド `aaa authorization` を使用すると、管理者のネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

`aaa authorization exec tacacs+ local` コマンドは、次の許可パラメータを設定します。

- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



(注) CLI を通してログインした認証済み管理者は、許可が設定されていても許可が省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa authorization network tacacs+</code>	ネットワーク関連のすべてのサービス要求に対して、管理者の TACACS+ 許可が受け入れられるようにアクセスポイントを設定します。

	コマンド	目的
ステップ 3	<code>aaa authorization exec tacacs+</code>	管理者の TACACS+ 許可に管理者が特権 EXEC アクセス権を持っているかどうかを判断するように、アクセス ポイントを設定します。 <code>exec</code> キーワードを指定すると、ユーザ プロファイル情報 ( <code>autocommand</code> 情報など) が返される場合があります。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

許可をディセーブルにするには、`no aaa authorization {network | exec} method1` グローバル コンフィギュレーション コマンドを使用します。

## TACACS+ アカウンティングの起動

AAA アカウンティング機能は、管理者がアクセスしているサービスと、サービスが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングが有効の場合、アクセス ポイントはアカウンティングの記録の形で管理者のアクティビティを TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント 請求、または監査のために分析できます。

Cisco IOS の権限レベルおよびネットワーク サービスに関する TACACS+ アカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa accounting network start-stop tacacs+</code>	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 3	<code>aaa accounting exec start-stop tacacs+</code>	TACACS+ アカウンティングにより、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信するように設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウンティングをディセーブルにするには、`no aaa accounting {network | exec} {start-stop} method1...` グローバル コンフィギュレーション コマンドを使用します。

## TACACS+ 設定の表示

TACACS+ サーバ統計情報を表示するには、`show tacacs` 特権 EXEC コマンドを使用します。



## VLAN の設定

---

この章では、有線 LAN に設定された VLAN を使って動作するようにアクセス ポイントを設定する方法について説明します。この章の内容は、次のとおりです。

- 「VLAN の概要」 (P.14-2)
- 「VLAN の設定」 (P.14-4)
- 「VLAN の設定例」 (P.14-10)

## VLAN の概要

VLAN は、物理的または地理的な基準ではなく、機能、プロジェクト チーム、あるいはアプリケーション別に論理的にセグメント化したスイッチド ネットワークです。たとえば、特定の作業グループ チームが使用するワークステーションおよびサーバを、ネットワークへの物理的接続や他のチームと混ざり合っている可能性などにかかわらず、すべて同じ VLAN に接続できます。VLAN によるネットワークの再設定は、デバイスやケーブルを物理的に取り外したり移動したりするのではなく、ソフトウェアを使って行います。

VLAN は、定義されたスイッチのセット内に存在するブロードキャスト ドメインと考えることができます。VLAN は、1 つのブリッジング ドメインによって接続された、ホストかネットワーク機器（ブリッジやルータなど）のいずれかに該当する複数のエンド システムで構成されます。ブリッジング ドメインは、さまざまなネットワーク機器でサポートされています。たとえば LAN スイッチは、VLAN ごとに異なるグループを使用して、スイッチ間のブリッジング プロトコルを処理します。

VLAN は、通常は LAN 設定のルータによって提供されるセグメンテーション サービスを提供します。VLAN はスケーラビリティ、セキュリティ、およびネットワーク管理に対応します。スイッチド LAN ネットワークを設計し構築する際は、いくつかの主要な問題を考慮する必要があります。

- LAN セグメンテーション
- セキュリティ
- ブロードキャスト制御
- パフォーマンス
- ネットワーク管理
- VLAN 間の通信

VLAN は、アクセス ポイントに IEEE 802.11Q タグ認識を追加することにより、無線 LAN に拡張することができます。異なる VLAN を宛先とするフレームは、Wired Equivalent Privacy (WEP) キーの異なる複数の Service Set Identifier (SSID; サービス セット ID) にアクセス ポイントによって無線送信されます。その VLAN と関連付けられたクライアントだけが、これらのパケットを受信できます。反対に、特定の VLAN と関連付けられたクライアントから送信されたパケットは、802.11Q タグが付加されてから、有線ネットワークに転送されます。

アクセス ポイントのファストイーサネット インターフェイスで 802.1q が設定されていると、そのアクセス ポイントは、VLAN1 が定義されていない場合でも、常に VLAN1 でキープアライブを送信します。その結果、Ethernet スイッチはアクセス ポイントに接続され、警告メッセージを生成します。アクセス ポイントおよびスイッチのどちらでも、機能が損なわれることはありません。ただし、スイッチのログに無意味なメッセージが混じり、重要なメッセージを包み込んで見えなくする可能性があります。

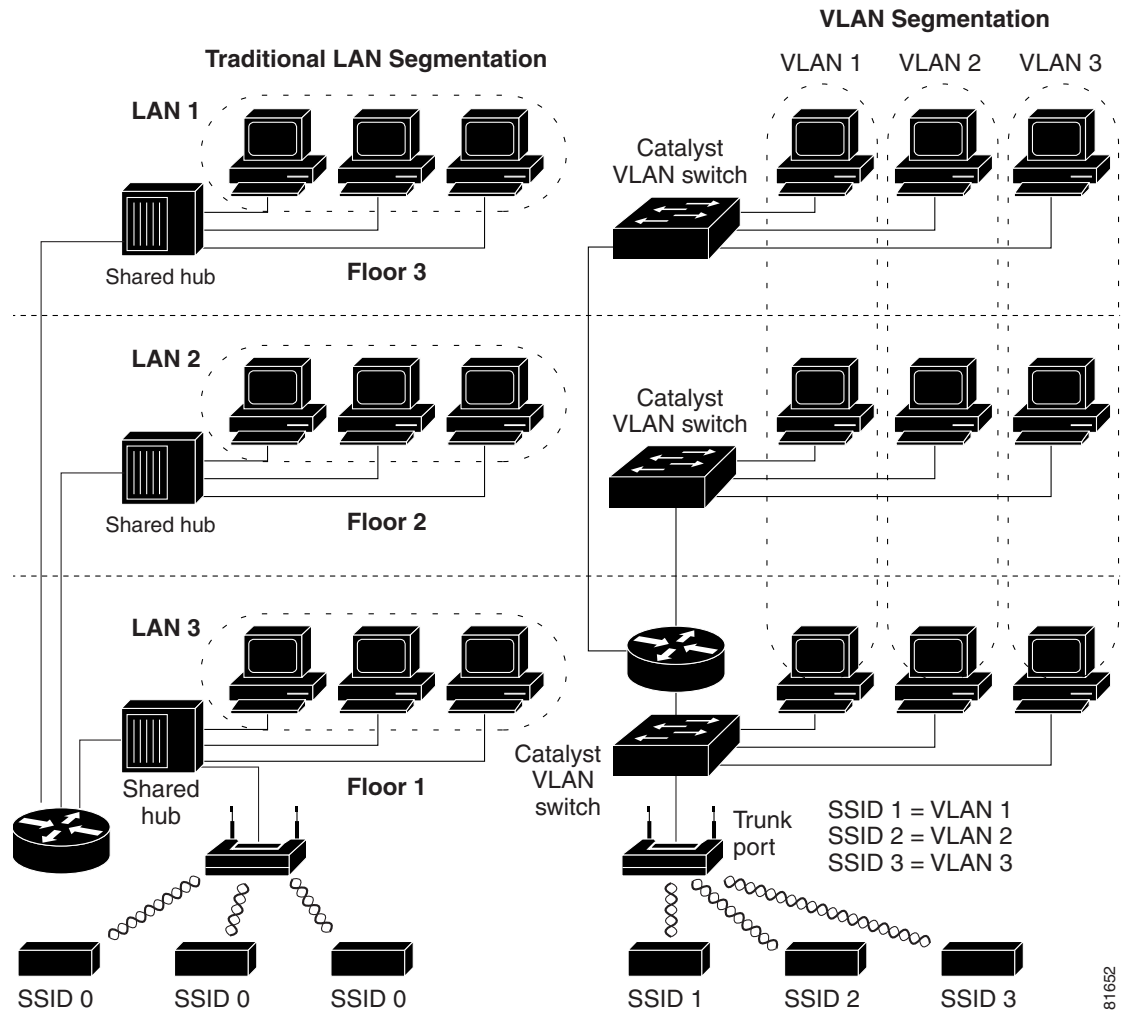
この動作は、アクセス ポイントのすべての SSID がモビリティ ネットワークに関連付けられている場合に問題となります。すべての SSID がモビリティ ネットワークに関連付けられている場合、アクセス ポイントが接続されている Ethernet スイッチ ポートをアクセス ポートとして設定することができます。アクセス ポートは通常、アクセス ポイントのネイティブ VLAN (必ずしも VLAN1 ではない) に割り当てられているため、イーサネット スイッチは 802.1q タグのトラフィックがアクセス ポイントから送信されたという警告メッセージを生成します。

キープアライブ機能を無効にすることにより、スイッチに関する過度のメッセージが生成されないようにすることができます。

図 14-1 は、無線デバイスが接続された状態での、従来の物理的な LAN セグメンテーションと論理的な VLAN セグメンテーションとの違いを示しています。



図 14-1 無線デバイスを使用する LAN セグメンテーションと VLAN セグメンテーション



81652

## 関連資料

VLAN の設計と設定に関する詳細は、次のマニュアルを参照してください。

- 『Cisco IOS Switching Services Configuration Guide』。次のリンクをクリックすると、この資料を参照できます。  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/index.htm)
- 『Cisco Internetwork Design Guide』。次のリンクをクリックすると、この資料を参照できます。  
<http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/index.htm>
- 『Cisco Internetworking Technology Handbook』。次のリンクをクリックすると、この資料を参照できます。  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/index.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm)
- 『Cisco Internetworking Troubleshooting Guide』。次のリンクをクリックすると、この資料を参照できます。  
[http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg\\_v1/index.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/index.htm)

## VLAN への無線デバイスの組み込み

VLAN の基本的な無線コンポーネントは、アクセス ポイントと、無線テクノロジーを使用してアクセス ポイントにアソシエートされるクライアントです。アクセス ポイントは、VLAN が設定されているネットワーク VLAN スイッチに、トランク ポートを介して物理的に接続されています。VLAN スイッチへの物理的な接続には、アクセス ポイントのイーサネット ポートが使用されます。

基本的に、特定の VLAN に接続するようにアクセス ポイントを設定する際に重要なのは、その VLAN を認識するように SSID を設定することです。VLAN は VLAN ID または名前によって識別されるため、アクセス ポイントの SSID が特定の VLAN ID または名前を認識するように設定された場合、VLAN との接続が確立されます。この接続が確立されると、同じ SSID を持つ、アソシエートされた無線クライアント デバイスは、このアクセス ポイントを介して VLAN にアクセスできます。VLAN は、有線ネットワークとのやり取りと同様に、クライアントとやり取りしてデータを処理します。アクセス ポイントには最大 16 の SSID を設定できるため、最大 16 の VLAN をサポートできます。1 つの VLAN には、1 つの SSID だけを割り当てることができます。

VLAN 機能を使用すると、より効率的かつ柔軟に無線デバイスを展開できます。たとえば、ネットワーク アクセスの方法や与えられている権限が多種多様にわたる複数のユーザの個別要件に、1 つのアクセス ポイントで対応できるようになります。VLAN 機能を使用しない場合は、許可されているアクセスの方法や与えられた権限に基づいて多様なユーザに対応するために、複数のアクセス ポイントを設置する必要があります。

無線 VLAN の配備には、2 つの一般的な戦略があります。

- ユーザ グループによるセグメンテーション：無線 LAN のユーザ コミュニティをセグメント化し、各ユーザグループに異なるセキュリティ ポリシーを適用できます。たとえば、企業環境で、正社員用、パートタイム従業員用、およびゲスト アクセス用の 3 つの有線および無線 VLAN を構築することが可能です。
- デバイス タイプによるセグメンテーション：無線 LAN をセグメント化して、セキュリティ機能の異なる複数のデバイスがネットワークに接続できるようにします。たとえば、無線ユーザは静的 WEP だけをサポートするハンドヘルド デバイスを使用する場合や、動的 WEP を使用する高度なデバイスを使用している場合があります。これらのデバイスをグループ化して、個別の VLAN として切り離すことができます。



(注) リピータ アクセス ポイントには複数の VLAN を設定できません。リピータ アクセス ポイントはネイティブ VLAN だけをサポートします。

## VLAN の設定

次の項では、アクセス ポイントに VLAN を設定する方法について説明します。

- 「VLAN の設定」 (P.14-5)
- 「VLAN への名前割り当て」 (P.14-7)
- 「Remote Authentication Dial-In User Service (RADIUS) サーバを使用した VLAN へのユーザの割り当て」 (P.14-8)
- 「アクセス ポイントに設定された VLAN の表示」 (P.14-9)

## VLAN の設定



(注)

アクセス ポイントに VLAN を設定するとき、ネイティブ VLAN は VLAN1 である必要があります。単一アーキテクチャでは、アクセス ポイントが受信するクライアント トラフィックは IP-GRE トンネルを通してトンネリングされます。IP-GRE トンネルは、アクセス ポイントのイーサネット インターフェイスのネイティブ VLAN で確立されます。IP-GRE トンネルのため、別のスイッチ ポートを VLAN1 として設定してしまうこともあります。この誤設定により、スイッチ ポートのエラーが発生します。

VLAN をサポートするようにアクセス ポイントを設定するプロセスは、次の 3 つの手順で行います。

1. 無線ポートとイーサネット ポートでの VLAN の有効化
2. SSID の VLAN への割り当て
3. 認証設定の SSID への割り当て

この項では、SSID を VLAN に割り当てる方法、およびアクセス ポイントの無線ポートとイーサネット ポートで VLAN を有効にする方法を説明します。SSID に認証タイプを割り当てる手順の詳細は、第 11 章「認証タイプの設定」を参照してください。その他の設定を SSID に割り当てる方法については、第 7 章「複数の SSID の設定」を参照してください。

アクセス ポイントには最大 16 の SSID を設定できるため、LAN に設定される VLAN は、最大 16 までサポートできます。

特権 EXEC モードから、次の手順に従って VLAN に SSID を割り当て、アクセス ポイントの無線ポートとイーサネット ポートで VLAN を有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio 0   1</code>	無線 インターフェイスの インターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。

	コマンド	目的
ステップ 3	<code>ssid ssid-string</code>	<p>SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。</p> <p>SSID には、最大 32 文字の英数字を使用でき、大文字と小文字が区別されます。</p> <p>最初の文字として次の文字は使用できません。</p> <ul style="list-style-type: none"> <li>感嘆符 (!)</li> <li>ポンド記号 (#)</li> <li>セミコロン (;)</li> </ul> <p>次の文字は無効とされ、SSID には使用できません。</p> <ul style="list-style-type: none"> <li>プラス記号 (+)</li> <li>閉じ大カッコ (])</li> <li>スラッシュ (/)</li> <li>引用符 (")</li> <li>タブ</li> <li>末尾のスペース</li> </ul> <p>(注) 各 SSID に認証タイプを設定する場合は、<code>ssid</code> コマンドの認証オプションを使用します。認証タイプの設定方法については、第 11 章「<a href="#">認証タイプの設定</a>」を参照してください。</p>
ステップ 4	<code>vlan vlan-id</code>	<p>(任意) ネットワーク上の VLAN に SSID を割り当てます。この SSID を使用してアソシエートするクライアントデバイスは、この VLAN にグループ化されます。VLAN ID を 1 ~ 4095 の範囲で入力します。1 つの VLAN には、1 つの SSID だけを割り当てることができます。</p> <p><b>ヒント</b> ネットワークで VLAN 名を使用している場合、アクセスポイントの VLAN にも名前を割り当てることができます。手順については、「<a href="#">VLAN への名前の割り当て</a>」(P.14-7) を参照してください。</p>
ステップ 5	<code>exit</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードに戻ります。
ステップ 6	<code>interface dot11radio 0.x   1.x</code>	無線 VLAN サブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 7	<code>encapsulation dot1q vlan-id [native]</code>	無線インターフェイスで VLAN を有効にします。 (任意) VLAN をネイティブ VLAN に指定します。多くのネットワークではネイティブ VLAN は VLAN 1 です。
ステップ 8	<code>exit</code>	グローバル コンフィギュレーション モードに戻ります。
ステップ 9	<code>interface fastEthernet0.x</code>	イーサネット VLAN サブインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 10	<code>encapsulation dot1q vlan-id</code> <code>[native]</code>	イーサネット インターフェイスで VLAN を有効にします。 (任意) VLAN をネイティブ VLAN に指定します。多くのネットワークではネイティブ VLAN は VLAN 1 です。
ステップ 11	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 12	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例は、次の方法を示します。

- SSID の名前の指定
- SSID の VLAN への割り当て
- 無線ポートとイーサネット ポートでのネイティブ VLAN として VLAN の有効化

```
ap1200# configure terminal
ap1200(config)# interface dot11radio0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# vlan 1
ap1200(config-ssid)# exit
ap1200(config)# interface dot11radio0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# interface fastEthernet0.1
ap1200(config-subif)# encapsulation dot1q 1 native
ap1200(config-subif)# exit
ap1200(config)# end
```

## VLAN への名前の割り当て

VLAN に ID 番号と名前を割り当てることができます。VLAN 名には、最大 32 文字の ASCII 文字を使用できます。アクセス ポイントでは、各 VLAN 名と ID のペアが表に格納されます。

## VLAN 名を使用する際のガイドライン

VLAN 名を使用する際は、次のガイドラインに留意してください。

- VLAN 名の VLAN ID へのマッピングは各アクセス ポイントだけで使用されるため、同じ VLAN 名をネットワーク内の別の VLAN ID に割り当てることができます。



(注) 無線 LAN のクライアントがシームレスなローミングを必要とする場合には、すべてのアクセス ポイントで同じ VLAN ID に対して同じ VLAN 名を割り当てるか、名前を使用せずに VLAN ID だけを使用することを推奨します。

- ID はアクセス ポイントに設定されているすべての VLAN に必要ですが、VLAN 名はオプションです。
- VLAN 名には、最大 32 文字の ASCII 文字を使用できます。ただし、VLAN 名を 1 ~ 4095 の数字にすることはできません。たとえば、`vlan4095` は VLAN 名として有効ですが、`4095` は無効です。アクセス ポイントでは、1 ~ 4095 の数字は VLAN ID 用に予約されています。

## VLAN 名の作成

特権 EXEC モードから、次の手順に従って VLAN に名前を割り当てます。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>dot11 vlan-name name vlan vlan-id</code>	VLAN 名を VLAN ID に割り当てます。名前には、最大 32 文字の ASCII 文字を使用できます。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

VLAN から名前を削除する場合は、コマンドの **no** 形式を使用します。アクセス ポイントに設定されている VLAN 名と ID の組み合わせをすべて表示するには、特権 EXEC コマンド `show dot11 vlan-name` を使用します。

## Remote Authentication Dial-In User Service (RADIUS) サーバを使用した VLAN へのユーザの割り当て

ユーザまたはユーザ グループがネットワークから認証を受けたときに、特定の VLAN に割り当てるように RADIUS 認証サーバを設定できます。



(注)

WPA 情報エレメントでアドバタイズされる（さらに 802.11 でのアソシエーション中に決定される）ユニキャストとマルチキャストの暗号スイートは、明示的に割り当てられた VLAN でサポートされている暗号スイートと一致しない可能性があります。RADIUS サーバにより、以前決定された暗号スイートとは別の暗号スイートを使用する、新規の VLAN ID が割り当てられた場合、アクセス ポイントとクライアントは、この新たな暗号スイートに切り替えることができなくなります。現在、WPA プロトコルと Cisco Centralized Key Management (CCKM) プロトコルでは、最初の 802.11 暗号ネゴシエーション フェーズ以降での暗号スイートの変更は認められていません。このような場合、クライアント デバイスと無線 LAN とのアソシエーションが解除されてしまいます。

VLAN マッピングのプロセスは、次の手順で行われます。

1. クライアント デバイスはアクセス ポイントに設定された任意の SSID を使用して、アクセス ポイントにアソシエートします。
2. クライアントは、RADIUS 認証を開始します。
3. クライアントの認証に成功すると、RADIUS サーバはクライアントを特定の VLAN にマッピングします。この場合、クライアントがアクセス ポイントで使用している SSID に定義された VLAN マッピングは無視されます。サーバがクライアントの VLAN 属性を返さない場合、クライアントはアクセス ポイントでローカルにマッピングされた SSID の指定する VLAN に割り当てられます。

これらは VLAN ID の割り当てに使用される RADIUS ユーザ属性です。各属性はグループ化された関係を特定するため、1 ~ 31 の範囲の共通のタグ値を保有していなければなりません。

- IETF 64 (トンネル タイプ) : 属性を **VLAN** に設定
- IETF 65 (トンネル メディア タイプ) : 属性を **802** に設定
- IETF 81 (トンネル プライベート グループ ID) : 属性を *vlan-id* に設定

## RADIUS サーバを使用した動的モビリティグループ割り当て

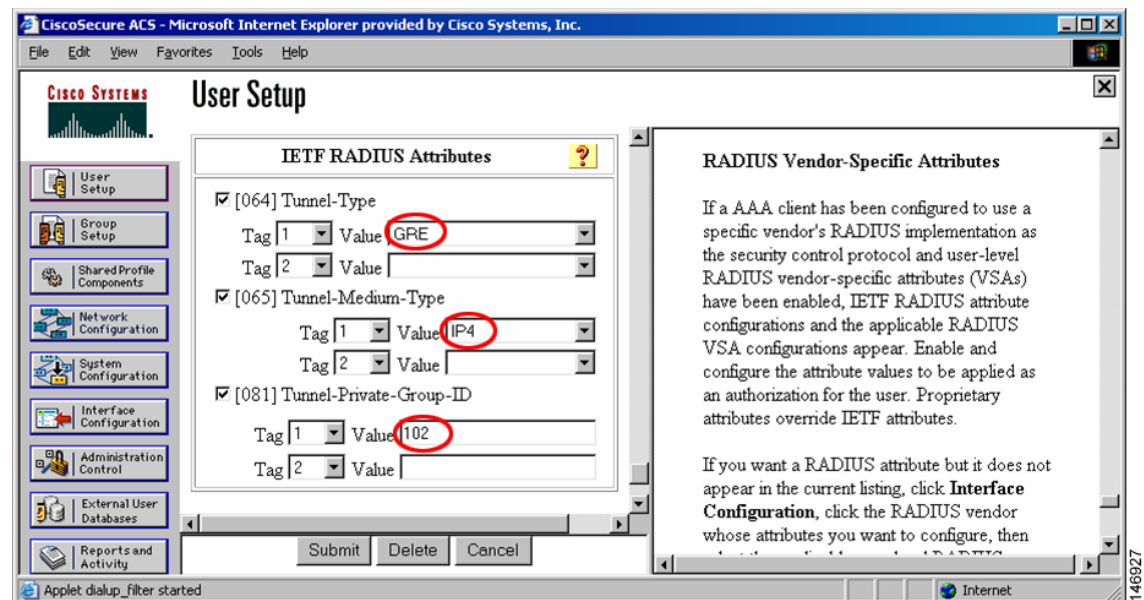
ユーザまたはユーザグループに動的にモビリティグループを割り当てるように RADIUS サーバを設定することができます。これにより、アクセスポイントに複数の SSID を設定する必要がなくなります。その代わりに、設定する SSID は、アクセスポイントあたり 1 つだけにする必要があります。

ユーザが SSID にアソシエートするとき、アクセスポイントはログイン情報を WLSM に渡し、Wireless LAN Services Module (WLSM) はその情報を RADIUS サーバに渡します。ログイン情報に基づき、RADIUS サーバは適当なモビリティグループにユーザを割り当て、認定証を返送します。

ダイナミックモビリティグループの割り当てを有効にするには、RADIUS サーバで次の属性を設定する必要があります。

- Tunnel-Type (64)
- Tunnel-Medium-Type (65)
- Tunnel-Private-Group-ID (81)

図 14-2 ダイナミックモビリティグループの割り当て



## アクセスポイントに設定された VLAN の表示

特権 EXEC モードで、**show vlan** コマンドを使用してアクセスポイントがサポートする VLAN を表示します。次に、**show vlan** コマンドの出力例を示します。

```
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)

      VLAN Trunk Interfaces: Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0
```

```

This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0
Virtual-Dot11Radio0

  Protocols Configured:  Address:          Received:      Transmitted:
    Bridging             Bridge Group 1    201688        0
    Bridging             Bridge Group 1    201688        0
    Bridging             Bridge Group 1    201688        0

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interfaces:  Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

  Protocols Configured:  Address:          Received:      Transmitted:

```

## VLAN の設定例

次の例は、VLAN を使用して、大学の構内で無線デバイスを管理する方法を示しています。この例では、有線ネットワークに設定された VLAN を介した 3 つのアクセス レベルが用意されています。

- 管理アクセス：最高のアクセス レベル。ユーザはすべての内部ドライブとファイル、学部のデータベース、トップレベルの財務情報、およびその他の機密情報にアクセスできます。管理ユーザは、Cisco LEAP を使用した認証が要求されます。
- 教職員アクセス：中級のアクセス レベル。ユーザは学内のイントラネットとインターネット、内部ファイル、および学生のデータベースにアクセスし、人事や給与、その他の教職員関連の資料といった内部情報を参照できます。教職員ユーザは、Cisco LEAP を使用した認証が要求されます。
- 学生アクセス：最も低いアクセス レベル。ユーザは学内のイントラネットおよびインターネットへのアクセス、授業日程の入手、成績の参照、面会の約束など学生に関係のある活動を実行できます。学生は静的 WEP を使用してネットワークに接続することが許可されます。

このシナリオでは、各アクセスレベルに 1 つずつ、少なくとも 3 つの VLAN 接続が必要です。アクセスポイントは最大 16 の SSID を処理できるため、表 14-1 に示す基本設計を使用できます。

表 14-1 アクセスレベルの SSID と VLAN の割り当て

アクセスレベル	SSID	VLAN ID
管理	boss	01
教職員	teach	02
学生	learn	03

マネージャは SSID boss を使用するように無線クライアントアダプタを設定し、教職員メンバーは SSID teach を使用するようにクライアントを設定し、学生は無線クライアントアダプタを SSID learn を使用するように設定します。これらのクライアントをアクセスポイントにアソシエートすると、自動的に適切な VLAN を選択します。



この例では、VLAN をサポートするために次の手順を実行します。

1. LAN スイッチのいずれかで、上記の VLAN を設定するか、VLAN 設定を確認します。
2. アクセス ポイントで、各 VLAN に SSID を割り当てます。
3. 各 SSID に認証タイプを割り当てます。
4. アクセス ポイント上のファスト イーサネットおよび dot11radio インターフェイスの両方に対し、VLAN 1 となる管理 VLAN を設定します。この VLAN は、ネイティブ VLAN にする必要があります。
5. アクセス ポイントのファスト イーサネットおよび dot11radio インターフェイスの両方に、VLAN 2 と VLAN 3 を設定します。
6. クライアント デバイスを設定します。

表 14-2 に、この例での 3 つの VLAN の設定に必要な各コマンドを示します。

表 14-2 VLAN のコンフィギュレーション コマンドの例

VLAN 1 の設定	VLAN 2 の設定	VLAN 3 の設定
<pre>ap1200# configure terminal ap1200(config)# interface dot11radio 0 ap1200(config-if)# ssid boss ap1200(config-ssid)# vlan 01 ap1200(config-ssid)# end</pre>	<pre>ap1200# configure terminal ap1200(config)# interface dot11radio 0 ap1200(config-if)# ssid teach ap1200(config-ssid)# vlan 02 ap1200(config-ssid)# end</pre>	<pre>ap1200# configure terminal ap1200(config)# interface dot11radio 0 ap1200(config-if)# ssid learn ap1200(config-ssid)# vlan 03 ap1200(config-ssid)# end</pre>
<pre>ap1200 configure terminal ap1200(config) interface FastEthernet0.1 ap1200(config-subif) encapsulation dot1q 1 native ap1200(config-subif) exit</pre>	<pre>ap1200(config) interface FastEthernet0.2 ap1200(config-subif) encapsulation dot1q 2 ap1200(config-subif) bridge-group 2 ap1200(config-subif) exit</pre>	<pre>ap1200(config) interface FastEthernet0.3 ap1200(config-subif) encapsulation dot1q 3 ap1200(config-subif) bridge-group 3 ap1200(config-subif) exit</pre>
<pre>ap1200(config)# interface Dot11Radio 0.1 ap1200(config-subif)# encapsulation dot1q 1 native ap1200(config-subif)# exit</pre> <p>(注) ネイティブ VLAN として設定したサブインターフェイスには、ブリッジグループを設定する必要はありません。このブリッジグループは、ネイティブ サブインターフェイスに自動的に移動し、無線インターフェイスとイーサネット インターフェイスの両方を表す BVI 1 とのリンクを維持します。</p>	<pre>ap1200(config) interface Dot11Radio 0.2 ap1200(config-subif) encapsulation dot1q 2 ap1200(config-subif) bridge-group 2 ap1200(config-subif) exit</pre>	<pre>ap1200(config) interface Dot11Radio 0.3 ap1200(config-subif) encapsulation dot1q 3 ap1200(config-subif) bridge-group 3 ap1200(config-subif) exit</pre>

表 14-3 は、表 14-2 のコンフィギュレーション コマンドの結果を示しています。アクセス ポイントで実行コンフィギュレーションを表示するには、**show running** コマンドを使用します。

表 14-3 コンフィギュレーション コマンド例の結果

VLAN 1 インターフェイス	VLAN 2 インターフェイス	VLAN 3 インターフェイス
<pre>interface Dot11Radio0.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled</pre>	<pre>interface Dot11Radio0.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled</pre>	<pre>interface Dot11Radio0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled</pre>
<pre>interface FastEthernet0.1 encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled</pre>	<pre>interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled</pre>	<pre>interface FastEthernet0.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled</pre>

無線インターフェイスのブリッジグループを設定する場合、次のコマンドが自動的に設定されることに注意してください。

```
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
```

ファスト イーサネット インターフェイスのブリッジグループを設定する場合、次のコマンドが自動的に設定されることに注意してください。

```
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
```



# 第 15 章

## QoS の設定

---

この章では、アクセス ポイントに Quality of Service (QoS) を設定する方法について説明します。この機能を使用すると、特定のトラフィックを優先的に処理できます。QoS を使用しない場合、パケットの内容やサイズに関係なく、アクセス ポイントは各パケットにベストエフォートでサービスを提供します。信頼性、遅延限度、またはスループットに関して保証することなく、スイッチはパケットを送信します。



(注)

---

この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

---

この章の内容は、次のとおりです。

- 「無線 LAN の QoS の概要」(P.15-2)
- 「QoS の設定」(P.15-6)
- 「QoS 設定例」(P.15-16)

## 無線 LAN の QoS の概要

ネットワークは通常、ベスト エフォート型の配信方式で動作します。したがって、すべてのトラフィックに等しいプライオリティが与えられ、適度なタイミングで配信される可能性はどのトラフィックでも同等です。輻輳が発生すると、すべてのトラフィックが等しくドロップされます。

アクセス ポイントに QoS を設定すると、特定のネットワークトラフィックを選択して優先順位を付け、輻輳管理と輻輳回避技術を使用して優先的に処理できます。無線 LAN に QoS を実装すると、ネットワークのパフォーマンスを予測可能にして、帯域幅を効果的に使用できます。

QoS を設定する場合、QoS ポリシーを作成して、アクセス ポイントに設定した VLAN に適用します。ネットワークで VLAN を使用しない場合、アクセス ポイントのイーサネットポートと無線ポートに QoS ポリシーを適用できます。



(注)

QoS を有効にすると、アクセス ポイントでは Wi-Fi Multimedia (WMM) モードがデフォルトで使用されます。WMM については、「[Wi-Fi Multimedia モードの使用方法](#)」(P.15-4) を参照してください。

## 無線 LAN の QoS と有線 LAN の QoS

無線 LAN の QoS 実装は、シスコの他のデバイスに対する QoS 実装とは異なります。アクセス ポイントで QoS を有効にすると、次の処理が実行されます。

- アクセス ポイントはパケットを分類しません。DSCP 値、クライアント タイプ (セルラー無線など)、または 802.1q か 802.1p タグの優先順位の値に基づいてパケットに優先順位を設定します。
- 内部 DSCP 値を構成しません。IP DSCP、優先順位、プロトコル値をレイヤ 2 Class of Service (COS; サービス クラス) 値に割り当てるマッピングだけをサポートします。
- 無線出力ポートに限り EDCF に類似したキューイングを実行します。
- イーサネット出力ポートで FIFO キューイングだけを実行します。
- 802.1Q/P タグ付きパケットだけをサポートします。アクセス ポイントは ISL をサポートしません。
- MQC ポリシーマップの **set cos** アクションだけをサポートします。
- QoS Elements for Wireless Phones 機能が有効な場合、他のクライアントのトラフィックよりも音声クライアントのトラフィック (Symbol フォンなど) を優先します。
- プロトコル値を 119 に設定したクラスマップ IP プロトコル節を使用して、Spectralink フォンをサポートします。

無線 LAN QoS 実装とシスコの他のネットワーク デバイスの QoS 実装を対比するには、次の URL の『*Cisco IOS Quality of Service Solutions Configuration Guide*』を参照してください。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm)

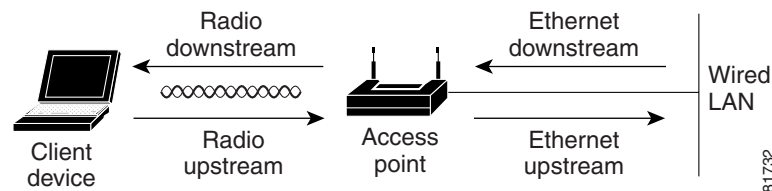
## 無線 LAN への QoS の影響

無線 LAN QoS 機能は、802.11e ドラフトのサブセットです。無線 LAN の QoS は、トラフィック分類に基づく WLAN より、アクセス ポイントのトラフィックを優先します。

他のメディアと同様、負荷の少ない無線 LAN では、QoS の影響に気付かない場合があります。QoS のメリットは無線 LAN の負荷が増加するにしたがって顕著になり、選択されたトラフィック タイプの待ち時間、ジッタ、損失は許容範囲内に維持されます。

無線 LAN の QoS は、アクセス ポイントのダウンストリームを優先します。図 15-1 は、アップストリームとダウンストリームのトラフィック フローを示しています。

図 15-1 アップストリームとダウンストリームのトラフィック フロー



- 無線ダウンストリームフローは、アクセス ポイントの無線から無線クライアント デバイスに送信されるトラフィックです。このトラフィックは、無線 LAN の QoS の主要な対象です。
- 無線アップストリームフローは、無線クライアント デバイスからアクセス ポイントに送信されるトラフィックです。無線 LAN の QoS は、このトラフィックには影響を及ぼしません。
- イーサネットのダウンストリームフローは、スイッチまたはルータからアクセス ポイント上のイーサネット ポートに送信されるトラフィックです。スイッチまたはルータで QoS が有効の場合、スイッチまたはルータはアクセス ポイントへのトラフィックを優先し、レートを制限する場合があります。
- イーサネットのアップストリームフローは、アクセス ポイントのイーサネット ポートから有線 LAN 上のスイッチまたはルータに送信されるトラフィックです。アクセス ポイントは、有線 LAN に送信するトラフィックの、トラフィック分類に基づく優先付けは行いません。

## QoS 設定の優先順位

QoS を有効にすると、アクセス ポイントは各パケットのレイヤ 2 サービス クラス値に基づいて、パケットをキューに置きます。アクセス ポイントは、次の順序で QoS ポリシーを適用します。

1. 分類済みのパケット : アクセス ポイントが QoS 対応スイッチまたはルータからゼロ以外の 802.1 Q/P user\_priority 値で分類されたパケットを受信する場合、アクセス ポイントはその分類を使用し、別の QoS ポリシー規則をパケットに適用しません。既存の分類がアクセス ポイントの他のどのポリシーよりも優先されます。



(注) QoS ポリシーを設定していなくても、アクセス ポイントは常に受信したタグ付き 802.1P パケットを無線インターフェイスより優先します。

2. *QoS Element for Wireless Phones* の設定 : *QoS Element for Wireless Phones* 設定を有効にすると、セルラー無線ベンダーのクライアントによってはダイナミック音声分類子が作成されるクライアントもあり、これによりセルラー無線のトラフィックが他のクライアントよりも優先されます。さらに、QoS Basic Service Set (QBSS; QoS 基本サービスセット) が、ビーコンとプローブ応答でチャネルロード情報をアダプタイズするために有効になります。トラフィック負荷に基づき、QBSS 要素を使用してアソシエートするアクセスポイントを決する IP フォンもあります。

Cisco IOS の `dot11 phone dot11e` コマンドを使用して 7920 セルラー無線のファームウェアを将来アップグレードし、標準の QBSS Load IE をサポートすることができます。7920 セルラー無線の新しいファームウェアは、後日発表されます。



(注)

このリリースでは、既存の 7920 セルラー無線ファームウェアを引き続きサポートします。セルラー無線の新ファームウェアが利用可能になり、セルラー無線をアップグレードできるようになるまで、7920 セルラー無線で新標準の (IEEE 802.11e draft 13) QBSS Load IE を使用しないようにしてください。

次の例は、従来の QBSS Load 要素で IEEE 802.11 セルラー無線のサポートを有効にする方法を示します。

```
AP(config)# dot11 phone
```

次の例は、標準 (IEEE 802.11e draft 13) の QBSS Load 要素で IEEE 802.11 セルラー無線のサポートを有効にする方法を示します。

```
AP(config)# dot11 phone dot11e
```

次の例は、IEEE 802.11 電話機のサポートを停止、無効にする方法を示します。

```
AP(config)# no dot11 phone
```

3. アクセスポイントで作成したポリシー : QoS のポリシーを作成して VLAN またはアクセスポイント インターフェイスに適用すると、この QoS ポリシーはすでに分類済みのパケットと *QoS Element for Wireless Phones* 設定に次いで 3 番目の優先順位になります。
4. VLAN の全パケットに適用されるデフォルト分類 : VLAN の全パケットにデフォルトの分類を設定すると、そのポリシーは優先順位リストで 4 番目になります。

## Wi-Fi Multimedia モードの使用方法

QoS を有効にすると、アクセスポイントでは Wi-Fi Multimedia (WMM) モードがデフォルトで使用されます。WMM では、基本的な QoS モードに対して、次のような拡張機能が用意されています。

- アクセスポイントは、各パケットのサービスクラスをパケットの 802.11 ヘッダーに追加し、このヘッダーを受信ステーションに渡します。
- 各アクセスクラスに 802.11 シーケンス番号が設定されます。このシーケンス番号により、受信側の重複チェック用バッファをオーバーフローさせずに、優先順位の高いパケットが優先順位の低いパケットの再試行を中断できます。
- WPA のリプレイ検出は、アクセスクラスごとに受信側で実行されます。802.11 のシーケンス番号設定と同じく、WPA のリプレイ検出でも、受信ステーションでリプレイをシグナリングせずに、優先順位の高いパケットが優先順位の低いパケットの再試行を中断できます。

- 通常のバックオフ手順で送信するように設定されたトランスミッタは、設定された送信のタイミング（所定のマイクロ秒数）の際に、送信を許可するアクセス クラスに対して保留中のパケットをセットで送信できます。保留中のパケットをセットで送信すると、各パケットがアクセスのためにバックオフを待機する必要がなく、即座にパケットを連続して送信できるため、スループットが向上します。
- U-APSD Power Save が有効になります。

WMM をサポートするクライアント デバイスに送信されたパケットに対して、アクセス ポイントは WMM 拡張機能を適用します。WMM をサポートしないクライアント デバイスに送信されたパケットに対して、アクセス ポイントは基本的な QoS ポリシーを適用します。

CLI を使用して WMM を無効にするには、設定インターフェイス コマンド `no dot11 qos mode wmm` を使用します。Web ブラウザ インターフェイスを使用して WMM を無効にするには、[QoS Advanced] ページで無線インターフェイスのチェックボックスをオフにします。図 15-3 は、[QoS Advanced] ページを示しています。

## バンド選択の使用

Wi-Fi 無線がデュアルバンド動作に対応していれば、バンド選択を利用してより混雑の少ない無線に移動できます。この機能は、ネットワークの全体的なパフォーマンスを向上させます。

この機能が有効な場合、アクセス ポイントは、バンド選択が有効にされているすべての SSID のすべての新規クライアントへのプローブ応答を抑制します。

バンド選択を有効にするには、次の手順に従ってください。

- 
- ステップ 1** [Security] > [SSID Manager] の順で選択します。
  - ステップ 2** [NEW] をクリックして、新しい SSID を作成します。  
または  
[Current SSID] から必要な SSID を選択します。
  - ステップ 3** [Band Select] オプション ボタンをクリックします。
  - ステップ 4** [Apply] をクリックします。
- 

バンド選択のパラメータの指定では、次の手順に従ってください。

- 
- ステップ 1** [Services] > [Band Select] の順で選択します。
  - ステップ 2** [Band Select] チェックボックスをオンにします。
  - ステップ 3** 次のフィールドに値を入力します。
    - [Client-Rssi] : クライアントがバンド選択可能となるための受信信号強度表示 (RSSI) の最小値 範囲は 20 ~ 90 です。
    - [Cycle-Count] : アクセス ポイントが無視するまたは遅延させるフレームまたはプローブ ビーコンの数。指定できる範囲は 1 ~ 10 です。
    - [Cycle-Threshold (ms)] : アクセス ポイントがクライアントからの各プローブを受け付けられる時間 (ミリ秒)。指定できる範囲は 1 ~ 1000 です。
    - [Expire-Suppression (secs)] : この時間経過後にクライアントは新しいクライアントとして宣言され、そのプローブ フレームが再度遅延されたり、無視される場合があります。範囲は 10 ~ 200 です。



- [Expire-Dual-Band (secs)] : [Expire-Suppression] と似ていますが、[Expire-Dual-Band] はデュアルバンド クライアントにのみ適用されます。範囲は 10 ~ 300 です。

ステップ 4 [Apply] をクリックします。

特権 EXEC モードから、次のコマンドを使用して、アクセス ポイント CLI を利用した SSH を設定します。

```
- ap(config)# dot11 band-select parameters
- ap(config-bs-profile)# cycle-count?
- ap(config-bs-profile)# cycle-threshold?
- ap(config-bs-profile)# expire-suppression?
- ap(config-bs-profile)# expire-dual-band?
- ap(config-bs-profile)# client-rssi?
- ap (config)# dot11 ssid abcd
- ap(config-ssid)# band-select
```

## QoS の設定

QoS はデフォルトでは無効に設定されています。ただし、無線インターフェイスは、QoS ポリシーを設定していなくても、常にタグ付き 802.1P パケットを優先します。この項では、アクセス ポイントで QoS を設定する方法について説明します。内容は次のとおりです。

- 「設定時の注意事項」 (P.15-6)
- 「Web ブラウザ インターフェイスを使用した QoS の設定」 (P.15-7)
- 「無線アクセス カテゴリの調整」 (P.15-13)
- 「AVVID 優先順位マッピング」 (P.15-12)

## 設定時の注意事項

アクセス ポイントに QoS を設定する前に、次の情報に注意する必要があります。

- QoS の導入で最も重要なのは、無線 LAN のトラフィックについて十分に把握することです。無線クライアント デバイスで使用するアプリケーション、アプリケーションが遅延の影響を受ける程度、およびアプリケーションに関連するトラフィック量が分かれば、パフォーマンスを向上させるように QoS を設定できます。
- QoS によって無線 LAN の帯域幅が増加することはありません。QoS は、帯域幅の割り当て制御を効率化します。無線 LAN に十分な帯域幅があれば、QoS を設定する必要がない可能性があります。
- **ampdu** コマンドは、802.11n 無線インターフェイスに使用できます。Aggregate MAC protocol data unit (AMPDU; 集成的 MAC プロトコル データ ユニット) は、物理層により単一の PSDU として転送された複数の MPDU を含む構造です。このコマンドの詳細については、『Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges』を参照してください。



## Web ブラウザ インターフェイスを使用した QoS の設定

この項では、Web ブラウザ インターフェイスを使用する QoS の設定について説明します。

CLI を使用して QoS を設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

QoS を設定する手順は、次のとおりです。

- 
- ステップ 1** 無線 LAN で VLAN を使用する場合、QoS を設定する前に必要な VLAN がアクセス ポイントに設定されていることを確認します。
  - ステップ 2** Web ブラウザ インターフェイスのページの左側にあるタスク メニューで [Services] をクリックします。Services のリストが展開されたら、[QoS] をクリックします。[QoS Policies] ページが表示されます。図 15-2 は、[QoS Policies] ページを示しています。

図 15-2 [QoS Policies] ページ

HOME

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP +

ASSOCIATION +

NETWORK INTERFACES +

SECURITY +

SERVICES

Telnet/SSH

Hot Standby

CDP

DNS

Filters

HTTP

QoS

STREAM

SNMP

SNTP

VLAN

ARP Caching

WIRELESS SERVICES +

SYSTEM SOFTWARE +

EVENT LOG +

QoS POLICIES

RADIO0-802.11G ACCESS CATEGORIES

RADIO1-802.11A ACCESS CATEGORIES

ADVANCED

Hostname ap

ap uptime is 1 week, 5 days, 3 hours, 49 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: <NEW>

Policy Name:

Classifications:

Delete Classification

Match Classifications:

IP Precedence: Routine (0)

IP DSCP: Best Effort (0-63)

IP Protocol 119

Filter: No Filters defined. [Define Filters.](#)

Rate Limiting:

Bits per Sec.: (8000-2000000000)

Burst Rate (Bytes): (1000-512000000)

Conform Action: Transmit

Exceed Action: Drop

Apply Class of Service:

Best Effort (0)

Best Effort (0)

Best Effort (0)

Apply Delete Cancel

Apply Policies to Interface/ VLANs

	FastEthernet	Radio0-802.11G	Radio1-802.11A
Incoming	<NONE>	<NONE>	<NONE>
Outgoing	<NONE>	<NONE>	<NONE>

Apply Cancel

**ステップ 3** [Create/Edit Policy] フィールドで [<NEW>] を選択して、[Policy Name] 入力フィールドに QoS ポリシーの名前を入力します。名前には、最大 25 文字の英数字を使用できます。ポリシー名には空白を入れないでください。



**(注)** 設定済みの 2 つの QoS ポリシーである WMM と Spectralink を選択することもできます。この 2 つのいずれかを選択すると、デフォルトの分類が自動的に [Classifications] フィールドに入力されます。

- ステップ 4** 優先順位を設定する必要があるパケットの [IP header TOS] フィールドに IP 優先情報が含まれている場合には、[IP Precedence] ドロップダウン リストから IP 優先順位の分類を選択します。メニューの選択項目は次のとおりです。
- Routine (0)
  - Priority (1)
  - Immediate (2)
  - Flash (3)
  - Flash Override (4)
  - Critic/CCP (5)
  - Internet Control (6)
  - Network Control (7)
- ステップ 5** [Apply Class of Service] ドロップダウン リストを使用して、[IP Precedence] メニューから選択したタイプのパケットにアクセス ポイントが適用するサービス クラスを選択します。アクセス ポイントは、[IP Precedence] の選択内容を選択したサービス クラスに一致させます。[Apply Class of Service] メニューの設定内容は次のとおりです。
- Best Effort (0)
  - Background (1)
  - Spare (2)
  - Excellent (3)
  - Control Lead (4)
  - Video <100ms Latency (5)
  - Voice <100ms Latency (6)
  - Network Control (7)
- ステップ 6** [IP Precedence] の [Class of Services] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。分類を削除するには、削除する分類を選択して、[Classifications] フィールドの横の [Delete] ボタンをクリックします。
- ステップ 7** 優先設定する必要があるパケットの [IP header TOS] フィールドに IP DSCP 優先情報が含まれている場合には、[IP DSCP] ドロップダウン リストから [IP DSCP] 分類を選択します。メニューの選択項目は次のとおりです。
- Best Effort
  - Assured Forwarding — Class 1 Low
  - Assured Forwarding — Class 1 Medium
  - Assured Forwarding — Class 1 High
  - Assured Forwarding — Class 2 Low
  - Assured Forwarding — Class 2 Medium
  - Assured Forwarding — Class 2 High
  - Assured Forwarding — Class 3 Low
  - Assured Forwarding — Class 3 Medium
  - Assured Forwarding — Class 3 High
  - Assured Forwarding — Class 4 Low

- Assured Forwarding — Class 4 Medium
- Assured Forwarding — Class 4 High
- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding (緊急転送)

- ステップ 8** [Apply Class of Service] ドロップダウン リストを使用して、[IP DSCP] メニューから選択したタイプのパケットにアクセス ポイントが適用するサービス クラスを選択します。アクセス ポイントは、IP DSCP の選択内容を選択したサービス クラスに一致させます。
- ステップ 9** [IP DSCP] の [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。
- ステップ 10** 無線 LAN で Spectralink フォン (IP Protocol 119) のパケットを優先設定する必要がある場合、[Apply Class of Service] ドロップダウン リストを使用して、アクセス ポイントが Spectralink フォン パケットに適用するサービス クラスを選択します。アクセス ポイントは、Spectralink フォン パケットを選択したサービス クラスに一致させます。
- ステップ 11** IP Protocol 119 の [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。
- ステップ 12** フィルタ処理されたパケットに優先順位を割り当てるには、[Filter] ドロップダウン リストを使用してポリシーに追加するフィルタを選択します (アクセス ポイントでフィルタが定義されていない場合、[Filter] ドロップダウン リストの代わりに [Apply Filters] ページへのリンクが表示されます)。たとえば、IP フォンの MAC アドレスを持つ MAC アドレス フィルタの優先順位を高くすることができます。



**(注)** QoS で使用するアクセス リストは、アクセス ポイントのパケット転送の決定に影響しません。

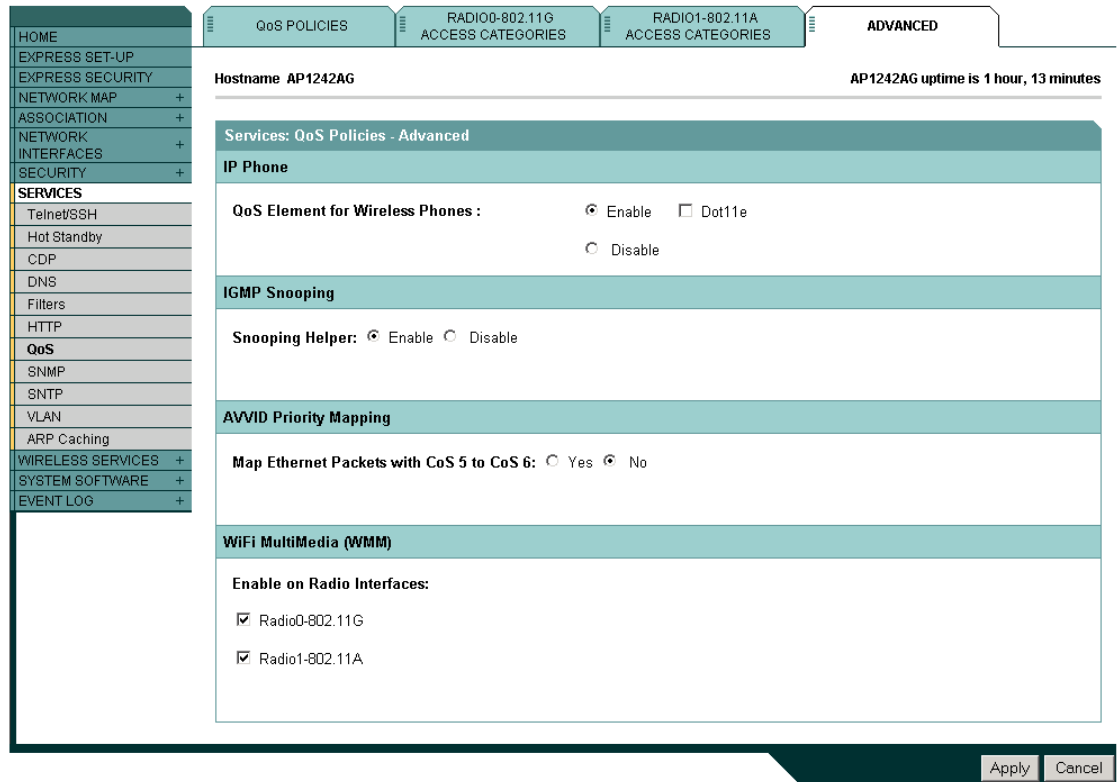
- ステップ 13** [Apply Class of Service] ドロップダウン リストを使用して、[Filter] メニューから選択したフィルタに一致するパケットに、アクセス ポイントが適用するサービス クラスを選択します。アクセス ポイントは、フィルタの選択内容を選択したサービス クラスに一致させます。
- ステップ 14** フィルタの [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。
- ステップ 15** VLAN 上の全パケットにデフォルトの分類を設定する場合、[Apply Class of Service] ドロップダウン リストを使用して、アクセス ポイントが VLAN 上の全パケットに適用するサービス クラスを選択します。アクセス ポイントは、全パケットを選択したサービス クラスに一致させます。
- ステップ 16** [Default classification for packets on the VLAN] の [Class of Service] メニューの横にある [Add] ボタンをクリックします。[Classifications] フィールドに分類項目が表示されます。
- ステップ 17** 分類をポリシーへ追加したら、[Apply Class of Service] ドロップダウン リストの [Apply] ボタンをクリックします。ポリシーをキャンセルして全フィールドをデフォルトにリセットするには、[Apply Class of Service] ドロップダウン リストの [Cancel] ボタンをクリックします。ポリシー全体を削除するには、[Apply Class of Service] ドロップダウン リストの [Delete] ボタンをクリックします。

- ステップ 18** [Apply Policies to Interface/VLAN] ドロップダウン リストを使用して、アクセス ポイントのイーサネット ポートと無線ポートにポリシーを適用します。アクセス ポイントに VLAN が設定されている場合、各 VLAN の仮想ポートのドロップダウン リストがこのセクションに表示されます。アクセス ポイントに VLAN が設定されていない場合、各インターフェイスのドロップダウン リストが表示されます。
- ステップ 19** ページの下にある [Apply] ボタンをクリックして、アクセス ポイントのポートにポリシーを適用します。

## [QoS Policies Advanced] ページ

[QoS Policies Advanced] ページ (図 15-3)

図 15-3 [QoS Policies - Advanced] ページ



[Enable] を選択するか [Apply] をクリックして、すべての音声パケットの優先順位が最も高くなるように定めます。

### QoS Element for Wireless Phones

QoS Element for Wireless Phones を有効にすると、QoS を有効にしていなくてもアクセス ポイントは音声パケットに最高の優先順位を指定します。この設定は、QoS ポリシーの設定とは無関係に機能します。

最新バージョンの QBSS Load IE を使用するには、**dot11e** を選択します。この設定をブランクのままにした場合、古いバージョンの QBSS Load IE が使用されます。

## IGMP スヌーピング

インターネット グループ管理プロトコル (IGMP) スヌーピングがスイッチで有効に設定されているときに、クライアントがアクセス ポイント間をローミングする場合、クライアントのマルチキャスト セッションはドロップされます。アクセス ポイントの IGMP スヌーピング ヘルパーが有効な場合、アクセス ポイントは汎用クエリを無線 LAN に送信して、クライアントに IGMP メンバーシップ レポートを送信するように求めます。ネットワーク インフラストラクチャがホストの IGMP メンバーシップ レポートを受け取ると、そのホストのマルチキャスト データ ストリームの配信が保証されます。

IGMP スヌーピング ヘルパーは、デフォルトで有効に設定されています。無効にするには、[QoS Policies - Advanced] ページを表示して [Disable] を選択し、[Apply] をクリックします。



(注)

ホストからの IGMP クエリと応答を処理するマルチキャスト ルータがない場合、アクセス ポイントに **no igmp snooping** が設定されていることが必須となります。IGMP スヌーピングが有効な場合、すべてのマルチキャスト グループトラフィックが IGMP クエリと応答パケットを送信する必要があります。IGMP クエリまたは応答パケットが検出されない場合、グループのすべてのマルチキャストトラフィックはドロップされます。

## AVVID 優先順位マッピング

AVVID 優先順位マッピングは、サービス クラス 5 のタグの付いたイーサネット パケットをサービス クラス 6 にマッピングします。この機能を使用すると、アクセス ポイントは、正しい優先順位を音声パケットに適用して Cisco AVVID ネットワークとの互換性を確保します。

AVVID 優先順位マッピングはデフォルトで有効に設定されています。マッピングを無効にするには、[QoS Policies - Advanced] ページを表示して [Map Ethernet Packets with CoS 5 to CoS 6] で [No] を選択し、[Apply] をクリックします。

## WiFi Multimedia (WMM)

[Admission Control] チェックボックスを使用して、アクセス ポイントの無線インターフェイスの WMM を有効にできます。アドミッション コントロールを有効にすると、アクセス ポイントにアソシエートされたクライアントは、WMM のアドミッション コントロール プロシージャを完了するまでそのアクセス カテゴリを使用できません。

## Rate Limiting

レート制限は、インターフェイスで送受信されるデータのトラフィックを制御します。クラスベースのポリシング機能により、次の動作が実行されます。

- ユーザ定義の基準に基づいて、トラフィックのクラスの入力または出力送信レートを制限します。
- IP precedence 値、IP DiffServ コード ポイント (DSCP) 値、および Quality of Service (QoS) グループを設定してパケットにマーク付けをします。

これは、P2MP 設定の場合に、各非ルート ブリッジからルート ブリッジへのアップストリームトラフィックをレート制限するために使用されます。ダウンストリームトラフィックのレート制限を行うためには、クラス マップがルート側のルータ/スイッチに適用されます。



(注) レート制限はイーサネット入力だけに適用できます。

## 無線アクセス カテゴリの調整

アクセス ポイントは、無線アクセス カテゴリを使用して各パケットのバックオフ時間を計算します。通常、優先順位の高いパケットは、バックオフ時間が短くなります。

[Min and Max Contention Window] フィールドと [Slot Time] フィールドのデフォルト値は、IEEE ドラフト規格 802.11e で推奨される設定に基づいています。これらの値の詳細は、同規格を参照してください。

[Radio Access Categories] ページではデフォルト設定を使用することを強く推奨します。これらの値を変更すると、無線 LAN に予期しないトラフィックのブロックが発生しやすくなり、発生したブロックの診断が容易ではない場合もあります。これらの値を変更後にデフォルトにリセットする必要がある場合は、表 15-1 のデフォルト設定を使用します。

表 15-1 に示された値は 2 の累乗係数です。アクセス ポイントは、次の式を使用して Contention Window の値を計算します。

$$CW = 2 ** X - 1$$

X は表 15-1 の値です。

表 15-1 QoS 無線アクセス カテゴリのデフォルト

Class of Service	Min Contention Window		Max Contention Window		Fixed Fixed Slot Time		Transmit Opportunity		Admission Control	
	Local	Cell	Local	Cell	Local	Cell	Local	Cell	Local	Cell
Background	4		10		6		0			
Best Effort	4		10		2		0			
Video <100ms Latency	3		2		1		3008			
Voice <100ms Latency	2		3		1		1504			

図 15-4 は [Radio Access Categories] ページを示しています。デュアル無線アクセス ポイントには、各無線に対して [Radio Access Categories] ページがあります。

図 15-4 [Radio Access Categories] ページ

Cisco Aironet 1240AG Series Access Point

Hostname AP1242AG AP1242AG uptime is 1 hour, 55 minutes

Services: QoS Policies - Access Category

Access Category Definition

Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2^x-1; x can be 0-10)	AP	5	5	4	3
	Client	5	5	4	3
Max Contention Window (2^x-1; x can be 0-10)	AP	10	6	5	4
	Client	10	10	5	4
Fixed Slot Time (0-20)	AP	7	3	1	1
	Client	7	3	2	2
Transmit Opportunity (0-65535 μS)	AP	0	0	3008	1504
	Client	0	0	3008	1504

Optimized Voice WFA Default Apply Cancel

Admission Control for Video and Voice

Video(CoS 4-5)  
 Admission Control

Voice(CoS 6-7)  
 Admission Control  
Max Channel Capacity (%): DISABLED  
Roam Channel Capacity (%): DISABLED

Apply Cancel



(注) このリリースでは、[Admission Control] を [Enable] にした場合、クライアントはアクセスカテゴリを使用できません。

## 公称レートの設定

アクセスポイントが WMM クライアントから add traffic stream (ADDTS; トラフィックストリーム) の追加要求を受け取ると、CLI コマンドの **traffic-stream** で定義された公称レートに対する、ADDTS 要求の公称レートまたは最小 PHY レートをチェックします。両者が一致しない場合、アクセスポイントは ADDTS 要求を拒否します。

[Optimized Voice] 設定 (図 15-4 を参照) を選択する場合、次の公称レートが設定されます。

- 5.5Mbps、6.0Mbps、11.0Mbps、12.0Mbps、および 24.0Mbps



**traffic-stream** コマンドの詳細については、『*Command Reference for Cisco Aironet Access Points and Bridges*』で参照できます。この資料は [cisco.com](http://cisco.com) の次の URL から入手できます。

[http://cisco.com/en/US/docs/wireless/access\\_point/12.4\\_10b\\_JA/command/reference/cr12410b-chap2.html#wp3257080](http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b-chap2.html#wp3257080)



(注) シスコの電話機は上記のレートで正しく動作します。サードパーティのセルラー無線では、公称レートまたは最小 PHY レートが異なっている場合があります。サードパーティのセルラー無線用に追加の公称レートを有効にする必要がある場合があります。

## 最適化された音声設定

[Admission Control] チェックボックスを使用して、クライアントによるアクセス カテゴリの使用を制御できます。アクセス カテゴリに対するアドミッション コントロールを有効にすると、アクセス ポイントにアソシエートされたクライアントは、WMM のアドミッション コントロール プロシージャを完了するまでそのアクセス カテゴリを使用できません。ただし、このリリースのアクセス ポイントではアドミッション コントロール プロシージャはサポートされないため、[Admission Control] を有効にした場合、クライアントはアクセス カテゴリを使用できません。

## コールアドミッション制御の設定

アクセス ポイントの Call Admission Control (CAC; コールアドミッション制御) の設定は次の手順で行います。

1. 無線の設定
2. SSID のアドミッション コントロールの有効化

### 無線の設定

この項では、アクセス ポイントの無線のアドミッション コントロール設定法について説明します。

コマンドライン インターフェイス (CLI) を使用してアドミッション コントロールを設定するための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

無線のアドミッション コントロールを設定する手順は、次のとおりです。

- ステップ 1** 設定する無線の [Access Categories] ページをクリックします。  
図 15-4 に、[Access Categories] ページの例を示します。
- ステップ 2** [Voice(CoS 6-7)] 下の [Admission Control] チェックボックスを選択します。
- ステップ 3** 音声で使用されるチャネルの最大利用率を [Max Channel Capacity (%)] フィールドに入力します。
- ステップ 4** ローミング コールで使用されるチャネルの最大利用率を [Roam Channel Capacity (%)] フィールドに入力します。

このフィールドで指定した値を最大とする、ローミング コールで使用されるチャネルの利用率は、[Max Channel Capacity (%)] フィールドで指定した値から差し引かれます。

たとえば、[Max Channel Capacity (%)] フィールドに 75% と入力し、[Roam Channel Capacity (%)] に 6% と入力したとします。ローミング コールがチャネルの 5% を使用している場合、同じチャネルの最大 70% を音声に使用できます。

- ステップ 5** シグナリングにビデオ アクセス カテゴリ (AC=2) を使用するには、[Video(CoS 4-5)] 下の [Admission Control] チェックボックスを選択します。



**(注)** この項で設定したアドミッション コントロール設定は、SSID のアドミッション コントロールを有効にするまでは無効です。

### アドミッション コントロールの有効化

この項では、SSID のアドミッション コントロールを有効にする方法について説明します。コマンドライン インターフェイス (CLI) を使用してアドミッション コントロールを有効にするための Cisco IOS コマンドのリストについては、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

次の手順に従って SSID のアドミッション コントロールを有効にします。

- ステップ 1** [SSID Manager] ページを開きます。
- ステップ 2** [SSID] を選択します。
- ステップ 3** [General Settings] の下、[Call Admission Control] フィールドの [Enable] を選択します。

### アドミッション コントロールのトラブルシューティング

2つの CLI コマンドを使用して、アドミッション コントロールの問題のトラブルシューティングに役立つ情報を表示できます。

- 無線 0 の現在のアドミッション コントロール設定を表示するには、次のコマンドを入力します。  
# `show dot11 cac int dot11Radio 0`
- 無線 1 の現在のアドミッション コントロール設定を表示するには、次のコマンドを入力します。  
# `show dot11 cac int dot11Radio 1`
- アドミッション コントロールおよび MT の admitted streams についての情報を表示するには、次のコマンドを入力します。  
# `show dot11 traffic-streams`

## QoS 設定例

次の項では、QoS の一般的な使用方法を 2つ説明します。

- 「音声トラフィックの優先指定」(P.15-17)
- 「ビデオトラフィックの優先指定」(P.15-18)

## 音声トラフィックの優先指定

この項では、無線ネットワークの音声 VLAN に QoS ポリシーを適用して、セルラー無線のトラフィックを優先する方法を示します。

この例では、ネットワーク管理者は `voice_policy` という名前のポリシーを作成して、Spectralink フォンのトラフィックに音声サービス クラスを適用します (プロトコル 119 パケット)。ユーザは入出力無線ポートと出力側のイーサネット ポートに `voice_policy` を適用します。図 15-5 は、管理者の QoS ポリシー ページを示しています。

図 15-5 音声の [QoS Policies] ページの例

Hostname ap1240 ap1240 uptime is 9 hours, 22 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: voice\_policy

Policy Name: voice\_policy

Classifications: IP Protocol 119 - COS Voice < 10ms Latency (6)

Delete Classification

Match Classifications:

IP Precedence: Routine (0) Best Effort (0) Add

IP DSCP: Best Effort (0-63) Best Effort (0) Add

IP Protocol 119: Best Effort (0) Add

Filter: No Filters defined. [Define Filters.](#)

Rate Limiting:

Bits per Sec.: (8000-2000000000) Burst Rate (Bytes): (1000-512000000) Add

Conform Action: Transmit Exceed Action: Drop Add

Apply Delete Cancel

Apply Policies to Interface/ VLANs

	FastEthernet	Radio0-802.11G	Radio1-802.11A
Incoming	< NONE >	voice_policy	< NONE >
Outgoing	voice_policy	voice_policy	< NONE >

Apply Cancel

また、ネットワーク管理者は [QoS Policies - Advanced] ページで、[QoS element for wireless phones] の設定を有効にします。この設定により、VLAN の設定とは関係なくすべての音声トラフィックが優先されます。

230773

## ビデオトラフィックの優先指定

この項では、ビデオトラフィック専用ネットワークの VLAN に QoS ポリシーを適用する方法を示します。

この例では、ネットワーク管理者は `video_policy` という名前のポリシーを作成して、ビデオトラフィックにビデオ サービス クラスを適用します。ユーザは入出力無線ポートと出力側のイーサネット ポートに `video_policy` を適用します。図 15-6 は、管理者の QoS ポリシー ページを示しています。

図 15-6 ビデオの [QoS Policies] ページの例

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
SECURITY +  
SERVICES  
Telnet/SSH  
Hot Standby  
CDP  
DNS  
Filters  
HTTP  
QoS  
STREAM  
SNMP  
SNTP  
VLAN  
ARP Caching  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

QoS POLICIES    RADIO0-802.11G ACCESS CATEGORIES    RADIO1-802.11A ACCESS CATEGORIES    ADVANCED

Hostname ap1240    ap1240 uptime is 10 hours, 16 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: video\_policy

Policy Name: video\_policy

Classifications:

Precedence Priority - COS Video < 100ms Latency (5)  
DSCP Class Selector 7 - COS Video < 100ms Latency (5)

Delete Classification

Match Classifications:

IP Precedence: Routine (0)    Apply Class of Service: Best Effort (0)    Add

IP DSCP: Best Effort    Best Effort (0)    Add

(0-63)

IP Protocol 119    Best Effort (0)    Add

Filter: No Filters defined. [Define Filters](#).

Rate Limiting:

Bits per Sec.: (8000-2000000000)    Burst Rate (Bytes): (1000-512000000)

Conform Action: Transmit    Exceed Action: Drop    Add

Apply    Delete    Cancel

Apply Policies to Interface/ VLANs

	FastEthernet	Radio0-802.11G	Radio1-802.11A
Incoming	< NONE >	< NONE >	video_policy
Outgoing	video_policy	< NONE >	video_policy

Apply    Cancel

230774



## フィルタの設定

---

この章では、Web ブラウザ インターフェイスを使用して、アクセス ポイントに MAC アドレス、IP、および EtherType フィルタを設定し、管理する方法について説明します。この章の内容は、次のとおりです。

- 「フィルタの概要」(P.16-2)
- 「CLI を使用したフィルタの設定」(P.16-2)
- 「Web ブラウザ インターフェイスを使ったフィルタの設定」(P.16-3)

## フィルタの概要

プロトコルフィルタ (IP プロトコル、IP ポート、および EtherType) は、アクセス ポイントのイーサネット ポートや無線ポートを経由した特定のプロトコルの使用を許可または禁止するために使用します。プロトコルフィルタは個別に、または複数をもとめて設定することができます。無線クライアント デバイス、または有線 LAN 上のユーザ、あるいはその両方について、プロトコルをフィルタできます。たとえば、アクセス ポイントの無線ポートに SNMP フィルタを設定すると、無線クライアント デバイスはアクセス ポイントで SNMP を使用できなくなります。しかし、有線 LAN からの SNMP アクセスは排除されません。

IP アドレスフィルタや MAC アドレスフィルタによって、特定の IP アドレスや MAC アドレスに対して送受信されるユニキャストおよびマルチキャスト パケットの転送が許可または禁止されます。指定以外のすべてのアドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべてのアドレスへのトラフィックを排除するフィルタを作成することもできます。

フィルタの設定には、Web ブラウザ インターフェイスを使用するか、または CLI にコマンドを入力します。



ヒント

アクセス ポイントの QoS ポリシーにフィルタを追加することもできます。QoS ポリシーの設定手順の詳細は、第 15 章「QoS の設定」を参照してください。



(注)

CLI を使用した場合、フィルタに設定できる MAC アドレスは最大 2,048 個です。Web ブラウザ インターフェイスを使用した場合には、フィルタに設定できる MAC アドレスは最大でも 43 個です。

## CLI を使用したフィルタの設定

CLI コマンドを使用してフィルタを設定するには、アクセス コントロール リスト (ACL) とブリッジグループを使用します。これらの概念に関する説明や、実装手順については、次の資料を参照してください。

- 『Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4』。このリンクをクリックすると、「Configuring Transparent Bridging」の章が表示されます。  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm\\_c/bcftp1/bcftb.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftp1/bcftb.htm)
- 『Catalyst 4908G-L3 Cisco IOS Release 12.0(10)W5(18e) Software Feature and Configuration Guide』。次のリンクをクリックすると、「Command Reference」の章を参照できます。  
[http://www.cisco.com/univercd/cc/td/doc/product/13sw/4908g\\_l3/ios\\_12/10w518e/config/cmd\\_ref.htm](http://www.cisco.com/univercd/cc/td/doc/product/13sw/4908g_l3/ios_12/10w518e/config/cmd_ref.htm)



(注)

ワイヤレス デバイスの設定に、CLI と Web ブラウザ インターフェイスの両方を使用することは避けてください。CLI を使用してワイヤレス デバイスを設定した場合、Web ブラウザ インターフェイスでは、設定が正しく表示されない場合があります。しかし、正しく表示されない場合でも、ワイヤレス デバイスは正しく設定されていることがあります。たとえば、CLI を使用して ACL を設定すると、Web ブラウザ インターフェイスに次のメッセージが表示されることがあります。「Filter 700 was configured on interface Dot11Radio0 using CLI. It must be cleared via

CLI to ensure proper operation of the web interface」。このメッセージが表示された場合、ACL を削除するには CLI を使用し、再設定するには Web ブラウザ インターフェイスを使用する必要があります。

## Web ブラウザ インターフェイスを使ったフィルタの設定

この項では、Web ブラウザ インターフェイスを使用してフィルタを設定し、有効化する方法について説明します。フィルタを設定し有効化する手順は次の 2 つにわかれます。

1. フィルタの設定ページを使用して、フィルタに名前をつけ、設定します。
2. [Apply Filters] ページを使用して、フィルタを有効化します。

次の項では 3 種類のフィルタの設定および有効化について説明します。

- 「MAC アドレス フィルタの設定と有効化」(P.16-3)
- 「IP フィルタの設定と有効化」(P.16-10)
- 「EtherType フィルタの設定と有効化」(P.16-14)

## MAC アドレス フィルタの設定と有効化

MAC アドレス フィルタによって、特定の MAC アドレスに対して送受信されるユニキャストおよびマルチキャスト パケットの転送が許可または禁止されます。指定以外のすべての MAC アドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべての MAC アドレスへのトラフィックを排除するフィルタを作成することもできます。作成したフィルタは、イーサネット ポートと無線ポートのいずれかまたは両方、および受信パケットと送信パケットのいずれかまたは両方に適用できます。



(注) CLI を使用して、フィルタリング用に MAC アドレスを設定することができますが、NVRAM の制約があるため、600 を超える MAC フィルタには FTP または TFTP が必要です。Web ブラウザ インターフェイスを使用した場合には、フィルタに設定できる MAC アドレスは最大でも 43 個です。



(注) MAC アドレス フィルタは強力なため、フィルタの設定を間違えると自分自身をアクセス ポイントからロックアウトしてしまう可能性があります。不注意でロックアウトされた場合は、CLI を使用してフィルタを無効にしてください。

[MAC Address Filters] ページを使用して、アクセス ポイントの MAC アドレス フィルタを作成します。図 16-1 は、[MAC Address Filters] ページを示しています。



図 16-1 [MAC Address Filters] ページ

HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP ASSOCIATION NETWORK INTERFACES SECURITY SERVICES Telnet/SSH Hot Standby CDP DNS Filters HTTP Proxy Mobile IP QoS SNMP NTP VLAN ARP Caching WIRELESS SERVICES SYSTEM SOFTWARE EVENT LOG

APPLY FILTERS MAC ADDRESS FILTERS IP FILTERS ETHERTYPE FILTERS

Hostname ap ap uptime is 2 days, 21 hours, 40 minutes

Services: Filters - MAC Address Filters

Create/Edit Filter Index: <NEW>

Filter Index: (700-799)

Add MAC Address: Mask: 0000.0000.0000 Action: Forward Add  
(HHHH.HHHH.HHHH) (HHHH.HHHH.HHHH)

Default Action: Block All

Filters Classes:

Delete Class

Apply Delete Cancel

次のリンク パスに従って、[Address Filters] ページを表示します。

1. ページ ナビゲーション バーの [Services] をクリックします。
2. [Services] ページ リストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [MAC Address Filters] タブをクリックします。

## MAC アドレス フィルタの作成

MAC アドレス フィルタを作成する手順は、次のとおりです。

- ステップ 1** リンク パスに従って、[MAC Address Filters] ページを表示します。
- ステップ 2** 新規 MAC アドレス フィルタを作成する場合、[Create/Edit Filter Index] メニューで [<NEW>] (デフォルト) が選択されていることを確認します。フィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ番号を選択します。
- ステップ 3** [Filter Index] フィールドで、フィルタに 700 ~ 799 の範囲で番号を付けます。割り当てた番号で、フィルタのアクセス コントロール リスト (ACL) が作成されます。
- ステップ 4** [Add MAC Address] フィールドに MAC アドレスを入力します。アドレスは、たとえば、0005.9a39.2110 のように、ピリオドを使って、4 つの英数字からなる 3 つのグループに分けて入力します。





(注) フィルタを確実に正しく動作させるためには、MAC アドレスで使用する文字はすべて小文字で入力してください。

- ステップ 5** [Mask] 入力フィールドには、フィルタが MAC アドレスに対して左から右にチェックするビット数を入力します。たとえば、MAC アドレスと正確に一致させる（すべてのビットをチェックする）には、**0000.0000.0000** と入力します。先頭 4 バイトだけをチェックするには、**0.0.FFFF** と入力します。
- ステップ 6** [Action] メニューから [Forward] または [Block] を選択します。
- ステップ 7** [Add] をクリックします。追加した MAC アドレスが [Filters Classes] フィールドに表示されます。[Filters Classes] リストから MAC アドレスを削除するには、そのアドレスを選択して [Delete Class] をクリックします。
- ステップ 8** このフィルタにさらにアドレスを追加するには、[ステップ 4](#) から [ステップ 7](#) を繰り返します。
- ステップ 9** [Default Action] メニューから [Forward All] または [Block All] を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つのアドレスのアクションの逆である必要があります。たとえば、複数のアドレスを入力したときに、これらのアドレスすべてに対するアクションとして [Block] を選択した場合、フィルタのデフォルト アクションには [Forward All] を選択する必要があります。

**ヒント**

許可された MAC アドレスのリストは、ネットワーク上の認証サーバに作成できます。MAC ベースの認証の使用方法については、「[認証タイプの設定](#)」(P.11-1) を参照してください。

- ステップ 10** [Apply] をクリックします。このフィルタはアクセス ポイントに保存されますが、[Apply Filters] ページで適用するまで有効化されません。
- ステップ 11** [Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。[図 16-2](#) は、[Apply Filters] ページを示しています。

図 16-2 [Apply Filters] ページ

		FastEthernet		Radio0-802.11B		Radio1-802.11A	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >	
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >	
	IP	< NONE >	IP	< NONE >	IP	< NONE >	
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >	
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >	
	IP	< NONE >	IP	< NONE >	IP	< NONE >	

**ステップ 12** [MAC] ドロップダウン リストの 1 つから、フィルタ番号を選択します。フィルタはイーサネットポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。

**ステップ 13** [Apply] をクリックします。選択したポートで、このフィルタが有効化されます。

クライアントがただちにフィルタされない場合は、[System Configuration] ページの [Reload] をクリックして、アクセスポイントを再起動します。[System Configuration] ページを表示するには、タスクメニューの [System Software] をクリックしてから、[System Configuration] をクリックします。



**(注)** 排除された MAC アドレスを持つクライアント デバイスは、アクセスポイントを介してデータを送受信できませんが、認証されていないクライアント デバイスとしてアソシエーションテーブルに保持されている場合があります。排除された MAC アドレスを持つクライアント デバイスは、アクセスポイントによるモニタリングが停止した場合、アクセスポイントがリブートした場合、またはクライアントが別のアクセスポイントとアソシエートした場合に、アソシエーションテーブルから消去されます。

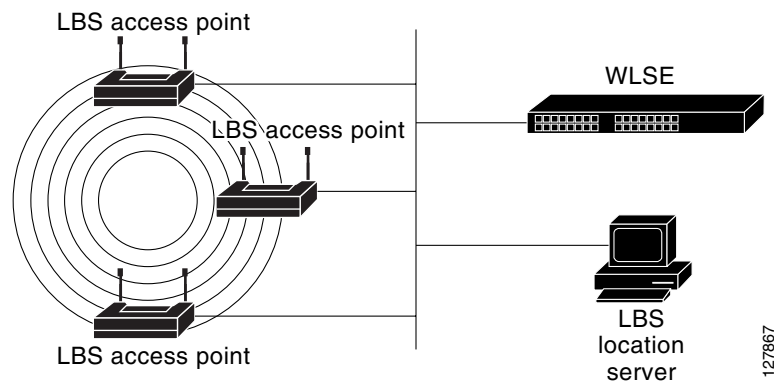
## MAC アドレス ACL を使用したアクセス ポイントへのクライアント アソシエーションの許可と禁止

MAC アドレス ACL を使用して、アクセス ポイントへのクライアント アソシエーションを許可または禁止できます。インターフェイスを通過するトラフィックをフィルタする代わりに、ACL を使用して、アクセス ポイントの無線とのアソシエーションをフィルタします。

ACL を使用して、アクセス ポイントの無線へのアソシエーションをフィルタする手順は、次のとおりです。

- ステップ 1** 「[MAC アドレス フィルタの作成](#)」(P.16-4) のステップ 1 ~ 10 に従って、ACL を作成します。アソシエートを許可する MAC アドレスについては、[Action] メニューから [Forward] を選択します。アソシエートを禁止するアドレスについては、[Block] を選択します。[Default Action] メニューから [Block All] を選択します。
- ステップ 2** [Security] をクリックして [Security Summary] ページを表示します。図 16-3 は、[Security Summary] ページを示しています。

図 16-3 [Security Summary] ページ



**ステップ 3** [Advanced Security] をクリックして、[Advanced Security: MAC Address Authentication] ページを表示します。図 16-4 は、[MAC Address Authentication] ページを示しています。

図 16-4 [Advanced Security : MAC Address Authentication] ページ

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
**SECURITY**  
Admin Access  
Encryption Manager  
SSID Manager  
Server Manager  
AP Authentication  
Intrusion Detection  
Local RADIUS Server  
**Advanced Security**  
SERVICES +  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

MAC ADDRESS AUTHENTICATION    TIMERS    ASSOCIATION ACCESS LIST

Hostname AP1242AG    AP1242AG uptime is 2 days, 16 hours, 34 minutes

Security: Advanced Security- MAC Address Authentication

MAC Address Authentication

MAC Addresses Authenticated by:

Local List Only  
 Authentication Server Only  
 Authentication Server if not found in Local List  
 Local List if no response from Authentication Server

Apply    Cancel

Local MAC Address List

Local List:

	Delete
--	--------

New MAC Address:  (HHHH.HHHH.HHHH)    Apply

146321

**ステップ 4** [Association Access List] タブをクリックして [Association Access List] ページを表示します。図 16-5 は [Association Access List] ページを示しています。

図 16-5 [Association Access List] ページ

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
**SECURITY**  
Admin Access  
Encryption Manager  
SSID Manager  
Server Manager  
Local RADIUS Server  
**Advanced Security**  
SERVICES +  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

MAC ADDRESS AUTHENTICATION    TIMERS    ASSOCIATION ACCESS LIST

Hostname ap    ap uptime is 11 minutes

Security: Advanced Security- Association Access List

Filter client association with MAC address access list: < NONE >    Define Filter

Apply    Cancel

111861

- ステップ 5** ドロップダウン リストから、必要な MAC アドレス ACL を選択します。
- ステップ 6** [Apply] をクリックします。

## Time-Based ACL の作成

Time-based ACL は、一定の時間、有効または無効にできる ACL です。この機能は、特定の種類のトラフィックを許可または拒否するアクセス コントロール ポリシーを定義する柔軟性と堅牢性を提供します。

この例は、CLI で Time-based ACL を設定する方法を説明しています。ここでは、平日の就業時間中、内部から外部への Telnet 接続が許可されています。



- (注)** Time-based ACL は、必要に応じて Aironet AP のファスト イーサネット ポートまたは無線ポートで定義できます。Bridge Group Virtual Interface (BVI; ブリッジグループ仮想インターフェイス) に適用されることはありません。

次の手順に従って Time-based ACL を作成します。

- ステップ 1** CLI で AP にログインします。
- ステップ 2** イーサネット インターフェイスまたは無線インターフェイスを介して ACL にアクセスするには、コンソール ポートまたは Telnet を使用します。
- ステップ 3** グローバル コンフィギュレーション モードを開始します。
- ステップ 4** Time Range を作成します。この例では Test です。

```
AP<config>#time-range Test
```

- ステップ 5** time-range を作成します。

```
AP<config>#time-range periodic weekdays 7:00 to 19:00
```



- (注)** 平日の 7 : 00 ~ 19 : 00 時までユーザのアクセスを許可します。

- ステップ 6** ACL を作成します。この例では 101 です。

```
AP<config># ip access-list extended 101
```

```
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test
```



- (注)** この ACL は、Test で指定した時間範囲の間、ネットワークへの Telnet トラフィックの出入りを許可します。平日の AP への Telnet セッションも許可します。

**ステップ 7** Time-based ACL をイーサネット インターフェイスに適用します。

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
```

---

## ACL ロギング

ACL ロギングは、AP プラットフォームのブリッジング インターフェイスではサポートされていません。ブリッジング インターフェイスに適用すると、「log」オプションを指定せずに設定したかのように動作し、ロギングは行われません。ただし、BVI インターフェイスに対しては、独立した ACL が使用される限り、ACL ロギングは行われます。

## CLI の設定例

次の例は、「[MAC アドレス ACL を使用したアクセス ポイントへのクライアント アソシエーションの許可と禁止](#)」(P.16-7) に記載された手順と同じ働きをする CLI コマンドを示しています。

```
AP# configure terminal
AP(config)# dot11 association access-list 777
AP(config)# end
```

この例では、アクセス リスト 777 にリストされている MAC アドレスを持つクライアント デバイスだけが、アクセス ポイントへのアソシエーションを許可されています。その他の MAC アドレスからのアソシエーションは、アクセス ポイントによりブロックされます。

この例で使用されているコマンドの詳細については、『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』を参照してください。

## IP フィルタの設定と有効化

IP フィルタ (IP アドレス、IP プロトコル、および IP ポート) は、アクセス ポイントのイーサネット ポートや無線ポートを経由した特定のプロトコルの使用を許可または禁止するために使用します。また、IP アドレス フィルタを使用して、特定の IP アドレスとの間で送受信されるユニキャスト パケットやマルチキャスト パケットの転送を許可または禁止することができます。指定以外のすべてのアドレスにトラフィックを転送するフィルタを作成することも、指定以外のすべてのアドレスへのトラフィックを排除するフィルタを作成することもできます。IP フィルタ方法の 1 つ、2 つ、または 3 つすべての要素をすべて含むフィルタを作成できます。作成したフィルタは、イーサネット ポートと無線ポートのいずれかまたは両方、および受信パケットと送信パケットのいずれかまたは両方に適用できます。

[IP Filters] ページを使用して、アクセス ポイントの IP フィルタを作成します。図 16-6 は、[IP Filters] ページを示しています。

図 16-6 [IP Filters] ページ

HOME  
EXPRESS SET-UP  
EXPRESS SECURITY  
NETWORK MAP +  
ASSOCIATION +  
NETWORK INTERFACES +  
SECURITY +  
**SERVICES**  
Telnet/SSH  
Hot Standby  
CDP  
DNS  
**Filters**  
HTTP  
Proxy Mobile IP  
QoS  
SNMP  
NTP  
VLAN  
ARP Caching  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

APPLY FILTERS    MAC ADDRESS FILTERS    **IP FILTERS**    ETHERTYPE FILTERS

Hostname ap    ap uptime is 2 hours, 49 minutes

**Services: Filters - IP Filters**

Create/Edit Filter Name: <NEW>

Filter Name:

Default Action: Block.All

**IP Address**

Destination Address:  Mask: 0.0.0.0

Source Address: 0.0.0.0 Mask: 255.255.255.255

Action: Forward Add

**IP Protocol**

IP Protocol:  Authentication Header Protocol (51) Action: Forward Add

Custom  (0-255)

**UDP/TCP Port**

TCP Port:  Border Gateway Protocol (179) Action: Forward Add

Custom  (0-65535)

UDP Port:  Biff (mail notification, comsat, 512) Action: Forward Add

Custom  (0-65535)

**Filters Classes**

Delete Class

Apply Delete Cancel

[IP Filters] ページは、次のリンク パスに従って表示します。

1. ページナビゲーションバーの [Services] をクリックします。
2. [Services] ページリストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [IP Filters] タブをクリックします。

## IP フィルタの作成

IP フィルタを作成する手順は、次のとおりです。

- 
- ステップ 1** リンク パスに従って、[IP Filters] ページを表示します。
  - ステップ 2** 新規フィルタを作成する場合、[Create/Edit Filter Index] メニューで [<NEW>] (デフォルト) が選択されていることを確認します。既存のフィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ名を選択します。
  - ステップ 3** [Filter Name] フィールドに、新しいフィルタにつける、わかりやすい名前を入力します。
  - ステップ 4** フィルタのデフォルト アクションとして、[Default Action] メニューから [Forward All] または [Block All] を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つのアドレスのアクションの逆である必要があります。たとえば、IP アドレス、IP プロトコル、IP ポートに適用されるフィルタを作成し、これらすべてに対するアクションとして [Block] を選択した場合、フィルタのデフォルト アクションには [Forward All] を選択する必要があります。
  - ステップ 5** IP アドレスをフィルタリングするには、[IP Address] フィールドにアドレスを入力します。



**(注)** 許可された MAC アドレスを除き、すべての IP アドレスへのトラフィックを禁止する場合は、自分の PC のアドレスを許可された MAC アドレスのリストに入力し、アクセスポイントへの接続が失われないようにします。

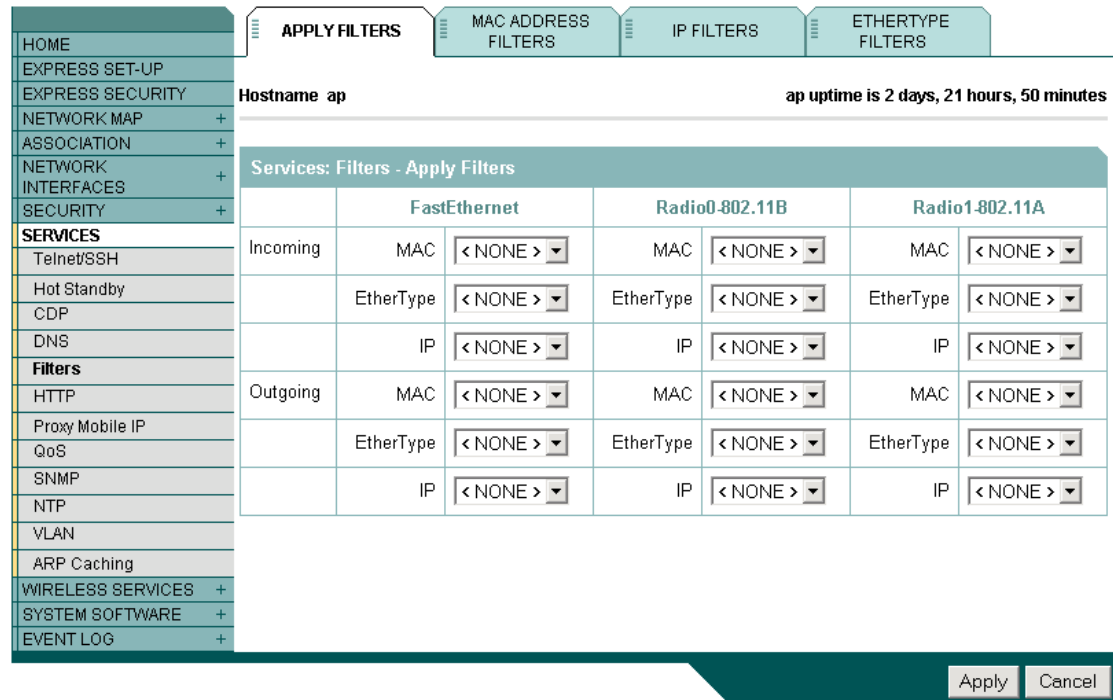
---

- ステップ 6** [Mask] フィールドに、この IP アドレスで使用するマスクを入力します。このマスクは、たとえば、112.334.556.778 のように、ピリオドを使って、文字のグループに分けて入力します。マスクに 255.255.255.255 を指定した場合、このアクセス ポイントはすべての IP アドレスを受け付けるようになります。0.0.0.0 を指定した場合、[IP Address] フィールドに入力した IP アドレスと完全に一致するアドレスが検索されます。このフィールドに入力したマスクは、CLI に入力したマスクと同様の動作をします。
- ステップ 7** [Action] メニューから [Forward] または [Block] を選択します。
- ステップ 8** [Add] をクリックします。追加したアドレスが [Filters Classes] フィールドに表示されます。[Filters Classes] リストからアドレスを削除するには、そのアドレスを選択して [Delete Class] をクリックします。このフィルタにさらにアドレスを追加するには、[ステップ 5](#) から [ステップ 8](#) を繰り返します。  
フィルタに IP プロトコルや IP ポート要素を追加する必要がない場合は、[ステップ 15](#) にスキップして、アクセスポイントにフィルタを保存します。
- ステップ 9** IP プロトコルをフィルタリングするには、[IP Protocol] ドロップダウン リストから共通プロトコルの 1 つを選択するか、[Custom] オプション ボタンを選択して、既存の ACL 番号を [Custom] フィールドに入力します。ACL 番号を 0 ~ 255 の範囲で入力します。IP プロトコルと対応する識別番号の一覧については、[付録 A 「プロトコル フィルタ」](#) を参照してください。
- ステップ 10** [Action] メニューから [Forward] または [Block] を選択します。
- ステップ 11** [Add] をクリックします。追加したプロトコルが [Filters Classes] フィールドに表示されます。[Filters Classes] リストからプロトコルを削除するには、そのプロトコルを選択して [Delete Class] をクリックします。このフィルタにさらにプロトコルを追加するには、[ステップ 9](#) から [ステップ 11](#) を繰り返します。  
フィルタに IP ポート要素を追加する必要がない場合は、[ステップ 15](#) にスキップして、アクセスポイントにフィルタを保存します。



- ステップ 12** TCP、または UDP ポート プロトコルをフィルタリングするには、[TCP Port]、または [UDP Port] ドロップダウン リストから共通ポート プロトコルの 1 つを選択するか、[Custom] オプション ボタンを選択して、既存のプロトコル番号を [Custom] フィールドの 1 つに入力します。プロトコル番号を 0 ～ 65535 の範囲で入力します。IP ポートプロトコルと対応する識別番号の一覧については、付録 A 「プロトコルフィルタ」を参照してください。
- ステップ 13** [Action] メニューから [Forward] または [Block] を選択します。
- ステップ 14** [Add] をクリックします。追加したプロトコルが [Filters Classes] フィールドに表示されます。[Filters Classes] リストからプロトコルを削除するには、そのプロトコルを選択して [Delete Class] をクリックします。このフィルタにさらにプロトコルを追加するには、ステップ 12 からステップ 14 を繰り返します。
- ステップ 15** フィルタが完成したら、[Apply] をクリックします。このフィルタはアクセス ポイントに保存されますが、[Apply Filters] ページで適用するまで有効化されません。
- ステップ 16** [Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。図 16-7 は、[Apply Filters] ページを示しています。

図 16-7 [Apply Filters] ページ



- ステップ 17** IP ドロップダウン リストの 1 つから、フィルタ名を選択します。フィルタはイーサネットポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。
- ステップ 18** [Apply] をクリックします。選択したポートで、このフィルタが有効化されます。

## EtherType フィルタの設定と有効化

EtherType フィルタは、アクセス ポイントのイーサネット ポートと無線ポートを経由した特定のプロトコルの使用を許可または禁止するために使用します。作成したフィルタは、イーサネット ポートと無線ポートのいずれかまたは両方、および受信パケットと送信パケットのいずれかまたは両方に適用できます。

[EtherType Filters] ページを使用して、アクセス ポイントの EtherType フィルタを作成します。図 16-8 は、[EtherType Filters] ページを示しています。

図 16-8 [EtherType Filters] ページ

HOME EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP + ASSOCIATION + NETWORK INTERFACES + SECURITY + SERVICES Telnet/SSH Hot Standby CDP DNS Filters HTTP Proxy Mobile IP QoS SNMP NTP VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +

APPLY FILTERS MAC ADDRESS FILTERS IP FILTERS ETHERTYPE FILTERS

Hostname ap ap uptime is 2 hours, 55 minutes

Services: Filters - EtherType Filters

Create/Edit Filter Index: <NEW>

Filter Index: (200-299)

Add EtherType: (0-FFFF) Mask: (0-FFFE) Action: Forward Add

Default Action: Block All

Filters Classes:

Delete Class

Apply Delete Cancel

次のリンク パスに従って、[EtherType Filters] ページを表示します。

1. ページ ナビゲーション バーの [Services] をクリックします。
2. [Services] ページ リストで [Filters] をクリックします。
3. [Apply Filters] ページで、ページの最上部にある [EtherType Filters] タブをクリックします。

## EtherType フィルタの作成

EtherType フィルタを作成する手順は、次のとおりです。

- ステップ 1** リンク パスに従って、[EtherType Filters] ページを表示します。
- ステップ 2** 新規フィルタを作成する場合、[Create/Edit Filter Index] メニューで [<NEW>] (デフォルト) が選択されていることを確認します。既存のフィルタを編集するには、[Create/Edit Filter Index] メニューからフィルタ番号を選択します。
- ステップ 3** [Filter Index] フィールドで、フィルタに 200 ~ 299 の範囲で番号を付けます。割り当てた番号で、フィルタのアクセス コントロール リスト (ACL) が作成されます。
- ステップ 4** [Add EtherType] フィールドに EtherType 番号を入力します。プロトコルと対応する識別番号の一覧については、[付録 A 「プロトコル フィルタ」](#) を参照してください。
- ステップ 5** [Mask] フィールドに、この EtherType で使用するマスクを入力します。マスクに **0** を指定した場合、EtherType との正確な一致が必要になります。
- ステップ 6** [Action] メニューから [Forward] または [Block] を選択します。
- ステップ 7** [Add] をクリックします。追加した EtherType が [Filters Classes] フィールドに表示されます。[Filters Classes] リストから EtherType を削除するには、その EtherType を選択して [Delete Class] をクリックします。このフィルタにさらに Ethertype を追加するには、[ステップ 4](#) から [ステップ 7](#) を繰り返します。
- ステップ 8** [Default Action] メニューから [Forward All] または [Block All] を選択します。このフィルタのデフォルト アクションは、フィルタに含まれる少なくとも 1 つの EtherType のアクションの逆である必要があります。たとえば、複数の EtherType を入力したときに、これらの Ethertype すべてに対するアクションとして [Block] を選択した場合、フィルタのデフォルト アクションには [Forward All] を選択する必要があります。
- ステップ 9** [Apply] をクリックします。このフィルタはアクセス ポイントに保存されますが、[Apply Filters] ページで適用するまで有効化されません。
- ステップ 10** [Apply Filters] タブをクリックして [Apply Filters] ページに戻ります。[図 16-9](#) は、[Apply Filters] ページを示しています。

図 16-9 [Apply Filters] ページ

Hostname ap ap uptime is 2 days, 21 hours, 50 minutes

Services: Filters - Apply Filters						
	FastEthernet		Radio0-802.11B		Radio1-802.11A	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >

Apply Cancel

**ステップ 11** [EtherType] ドロップダウン リストの 1 つから、フィルタ番号を選択します。フィルタはイーサネット ポートと無線ポートのいずれか、または両方に適用できます。また、受信パケットか送信パケット、または両方に適用することも可能です。

**ステップ 12** [Apply] をクリックします。選択したポートで、このフィルタが有効化されます。



## CDP の設定

---

この章では、アクセス ポイントに Cisco Discovery Protocol (CDP) を設定する方法について説明します。



(注)

---

この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco Aironet IOS Command Reference for Access Points and Bridges*』、およびリリース 12.2 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

---

この章の内容は、次のとおりです。

- 「CDP の概要」 (P.17-2)
- 「CDP の設定」 (P.17-2)
- 「CDP のモニタおよびメンテナンス」 (P.17-5)

## CDP の概要

Cisco Discovery Protocol (CDP) は、すべてのシスコ製ネットワーク機器で実行されるデバイス検出プロトコルです。各デバイスはマルチキャストアドレスに識別メッセージを送信し、他のデバイスから送信されたメッセージをモニタします。CDP パケット内の情報は、CiscoWorks2000 などのネットワーク管理ソフトウェアで使用されます。

デフォルトでは、CDP はアクセス ポイントのイーサネット ポートで有効になっています。アクセス ポイントの無線ポートでは、無線がアクセス ポイントやブリッジなどの他の無線インフラストラクチャデバイスにアソシエートされている場合だけ CDP が有効です。CDP は、アクセス ポイントに設定された最小の VLAN 番号に送信されます。無線ネットワークで複数の VLAN が使用される場合、設定された最小の VLAN 番号をネイティブ VLAN として使用することを推奨します。



(注)

無線 LAN で最大限のパフォーマンスを得るために、VLAN がアクセス ポイントで有効になっている場合は、すべての無線インターフェイスおよびサブインターフェイスで CDP を無効にします。

## CDP の設定

この項では、CDP の設定情報と設定の手順を説明します。

- 「CDP のデフォルト設定」(P.17-2)
- 「CDP 特性の設定」(P.17-2)
- 「CDP のディセーブル化およびイネーブル化」(P.17-3)
- 「インターフェイス上での CDP のディセーブル化およびイネーブル化」(P.17-4)

## CDP のデフォルト設定

表 17-1 は、デフォルトの CDP 設定を示しています。

表 17-1 CDP のデフォルト設定

機能	デフォルト設定
CDP グローバル ステート	イネーブル
CDP インターフェイス ステート	イネーブル
CDP 保持時間 (パケットの保持時間、秒)	180
CDP タイマー (パケットの送信間隔、秒)	60

## CDP 特性の設定

CDP 保持時間 (アクセス ポイントが CDP パケットを廃棄するまでの秒数) と CDP タイマー (アクセス ポイントが次の CDP パケットを送信するまでの秒数) を設定できます。

特権 EXEC モードから、次の手順に従って CDP 保持時間と CDP タイマーを設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>cdp holdtime seconds</b>	(任意) デバイスから送信された情報を受信側デバイスが廃棄するまで保持する期間を指定します。 有効範囲は 10 ~ 255 秒で、デフォルトは 180 秒です。
ステップ 3	<b>cdp timer seconds</b>	(任意) CDP 更新の送信頻度 (秒) を設定します。 有効範囲は 5 ~ 254 秒で、デフォルトは 60 秒です。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。

デフォルト設定に戻すには、CDP コマンドの **no** 形式を使用します。

次の例は、CDP 特性を設定し、確認する方法を示しています。

```
AP# configure terminal
AP(config)# cdp holdtime 120
AP(config)# cdp timer 50
AP(config)# end

AP# show cdp

Global CDP information:
    Sending a holdtime value of 120 seconds
    Sending CDP packets every 50 seconds
```

その他の CDP **show** コマンドについては、「[CDP のモニタおよびメンテナンス](#)」(P.17-5) を参照してください。

## CDP のディセーブル化およびイネーブル化

CDP はデフォルトで有効になっています。特権 EXEC モードから、次の手順に従って CDP デバイス検出機能を無効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>no cdp run</b>	CDP をディセーブルにします。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。

特権 EXEC モードから、次の手順に従って CDP を有効にします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>cdp run</b>	ディセーブル化されている CDP をイネーブルにします。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。

次の例は CDP を有効にする方法を示しています。

```
AP# configure terminal
AP(config)# cdp run
AP(config)# end
```

## インターフェイス上での CDP のディセーブル化およびイネーブル化

デフォルトでは、CDP は CDP 情報の送受信がサポートされるすべてのインターフェイスで有効になっています。

特権 EXEC モードから、次の手順に従ってインターフェイス上の CDP を無効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、CDP をディセーブルにするインターフェイスを入力します。
ステップ 3	<code>no cdp enable</code>	インターフェイスの CDP をディセーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

特権 EXEC モードから、次の手順に従ってインターフェイス上の CDP を有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	インターフェイス コンフィギュレーション モードを開始し、CDP をイネーブルにするインターフェイスを入力します。
ステップ 3	<code>cdp enable</code>	ディセーブルになっているインターフェイスの CDP をイネーブルにします。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

次の例はインターフェイスで CDP を有効にする方法を示しています。

```
AP# configure terminal
AP(config)# interface x
AP(config-if)# cdp enable
AP(config-if)# end
```



# CDP のモニタおよびメンテナンス

デバイス上の CDP をモニタおよびメンテナンスするには、特権 EXEC モードで次の手順を 1 つまたは複数実行します。

コマンド	説明
<code>clear cdp counters</code>	トラフィック カウンタをゼロにリセットします。
<code>clear cdp table</code>	ネイバーに関する情報を格納する CDP テーブルを削除します。
<code>show cdp</code>	送信の頻度、送信されたパケットのホールドタイムなど、グローバルな情報を表示します。
<code>show cdp entry entry-name</code> <code>[protocol   version]</code>	特定のネイバーに関する情報を表示します。 アスタリスク (*) を入力してすべての CDP ネイバーを表示することも、情報が必要なネイバーの名前を入力することもできます。 また、指定されたネイバー上でイネーブになっているプロトコルの情報や、デバイス上で稼働しているソフトウェアのバージョン情報が表示されるように、表示内容を制限することもできます。
<code>show cdp interface [type number]</code>	CDP がイネーブに設定されているインターフェイスに関する情報を表示します。 表示対象を、インターフェイスのタイプまたは情報が必要なインターフェイスの番号に限定できます (たとえば、 <b>gigabitethernet 0/1</b> と入力すると、ギガビット イーサネット ポート 1 に関する情報だけが表示されます)。
<code>show cdp neighbors [type number]</code> <code>[detail]</code>	デバイス タイプ、インターフェイスのタイプや番号、ホールドタイム設定、機能、プラットフォーム、ポート ID など、ネイバーに関する情報を表示します。 表示対象を特定のタイプのネイバーやインターフェイスの番号に限定することも、表示対象を拡大してより詳細な情報を得ることもできます。
<code>show cdp traffic</code>	CDP カウンタ (送受信されたパケット数、チェックサム エラーなど) を表示します。

次に、CDP の `show` 特権 EXEC コマンドの 6 つの出力例を示します。

```
AP# show cdp
Global CDP information:
  Sending CDP packets every 50 seconds
  Sending a holdtime value of 120 seconds

AP# show cdp entry *
-----
Device ID: AP
Entry address(es):
IP address: 10.1.1.66
Platform: cisco WS-C3550-12T, Capabilities: Switch IGMP
Interface: GigabitEthernet0/2, Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 129 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Experimental Version 12.1(20010612:021
316) [jang-flamingo 120]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 06-Jul-01 18:18 by jang
```

```
advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
FFFFFFFFF010221FF000000000000000024B293A00FF0000
VTP Management Domain: ''
Duplex: full
```

```
-----
Device ID: idf2-1-lab-13.cisco.com
Entry address(es):
IP address: 10.1.1.10
Platform: cisco WS-C3524-XL, Capabilities: Trans-Bridge Switch
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/10
Holdtime : 141 sec
```

```
Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.1)XP, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 10-Dec-99 11:16 by cchang
```

```
advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=25, value=0000000
FFFFFFFFF010101FF0000000000000000142EFA400FF
VTP Management Domain: ''
```

```
AP# show cdp entry * protocol
Protocol information for talSwitch14 :
IP address: 172.20.135.194
Protocol information for tstswitch2 :
IP address: 172.20.135.204
  IP address: 172.20.135.202
Protocol information for tstswitch2 :
IP address: 172.20.135.204
  IP address: 172.20.135.202
```

```
AP# show cdp interface
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/2 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/3 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/4 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/5 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/6 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/7 is up, line protocol is down
  Encapsulation ARPA
```

```
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
GigabitEthernet0/8 is up, line protocol is down
Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
```

AP# **show cdp neighbor**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater

```
Device IDLocal InterfaceHoldtmeCapabilityPlatformPort ID
Perdido2Gig 0/6125R S IWS-C3550-1Gig0/6
Perdido2Gig 0/5125R S IWS-C3550-1Gig 0/5
```

AP# **show cdp traffic**

CDP counters :

```
Total packets output: 50882, Input: 52510
Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
No memory: 0, Invalid packet: 0, Fragmented: 0
CDP version 1 advertisements output: 0, Input: 0
CDP version 2 advertisements output: 50882, Input: 52510
```





# 第 18 章

## SNMP の設定

---

この章では、アクセス ポイントで簡易ネットワーク管理プロトコル (SNMP) を設定する方法について説明します。



(注)

---

この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*』、および Release 12.3 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

---

この章の内容は、次のとおりです。

- 「SNMP の概要」 (P.18-2)
- 「SNMP の設定」 (P.18-5)
- 「SNMP ステータスの表示」 (P.18-13)

## SNMP の概要

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージフォーマットを提供します。SNMP マネージャは、CiscoWorks などのネットワーク管理システム (NMS) に統合できます。エージェントと管理情報ベース (MIB) は、アクセスポイント上に置かれます。アクセスポイント上で SNMP を設定する場合、マネージャとエージェント間の関連性を定義します。

SNMP エージェントは MIB 変数を格納し、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりできます。エージェントは、デバイスパラメータやネットワークデータの保存場所である MIB から値を収集します。また、エージェントはマネージャのデータ取得またはデータ設定の要求に応答できます。

エージェントは非送信請求トラップをマネージャに送信できます。トラップは、ネットワーク上のある状態を SNMP マネージャに通知するメッセージです。トラップは不正なユーザ認証、再起動、リンクステータス (アップまたはダウン)、MAC アドレス追跡、TCP 接続の終了、ネイバーとの接続の切断などの重要なイベントの発生を意味する場合があります。

この項では、次の概念を説明します。

- 「SNMP バージョン」 (P.18-2)
- 「SNMP マネージャ機能」 (P.18-3)
- 「SNMP エージェント機能」 (P.18-4)
- 「SNMP コミュニティストリング」 (P.18-4)
- 「SNMP を使用して MIB 変数にアクセスする方法」 (P.18-4)

## SNMP バージョン

このソフトウェアリリースでは、次の SNMP バージョンをサポートします。

- SNMPv1 : 簡易ネットワーク管理プロトコル。RFC 1157 で定義される詳細なインターネット規格。
- SNMPv2C には、次の機能があります。
  - SNMPv2 : 簡易ネットワーク管理プロトコルのバージョン 2。RFC 1902 ~ 1907 で定義されるドラフト インターネット規格。
  - SNMPv2C : SNMPv2 のコミュニティベースの管理フレームワーク。RFC 1901 で定義される試用段階のインターネットプロトコル。
- SNMPv3 には、次の機能があります。
  - SHA および Message Digest 5 (MD5; メッセージダイジェスト 5) 認証プロトコルと DES56 暗号のサポート。
  - 3 つのセキュリティレベル : 認証なしプライバシーなし (NoAuthNoPriv)、認証ありプライバシーなし (AuthNoPriv)、および認証ありプライバシーあり (AuthPriv)。

SNMPv3 は、SNMP 通信に利用できる高度なセキュリティをサポートしています。SNMPv1 と SNMPv2 のコミュニティストリングは、暗号化なしのプレーンテキストとして格納、転送されます。SNMPv3 セキュリティモデルでは、SNMP ユーザはユーザグループの認証と参加を行います。システムデータへのアクセスは、グループに基づいて制限されます。

SNMP エージェントは、管理ステーションでサポートされる SNMP のバージョンを使用するように設定する必要があります。エージェントは複数のマネージャと対話できるため、SNMPv3 プロトコルを使用する管理ステーションや、SNMPv2 または SNMPv1 プロトコルを使用する管理ステーションとの通信をサポートするようにソフトウェアを設定できます。

表 18-1 は、アクセス ポイントでサポートされている SNMP のバージョンとセキュリティ レベルを示しています。

表 18-1 SNMP のバージョンとセキュリティ レベル

SNMP Version	セキュリティ レベル	認証	暗号化
v1	NoAuthNoPriv	コミュニティ ストリングの一致	なし
v2C	NoAuthNoPriv	コミュニティ ストリングの一致	なし
v3	NoAuthNoPriv	ユーザ名の一致	なし
v3	AuthNoPriv	HMAC-MD5 または HMAC-SHA アルゴリズム	なし
v3	AuthPriv	HMAC-MD5 または HMAC-SHA アルゴリズム	データ暗号規格 (DES) 56 ビット暗号

SNMPv3 の詳細については、次のリンクをクリックして、Cisco IOS Release 12.0(3)T の「*New Feature Documentation*」を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/snmp3.htm>

## SNMP マネージャ機能

SNMP マネージャは、MIB 情報を使用して、表 18-2 に示す動作を実行します。

表 18-2 SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。 <sup>1</sup>
get-bulk-request <sup>2</sup>	テーブル内の複数行など、小さなデータ ブロックを数多く送信する代わりに、大きなブロックでデータを取得します。
get-response	NMS から送信される get-request、get-next-request、および set-request に対して応答します。
set-request	特定の変数に値を格納します。
trap	SNMP エージェントから SNMP マネージャに送られる、イベントの発生を伝える非送信請求メッセージです。

- この動作では、SNMP マネージャに正確な変数名を認識させる必要はありません。テーブル内を順に検索して、必要な変数を検出します。
- get-bulk コマンドは、SNMPv2 に限り機能します。

## SNMP エージェント機能

SNMP エージェントは、次のようにして SNMP マネージャ要求に応答します。

- **MIB 変数の取得**：SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、この値を使用して NMS に応答します。
- **MIB 変数の設定**：SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

エージェントで重要なイベントが発生したことを NMS に通知するために、SNMP エージェントは非送信請求トラップ メッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパニングツリートポロジが変更された場合、認証に失敗した場合などがあります。

## SNMP コミュニティストリング

SNMP コミュニティストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS がアクセスポイントにアクセスするためには、NMS のコミュニティストリングの定義が少なくともアクセスポイントの 3 つのコミュニティストリング定義のうち、1 つと一致している必要があります。

コミュニティストリングの属性は、次のいずれかです。

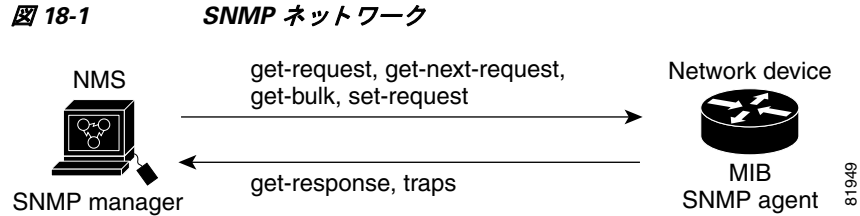
- **読み取り専用**：許可された管理ステーションへの読み取りアクセスを、コミュニティストリングを除く MIB のすべてのオブジェクトに許可しますが、書き込みアクセスは許可しません。
- **読み取り/書き込み**：許可された管理ステーションへの読み取りおよび書き込みアクセスを、MIB のすべてのオブジェクトに許可しますが、コミュニティストリングには許可しません。

## SNMP を使用して MIB 変数にアクセスする方法

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks 2000 ソフトウェアは、アクセスポイントの MIB 変数を使用して、デバイス変数を設定し、ネットワーク上のデバイスで特定の情報をポーリングします。ポーリング結果は、グラフ形式で表示されます。この結果を解析して、インターネットワーキング関連の問題のトラブルシューティング、ネットワークパフォーマンスの改善、デバイス設定の確認、トラフィック負荷のモニタなどを行うことができます。

図 18-1 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャにトラップ（特定のイベントの通知）を送信でき、SNMP マネージャはトラップを受信して処理します。トラップは、不適切なユーザ認証、再起動、リンクステータス（起動または停止）、MAC アドレスの追跡などの、ネットワーク上の状況を SNMP マネージャに警告するメッセージです。SNMP エージェントはさらに、SNMP マネージャから *get-request*、*get-next-request*、および *set-request* 形式で送信される MIB 関連のクエリに応答します。





サポート対象の MIB の詳細、およびアクセス手順については、付録 B 「サポート対象 MIB」を参照してください。

## SNMP の設定

この項では、アクセス ポイントで SNMP を設定する方法について説明します。内容は次のとおりです。

- 「SNMP のデフォルト設定」 (P.18-5)
- 「SNMP エージェントのイネーブル化」 (P.18-6)
- 「コミュニティ スtring の設定」 (P.18-6)
- 「SNMP サーバグループ名の指定」 (P.18-8)
- 「SNMP サーバホストの設定」 (P.18-8)
- 「SNMP サーバユーザの設定」 (P.18-8)
- 「トラップ マネージャの設定とトラップの有効化」 (P.18-9)
- 「エージェント コンタクトおよびロケーションの設定」 (P.18-11)
- 「snmp-server view コマンドの使用」 (P.18-11)
- 「SNMP での例」 (P.18-11)

## SNMP のデフォルト設定

表 18-3 に、SNMP のデフォルト設定を示します。

表 18-3 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	ディセーブル
SNMP コミュニティ スtring	どのストリングもデフォルトでは設定されていません。しかし、Web ブラウザ インターフェイスを使って SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、public コミュニティを生成します。
SNMP トラップ レシーバ	未設定
SNMP トラップ	有効なトラップなし。

## SNMP エージェントのイネーブル化

SNMP を有効にするための特定の CLI コマンドはありません。最初に入力したグローバル コンフィギュレーション コマンド `snmp-server` を使用すると、サポートされているバージョンの SNMP が有効になります。

また、Web ブラウザ インターフェイスの [SNMP Properties] ページで SNMP を有効にすることもできます。Web ブラウザ インターフェイスで SNMP を有効にする場合、アクセス ポイントは自動的に、IEEE802dot11 MIB 読み取り専用アクセスで、*public* と呼ばれるコミュニティ ストリングを生成します。

## コミュニティ ストリングの設定

SNMP マネージャとエージェントの関係を定義するには、SNMP コミュニティ ストリングを使用します。コミュニティ ストリングはパスワードと同様に機能し、アクセス ポイント上のエージェントへのアクセスを許可します。

ストリングに対応する次の特性を 1 つまたは複数指定することもできます。

- コミュニティ ストリングを使用してエージェントにアクセスできる SNMP マネージャの IP アドレスのアクセス リスト
- 指定のコミュニティにアクセスできるすべての MIB オブジェクトのサブセットを定義する MIB ビュー
- コミュニティにアクセスできる MIB オブジェクトの読み書き権限または読み取り専用権限



(注)

現在の Cisco IOS MIB エージェント実装では、デフォルトのコミュニティ ストリングは、インターネット MIB オブジェクト サブツリーに対するものです。IEEE802dot11 は、MIB オブジェクト ツリーの別のブランチのもとにあるため、IEEE802dot11 MIB 上の別のコミュニティ ストリングとビュー、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通のビューとコミュニティ ストリングのいずれかを有効にする必要があります。ISO は、IEEE (IEEE802dot11) およびインターネットの共通の親ノードです。この MIB エージェントの動作は、Cisco IOS ソフトウェアを実行していないアクセス ポイントでの MIB エージェントの動作とは異なります。

特権 EXEC モードから、次の手順に従ってアクセス ポイントにコミュニティ スtring を設定します。

コマンド	目的
ステップ 1 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>snmp-server community string</code> [ <code>access-list-number</code> ] [ <code>view mib-view</code> ] [ <code>ro</code>   <code>rw</code> ]	<p>コミュニティ スtring を設定します。</p> <ul style="list-style-type: none"> <li>• <code>string</code> には、パスワードと同様に機能し、SNMP プロトコルへのアクセスを許可する String を指定します。任意の長さのコミュニティ スtring を 1 つまたは複数設定できます。</li> <li>• (任意) <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の標準 IP アクセス リスト番号を入力します。</li> <li>• (任意) <code>view mib-view</code> には、<code>ieee802dot11</code> など、このコミュニティがアクセスできる MIB ビューを指定します。IEEE ビューを通じて標準 IEEE 802.11 MIB オブジェクトにアクセスする <code>snmp-server view</code> コマンドの使用方法については、「<a href="#">snmp-server view コマンドの使用</a>」(P.18-11)を参照してください。</li> <li>• (任意) 許可された管理ステーションで MIB オブジェクトを取得する場合は、読み取り専用 (<code>ro</code>) を指定し、許可された管理ステーションを使用して MIB オブジェクトを取得し、修正する場合は、読み取り/書き込み (<code>rw</code>) を指定します。デフォルトでは、コミュニティ スtring はすべてのオブジェクトに対する読み取り専用アクセスを許可します。</li> </ul> <p>(注) IEEE802dot11 MIB にアクセスするには、IEEE802dot11 MIB 上の別のコミュニティ スtring とビュー、あるいは、MIB オブジェクト ツリー内の ISO オブジェクト上の共通のビューとコミュニティ スtring を有効にする必要があります。</p>
ステップ 3 <code>access-list access-list-number</code> { <code>deny</code>   <code>permit</code> } <code>source</code> [ <code>source-wildcard</code> ]	<p>(任意) ステップ 2 で標準 IP アクセス リスト番号を指定してリストを作成した場合は、必要に応じてコマンドを繰り返します。</p> <ul style="list-style-type: none"> <li>• <code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。</li> <li>• <code>deny</code> キーワードは、条件が一致した場合にアクセスを拒否します。<code>permit</code> キーワードは、条件が一致した場合にアクセスを許可します。</li> <li>• <code>source</code> には、コミュニティ スtring を使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを入力します。</li> <li>• (任意) <code>source-wildcard</code> には、<code>source</code> に適用されるワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置には 1 を設定します。</li> </ul> <p>アクセス リストの末尾には、すべてに対する暗黙の拒否ステートメントが常に存在することに注意してください。</p>

	コマンド	目的
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティのコミュニティストリングをヌルストリングに設定します (コミュニティストリングに値を入力しないでください)。特定のコミュニティストリングを削除するには、`no snmp-server community string` グローバルコンフィギュレーションコマンドを使用します。

次の例は、コミュニティストリング `open` と `ieee` を SNMP に割り当てる方法、両方に対する読み取り/書き込みアクセスを許可する方法、`open` が非 IEEE802dot11-MIB オブジェクトのクエリに対するコミュニティストリングであり、`ieee` が IEEE802dot11 MIB オブジェクトのクエリに対するコミュニティストリングであることを指定する方法を示します。

```
ap(config)# snmp-server view dot11view ieee802dot11 included
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view ieee802dot11 rw
```

## SNMP サーバグループ名の指定

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
<code>snmp-server group [groupname {v1   v2c   v3 [auth   noauth   priv]}][read readview] [write writeview] [notify notifyview] [access access-list]</code>	新しい SNMP グループの設定、または SNMP ユーザを SNMP ビューにマップするテーブルの設定を行います。

## SNMP サーバホストの設定

SNMP トラップ操作の受信者を設定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
<code>snmp-server host host [traps   informs][version {1   2c   3 [auth   noauth   priv]}] community-string [udp-port port] [notification-type]</code>	SNMP トラップ操作の受信者を設定します。

## SNMP サーバユーザの設定

SNMP グループに新しいユーザを設定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
<code>snmp-server user username [groupname remote ip-address [udp-port port] {v1   v2c   v3 [encrypted]} [auth {md5   sha} auth-password [priv des56 priv password]] [access access-list]</code>	SNMP グループに新しいユーザを設定します。

## トラップ マネージャの設定とトラップの有効化

トラップ マネージャは、トラップを受信して処理する管理ステーションです。トラップは、特定のイベントが発生したときにアクセス ポイントが生成するシステム アラートです。デフォルトではトラップ マネージャは定義されておらず、トラップは発行されません。

この Cisco IOS Release を実行するアクセス ポイントには、トラップ マネージャを無制限に設定できます。コミュニティ スtring の長さは任意です。

表 18-4 は、サポートされるアクセス ポイントのトラップ（通知タイプ）を示しています。これらのトラップの一部または全部をイネーブルにして、これを受信するようにトラップ マネージャを設定できます。

表 18-4 通知タイプ

通知タイプ	説明
<b>authenticate-fail</b>	認証の失敗のトラップを有効にします。
<b>config</b>	SNMP 設定変更のトラップを有効にします。
<b>deauthenticate</b>	クライアント デバイスの認証取り消しのトラップを有効にします。
<b>disassociate</b>	クライアント デバイスのアソシエーション解除のトラップを有効にします。
<b>dot11-qos</b>	QoS 変更のトラップを有効にします。
<b>entity</b>	SNMP のエンティティ変更のトラップを有効にします。
<b>rogue-ap</b>	不正なアクセス ポイントの検出のトラップを有効にします。
<b>snmp</b>	SNMP イベントのトラップを有効にします。
<b>switch-over</b>	切り替えのトラップを有効にします。
<b>syslog</b>	syslog トラップを有効にします。
<b>wlan-wep</b>	WEP トラップを有効にします。

`udp-port` などの一部の通知タイプは、グローバル コンフィギュレーション コマンド `snmp-server enable` で制御できません。これらの通知タイプは、常に有効です。表 18-4 に示す通知タイプを受信するには、特定のホストに対して `snmp-server host` グローバル コンフィギュレーション コマンドを実行します。

特権 EXEC モードから、次の手順に従ってホストにトラップを送信するようにアクセス ポイントを設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server host host-addr {traps   informs} {version {1   2c   3 {auth   noauth   priv}}}</code> <code>community-string [udp-port port]</code> <code>notification-type</code>	<p>トラップ メッセージの受信側を指定します。</p> <ul style="list-style-type: none"> <li><code>host-addr</code> には、(ターゲットの受信者) ホストの名前またはアドレスを指定します。</li> <li>SNMP トラップをホストに送信するには、<b>traps</b> (デフォルト) を指定します。SNMP 情報をホストに送信するには、<b>informs</b> を指定します。</li> <li>サポートする SNMP バージョンを指定します。<b>informs</b> にはバージョン 1 (デフォルト) を使用できません。バージョン 3 には、次の 3 つのセキュリティ レベルがあります。 <ul style="list-style-type: none"> <li><b>auth</b> : 暗号化なしのパケットの認証を指定します。</li> <li><b>noauth</b> : パケットの認証と暗号化をしないように指定します。</li> <li><b>priv</b> : パケットの認証と暗号化を指定します。</li> </ul> </li> <li><code>community-string</code> には、通知動作時に送信するストリングを指定します。この文字列は <b>snmp-server host</b> コマンドを使用して設定できますが、<b>snmp-server community</b> コマンドでこの文字列を定義してから、<b>snmp-server host</b> コマンドを使用することを推奨します。</li> <li><code>notification-type</code> には、表 18-4 (P.18-9) 内のキーワードを使用します。</li> </ul>
ステップ 3	<code>snmp-server enable traps notification-types</code>	<p>アクセス ポイントで特定のトラップの送信を有効にします。トラップのリストは、表 18-4 (P.18-9) を参照してください。</p> <p>複数のタイプのトラップを有効にする場合、各トラップタイプに <b>snmp-server enable traps</b> コマンドを個別に発行します。</p>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定したホストがトラップを受信しないようにするには、**no snmp-server host host** グローバル コンフィギュレーション コマンドを使用します。特定のトラップタイプをディセーブルにするには、**no snmp-server enable traps notification-types** グローバル コンフィギュレーション コマンドを使用します。

## エージェント コンタクトおよびロケーションの設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>snmp-server contact text</code>	システムに関する問い合わせ先を表すストリングを設定します。 次に例を示します。 <code>snmp-server contact Dial System Operator at beeper 21555.</code>
ステップ 3	<code>snmp-server location text</code>	システムのロケーションを表すストリングを設定します。 次に例を示します。 <code>snmp-server location Building 3/Room 222</code>
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	入力内容を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## snmp-server view コマンドの使用

グローバル コンフィギュレーション モードで `snmp-server view` コマンドを使用して、IEEE ビューおよび dot11 読み取り/書き込みコミュニティ ストリングを通じて、標準 IEEE 802.11 MIB オブジェクトにアクセスします。

次の例は、IEEE ビューと dot11 読み取り/書き込みコミュニティ ストリングを有効にする方法を示しています。

```
AP(config)# snmp-server view ieee ieee802dot11 included
AP(config)# snmp-server community dot11 view ieee RW
```

## SNMP での例

次の例は、SNMPv1、SNMPv2C、および SNMPv3 を有効にする方法を示しています。この設定では、任意の SNMP マネージャがコミュニティ ストリング `public` を使用して、読み取り専用権限ですべてのオブジェクトにアクセスできます。この設定でアクセス ポイントがトラップを送信することはありません。

```
AP(config)# snmp-server community public
```

次の例は、コミュニティ ストリング `open` と `ieee` を SNMP に割り当てる方法、両方に対する読み取り/書き込みアクセスを許可する方法、`open` が非 IEEE802dot11-MIB オブジェクトのクエリに対するコミュニティ ストリングであり、`ieee` が IEEE802dot11 MIB オブジェクトのクエリに対するコミュニティ ストリングであることを指定する方法を示します。

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

次に、任意の SNMP マネージャがコミュニティ ストリング *public* を使用して、読み取り専用権限ですべてのオブジェクトにアクセスする例を示します。また、アクセス ポイントは SNMPv1 を使用してホスト 192.180.1.111 と 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に設定トラップを送信します。コミュニティ ストリング *public* は、トラップとともに送信されます。

```
AP(config)# snmp-server community public
AP(config)# snmp-server enable traps config
AP(config)# snmp-server host 192.180.1.27 version 2c public
AP(config)# snmp-server host 192.180.1.111 version 1 public
AP(config)# snmp-server host 192.180.1.33 public
```

次に、*comaccess* コミュニティ ストリングを使用するアクセス リスト 4 のメンバに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、どのオブジェクトにもアクセスできません。SNMP 認証障害トラップは、SNMPv2C がコミュニティ ストリング *public* を使用してホスト *cisco.com* に送信します。

```
AP(config)# snmp-server community comaccess ro 4
AP(config)# snmp-server enable traps snmp authentication
AP(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト *cisco.com* に送信する例を示します。コミュニティ ストリングは制限されます。最初の行で、アクセス ポイントはそれまでに有効になったトラップ以外にエンティティ MIB トラップを送信できます。2 行目はこれらのトラップの宛先を指定し、ホスト *cisco.com* に対する以前の **snmp-server host** コマンドを無効にします。

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted entity
```

次の例は、アクセス ポイントがコミュニティ ストリング *public* を使用して、ホスト *myhost.cisco.com* にすべてのトラップを送信することを有効にする方法を示します。

```
AP(config)# snmp-server enable traps
AP(config)# snmp-server host myhost.cisco.com public
```

次の例は、これらの SNMPv3 設定の方法を示しています。

- ビュー名 (*iso*)
- IP アドレス *1.4.74.10* のリモート ホストに対して自身を識別するために、このエージェントが使用する SNMP エンジン ID (*1234567890*)
- プライバシー暗号をサポートする SNMPv3 グループ (*admin*) で、このグループのユーザは全員、(*iso*) ビューで定義されているすべてのオブジェクトに対する読み取りおよび書き込みアクセスが許可されています。
- *admin* グループに属する SNMP ユーザ (*joe*) で、クエリに MD5 認証を使用し、MD5 用のパスワードに *xyz123* を使用し、DES56 データ クエリ暗号を使用し、暗号キーとして *key007* を使用します。
- *admin* グループに属する SNMP ユーザ (*fred*) で、クエリに MD5 認証を使用し、MD5 用の暗号化されたパスワードに *abc789* を使用し、DES56 データ クエリ暗号を使用し、暗号キーとして *key99* を使用します。

```
AP(config)# snmp-server view iso iso included
AP(config)# snmp-server engineID remote 1.4.74.10 1234567890
AP(config)# snmp-server group admin v3 priv
AP(config)# snmp-server group admin v3 priv read iso write iso
AP(config)# snmp-server user joe admin v3 auth md5 xyz123 priv des56 key007
AP(config)# snmp-server user fred admin v3 encrypted auth md5 abc789 priv des56 key99
```





(注) この例で最後のコマンドを入力すると、**show running-config** コマンドと **show startup-config** コマンドでは、一部の SNMP 設定だけが表示されるようになります。

## SNMP ステータスの表示

不正なコミュニティ ストリング エントリ、エラー、要求変数の数など、SNMP の入出力統計情報を表示するには、**show snmp** 特権 EXEC コマンドを使用します。この表示のフィールドについては、Release 12.3 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。





# リピータ / スタンバイ アクセス ポイント および ワークグループ ブリッジ モード の 設定

この章では、アクセス ポイントをリピータ、ホット スタンバイ ユニット、またはワークグループ ブリッジとして設定する方法について説明します。この章の内容は、次のとおりです。

- 「リピータ アクセス ポイントの概要」 (P.19-2)
- 「リピータ アクセス ポイントの設定」 (P.19-3)
- 「ホット スタンバイの概要」 (P.19-9)
- 「ホット スタンバイ アクセス ポイントの設定」 (P.19-10)
- 「ワークグループ ブリッジ モードの概要」 (P.19-14)
- 「ワークグループ ブリッジ モードの設定」 (P.19-19)
- 「Lightweight 環境でのワークグループ ブリッジの使用」 (P.19-21)

## リピータ アクセスポイントの概要

リピータ アクセスポイントは有線 LAN には接続されません。インフラストラクチャの範囲を拡大したり、無線通信を妨げる障害物を回避したりするために、有線 LAN に接続されているアクセスポイントの無線範囲内に配置されます。2.4GHz 無線または 5GHz 無線をリピータとして設定できます。2 種類の無線が設定されたアクセスポイントでは、片方の無線だけをリピータに指定でき、もう一方の無線はルート無線として設定する必要があります。

リピータは、別のリピータや、有線 LAN に接続されているアクセスポイントにパケットを送信することによって、無線ユーザと有線 LAN との間でトラフィックを転送します。データは、クライアントに最高のパフォーマンスを提供するルートを経由して送信されます。アクセスポイントのリピータとして設定した場合、アクセスポイントのイーサネットポートはトラフィックを転送しません。

複数のリピータ アクセスポイントをチェーンとして設定することもできますが、リピータチェーンの末端のクライアント デバイスのスループットは大幅に低下します。これは、それぞれのリピータが各パケットの受信と再送に同じチャネルを使用するため、チェーンに追加された各リピータのスループットが半分に減少することによります。

リピータのアクセスポイントは、最適な接続を確立しているアクセスポイントにアソシエートします。ただし、リピータがアソシエートするアクセスポイントを指定することはできません。リピータとルート アクセスポイント間に静的な特定のアソシエーションを設定すると、リピータのパフォーマンスが向上します。

リピータを設定するには、親（ルート）アクセスポイントとリピータ アクセスポイントの両方で Aironet 拡張機能を有効にする必要があります。Aironet 拡張機能はデフォルトで有効になっており、これらを使用すると、アクセスポイントで、アソシエートされている Cisco Aironet クライアント デバイスの能力がより正確に認識されるようになります。Aironet 拡張機能を無効にすると、アクセスポイントとシスコ以外のクライアント デバイス間の相互運用性が改善される場合があります。シスコ以外のクライアント デバイスでは、リピータ アクセスポイントおよびリピータがアソシエートしているルート アクセスポイントとの通信に問題が生じる場合があります。

インフラストラクチャ Service Set Identifier (SSID; サービスセット ID) はネイティブ VLAN に割り当てる必要があります。アクセスポイントまたはワイヤレスブリッジに複数の VLAN が作成されている場合、インフラストラクチャ SSID は非ネイティブ VLAN に割り当てできません。インフラストラクチャ SSID を非ネイティブ VLAN に設定すると、次のメッセージが表示されます。

```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```



(注)

アクセスポイントは、各無線インターフェイスに対して仮想インターフェイスを生成するため、リピータ アクセスポイントはルート アクセスポイントに 2 回（実際のインターフェイスに 1 回、仮想インターフェイスに 1 回）アソシエートします。

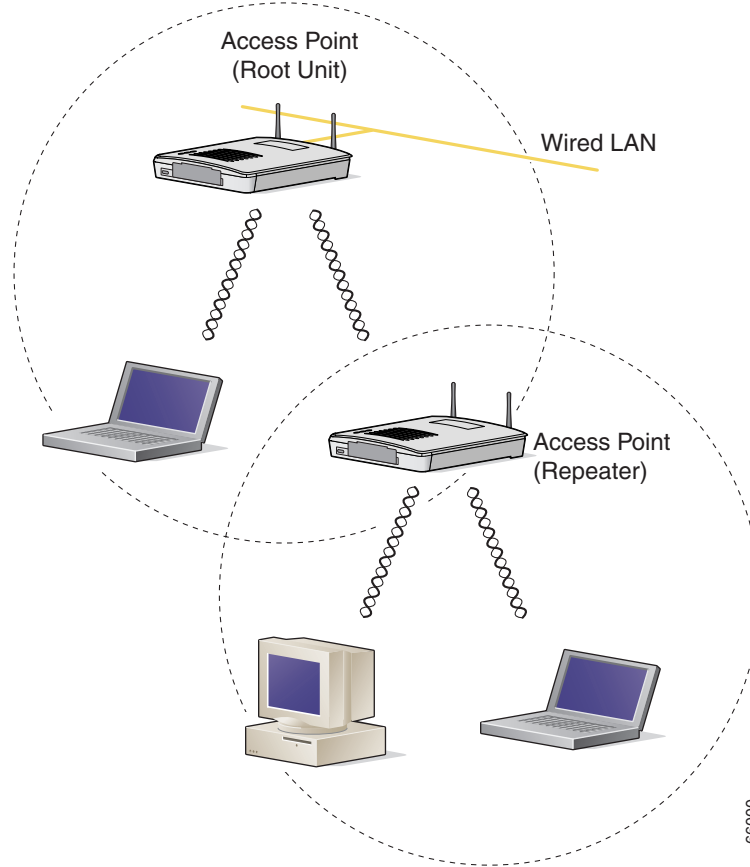


(注)

リピータ アクセスポイントには複数の VLAN を設定できません。リピータ アクセスポイントはネイティブ VLAN だけをサポートします。

図 19-1 は、リピータとして機能するアクセスポイントを示しています。

図 19-1 リピータとしてのアクセスポイント



## リピータ アクセスポイントの設定

この項では、アクセスポイントをリピータとして設定する手順について、次の項目で説明します。

- 「デフォルト設定」(P.19-4)
- 「リピータのガイドライン」(P.19-4)
- 「リピータの設定」(P.19-5)
- 「リピータ操作の確認」(P.19-7)
- 「アンテナの位置合わせ」(P.19-7)
- 「リピータの LEAP クライアントとしての設定」(P.19-7)
- 「リピータの WPA クライアントとしての設定」(P.19-9)

## デフォルト設定

アクセスポイントは、デフォルトではルートユニットとして設定されています。表 19-1 は、無線 LAN におけるアクセスポイントの役割を制御する設定のデフォルト値を示しています。

表 19-1 無線 LAN での役割のデフォルト値

機能	デフォルト設定
ステーションの役割	Root
親	none
拡張機能	Aironet

## リピータのガイドライン

リピータアクセスポイントを設定する場合は、次のガイドラインに従います。

- 高いスループットを要求しないクライアント デバイスを構成する場合は、リピータを使用します。リピータは無線 LAN のカバレッジ領域を拡大しますが、スループットを大きく減少させます。
- リピータは、それにアソシエートするクライアント デバイスのすべて、または大半が Cisco Aironet クライアントの場合に使用します。シスコ以外のクライアント デバイスを使用すると、リピータアクセスポイントとの通信に問題が生じる可能性があります。
- リピータアクセスポイントに設定されたデータレートが、親アクセスポイントのデータレートと一致しているかどうか確認してください。データレートの設定については、「無線データレートの設定」(P.6-8) を参照してください。
- リピータアクセスポイントはネイティブ VLAN だけをサポートします。リピータアクセスポイントには複数の VLAN を設定できません。



(注) Cisco IOS ソフトウェアを実行するリピータアクセスポイントは、IOS を実行しない親アクセスポイントにアソシエートできません。



(注) リピータアクセスポイントは Wireless Domain Service (WDS; 無線ドメイン サービス) をサポートしません。リピータアクセスポイントを WDS 候補として設定しないでください。また、WDS アクセスポイントを、イーサネット障害時にリピータモードに戻るよう設定しないでください。



(注) リピータの親として指定されているルートアクセスポイント上で複数の Basic Service Set Identifier (BSSID) が設定されている場合、親アクセスポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用し、無線 LAN 上のリピータが特定の親にアソシエートするように設定されている場合、親アクセスポイント上で BSSID を追加または削除するときは、リピータのアソシエーションの状態を確認します。必要に応じて、アソシエートされていないデバイスを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

## リピータの設定

特権 EXEC モードから、次の手順に従ってアクセスポイントをリピータとして設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。  5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	リピータがルート アクセスポイントにアソシエートするときに使用する SSID を作成します。次の手順で、この SSID をインフラストラクチャ SSID に指定します。ルート アクセスポイントにインフラストラクチャ SSID を作成している場合、リピータにも同じ SSID を作成します。
ステップ 4	<code>infrastructure-ssid [optional]</code>	SSID をインフラストラクチャ SSID に指定します。リピータは、この SSID を使用してルート アクセスポイントにアソシエートします。 <b>optional</b> キーワードを入力している場合を除き、インフラストラクチャ デバイスはこの SSID を使用して、リピータ アクセスポイントにアソシエートする必要があります。  インフラストラクチャ Service Set Identifier (SSID; サービスセット ID) はネイティブ VLAN に割り当てる必要があります。アクセスポイントまたはワイヤレスブリッジに複数の VLAN が作成されている場合、インフラストラクチャ SSID は非ネイティブ VLAN に割り当てできません。インフラストラクチャ SSID を非ネイティブ VLAN に設定すると、次のメッセージが表示されます。  SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
ステップ 5	<code>exit</code>	SSID コンフィギュレーション モードを終了し、無線インターフェイス コンフィギュレーション モードに戻ります。
ステップ 6	<code>station-role repeater</code>	アクセスポイントの無線 LAN での役割をリピータに設定します。
ステップ 7	<code>dot11 extension aironet</code>	Aironet 拡張機能が無効になっている場合、Aironet 拡張機能を有効にします。

## ■ リピータアクセスポイントの設定

	コマンド	目的
ステップ 8	<code>parent {1-4} mac-address [timeout]</code>	<p>(任意) リピータがアソシエートするアクセスポイントのMACアドレスを入力します。</p> <ul style="list-style-type: none"> <li>最大4つの親アクセスポイントのMACアドレスを入力できます。このポイントには、1～4の番号が指定されます。リピータは、必ずその親アクセスポイントのリストからベストなアクセスポイントにアソシエートしようとします。リピータは、「タイムアウト」オプションを設定しない限り、親リストにないMACアドレスにはアソシエートしません。</li> </ul> <p>(注) 複数のBSSIDが親アクセスポイント上で設定されている場合、親アクセスポイントでBSSIDが追加または削除されると、親MACアドレスが変更される可能性があります。</p> <ul style="list-style-type: none"> <li>(任意) タイムアウト値は秒単位で入力できますが、これはどれだけ時間、リピータがその親リストにあるアクセスポイントとアソシエートしようとするかを決めています。このタイムアウト期間内にアソシエートできない場合、リピータは親リストにないアクセスポイントにアソシエートしようとします。0～65535秒の範囲のタイムアウト値を入力できます。</li> </ul>
ステップ 9	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 10	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

3つの潜在的な親アクセスポイントをもつリピータアクセスポイントの設定例を次に示します。このアクセスポイントには、1～3の番号が指定されます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extension aironet
AP(config-if)# parent 1 0987.1234.h345
AP(config-if)# parent 2 7809.b123.c345
AP(config-if)# parent 3 6543.a456.7421
AP(config-if)# end
```

次の例は、1つの親を親リストから除く方法を示しています。この例では、親2を除いています。

```
AP(config-if)# no parent 2
```

次に、親リストに60秒のタイムアウトを設定する例を示します。

```
AP(config-if)# parent timeout 60
```

次に、親リストのタイムアウト値をディセーブルにする例を示します。

```
AP(config-if)# no parent timeout
```



## アンテナの位置合わせ

アクセスポイントをリピータとして設定するとき、**dot11 antenna-alignment** CLI コマンドを使用して、アクセスポイントのアンテナを別のリモートアンテナと位置合わせできます。

コマンドによって位置合わせテストが開始します。無線は親からのアソシエーションが解除され、隣接する無線デバイスをプローブし、受け取る応答の MAC アドレスおよび信号強度を記録します。タイムアウトの後、無線は親と再アソシエートされます。

アンテナ位置合わせテストを実行する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<b>enable</b>	特権 EXEC モードを開始します。
ステップ 2	<b>dot11 dot11radio { 0   1 }</b>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。 2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<b>antenna-alignment timeout</b>	アンテナ位置合わせテストを実行するタイムアウトまでの時間を秒数で設定します。デフォルトは 5 秒です。

**show dot11 antenna-alignment** コマンドを使用すると、プローブに最後に応答した 10 台のデバイスの MAC アドレスおよび信号レベルをリストします。

## リピータ操作の確認

リピータを設定した後、リピータアクセスポイントの上部の LED を確認します。リピータが正常に機能している場合、リピータとリピータがアソシエートするルートアクセスポイントの LED は、次のように表示されます。

- ルートアクセスポイントのステータス LED が緑色に点灯し、少なくとも 1 つのクライアントデバイスが（この場合はリピータに）アソシエートされていることを示します。
- リピータアクセスポイントのステータス LED は、リピータアクセスポイントがルートアクセスポイントにアソシエートされていて、さらにそのリピータアクセスポイントにクライアントデバイスがアソシエートされている場合、緑色に点灯します。リピータアクセスポイントがルートアクセスポイントにアソシエートされていても、クライアントデバイスがリピータアクセスポイントにアソシエートされていなければ、ステータス LED は 7/8 秒:1/8 秒の比率で点滅を繰り返します。

リピータアクセスポイントは、ルートアクセスポイントのアソシエーションテーブルにも、アソシエートされているデバイスとして表示されます。

## リピータの LEAP クライアントとしての設定

リピータアクセスポイントを、他の無線クライアントデバイスと同様に、ネットワークで認証されるよう設定できます。リピータアクセスポイントのネットワークユーザ名とパスワードを入力すると、リピータはシスコの無線認証方法である Light Extensible Authentication Protocol (LEAP; 拡張認証プロトコル) を使用してネットワークで認証され、動的な Wired Equivalent Privacy (WEP) キーを受け取ります。

リピータを LEAP クライアントとして設定する場合、次の 3 つの手順が必要です。

1. 認証サーバでリピータの認証ユーザ名とパスワードを作成します。
2. リピータがアソシエートするルート アクセス ポイントに、LEAP 認証を設定します。リピータがアソシエートするアクセス ポイントは、親アクセス ポイントと呼ばれます。認証の設定方法については、第 11 章「認証タイプの設定」を参照してください。



(注) リピータ アクセス ポイントでは、親アクセス ポイントで有効にしたものと同じ暗号スイートまたは WEP 暗号化方式と WEP 機能を有効にする必要があります。

3. LEAP クライアントとして機能するようにリピータを設定します。特権 EXEC モードから、次の手順に従ってリピータを LEAP クライアントとして設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できますが、空白を使用できません。SSID では、大文字と小文字が区別されます。
ステップ 4	<code>authentication network-eap list-name</code>	リピータで LEAP 認証を有効にして、LEAP が有効なクライアント デバイスがリピータを通じて認証されるようにします。list-name には、Extensible Authentication Protocol (EAP; 拡張認証プロトコル) 認証に使用するリスト名を指定します。EAP および MAC アドレスのリスト名は、 <b>aaa authentication login</b> コマンドを使用して定義します。これらのリストは、ユーザがログインしたときに有効となる認証方式を定義し、認証情報が保存された場所を間接的に識別します。
ステップ 5	<code>authentication client username username password password</code>	リピータが LEAP 認証を実行するときに使用するユーザ名とパスワードを設定します。このユーザ名とパスワードは、認証サーバでリピータに設定したユーザ名とパスワードに一致する必要があります。
ステップ 6	<code>infrastructure ssid [optional]</code>	(任意) SSID を、他のアクセス ポイントおよびワークグループブリッジがこのアクセス ポイントにアソシエートするために使用する SSID として指定します。SSID をインフラストラクチャ SSID として指定しない場合、インフラストラクチャ デバイスはどの SSID を使用してもアクセス ポイントにアソシエートできます。SSID をインフラストラクチャ SSID として指定する場合、 <b>optional</b> キーワードも入力する場合を除き、インフラストラクチャ デバイスはその SSID を使用してアクセス ポイントにアソシエートする必要があります。

	コマンド	目的
ステップ 7	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## リピータの WPA クライアントとしての設定

WPA キー管理では暗号化方式を組み合わせる用い、クライアント デバイスとアクセス ポイントとの通信を保護します。リピータ アクセス ポイントを、他の WPA 対応のクライアント デバイスと同様に、ネットワークで認証されるよう設定できます。

特権 EXEC モードから、次の手順に従ってリピータを WPA クライアントとして設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio { 0   1 }</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。  2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。 5GHz 無線および 5GHz 802.11n 無線は 1 です。
ステップ 3	<code>ssid ssid-string</code>	SSID を作成し、新しい SSID の SSID コンフィギュレーション モードを入力します。SSID には、最大 32 文字の英数字を使用できます。SSID では、大文字と小文字が区別されます。
ステップ 4	<code>authentication open</code>	SSID 用の open 認証を有効にします。
ステップ 5	<code>authentication key-management wpa</code>	SSID 用の WPA 認証済みキー管理を有効にします。
ステップ 6	<code>infrastructure ssid</code>	SSID を、リピータが他のアクセス ポイントにアソシエートするために使用する SSID として指定します。
ステップ 7	<code>wpa-psk { hex   ascii } [ 0   7 ] encryption-key</code>	リピータの事前共有キーを入力します。  16 進数または ASCII 文字を使用して、キーを入力します。16 進数を使用する場合は、256 ビット キーを完成するために 64 桁の 16 進数を入力する必要があります。ASCII を使用する場合は、8 ~ 63 個の ASCII 文字を入力する必要があります。アクセス ポイントがキーを展開します。
ステップ 8	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## ホットスタンバイの概要

ホットスタンバイ モードでは、アクセス ポイントが他のアクセス ポイントのバックアップとして指定されます。スタンバイ アクセス ポイントは、モニタするアクセス ポイントの近くに配置され、そのアクセス ポイントとまったく同じように設定する必要があります。スタンバイ アクセス ポイントは、モニタするアクセス ポイントにクライアントとしてアソシエートし、

イーサネットポートと無線ポートの両方からそのアクセスポイントに対して IAPP クエリを送信します。モニタするアクセスポイントから応答がない場合、スタンバイアクセスポイントはオンラインに切り替わり、そのアクセスポイントの役割をネットワーク上で引き継ぎます。

スタンバイアクセスポイントの設定は、IP アドレスを除き、モニタするアクセスポイントの設定と一致している必要があります。モニタするアクセスポイントがオフラインになり、スタンバイアクセスポイントがネットワークでその役割を引き継ぐ場合、設定のマッチングによりクライアントデバイスは簡単にスタンバイアクセスポイントに切り替わります。

スタンバイアクセスポイントは、インターフェイスとインターフェイスの関係ではなく、デバイスとデバイスの関係として、別のアクセスポイントをモニタします。たとえば、スタンバイアクセスポイントの 5GHz 無線はアクセスポイント alpha 内の 5GHz 無線をモニタするように設定し、スタンバイの 2.4GHz 無線はアクセスポイント bravo 内の 2.4GHz 無線をモニタするように設定するということはできません。また、デュアル無線のアクセスポイント内の 1 つの無線をスタンバイ無線として設定し、もう 1 つの無線をクライアントデバイスに対応するように設定することもできません。

ホットスタンバイモードはデフォルトでは、無効に設定されています。



(注) モニタするアクセスポイントに障害が発生し、スタンバイアクセスポイントがその役割を引き継いだ場合は、モニタするアクセスポイントを修復または交換する際に、スタンバイアクセスポイントのホットスタンバイを再度設定してください。スタンバイアクセスポイントは、自動的にスタンバイモードに戻りません。



(注) モニタするユニット上の BSSID が追加または削除されると、モニタするアクセスポイントの MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用する場合は、モニタするアクセスポイント上で BSSID を追加または削除するときに、スタンバイユニットの状態を確認します。必要に応じて、スタンバイユニットを再設定して、BSSID の新しい MAC アドレスを使用するようにします。



(注) ホットスタンバイは、AP モードに設定されている BR1410 ではサポートされていません。

## ホットスタンバイアクセスポイントの設定

スタンバイアクセスポイントを設定する場合、スタンバイユニットがモニタするアクセスポイントの MAC アドレスを入力する必要があります。スタンバイアクセスポイントを設定する前に、モニタするアクセスポイントの MAC アドレスを記録してください。

スタンバイアクセスポイントでは、モニタするアクセスポイントのいくつかの主要な設定を複製する必要があります。複製するのは次の設定です。

- プライマリ SSID (およびモニタするアクセスポイントに設定された追加 SSID)
- デフォルト IP サブネット マスク
- デフォルト ゲートウェイ
- データレート
- WEP 設定
- 認証タイプと認証サーバ

スタンバイアクセスポイントを設定する前に、モニタするアクセスポイントを確認し、設定を記録してください。



**(注)** スタンバイアクセスポイントにアソシエートされている無線クライアント デバイスは、ホットスタンバイを設定している間、接続が切断されます。



**ヒント** スタンバイアクセスポイント上でモニタするアクセスポイントの設定をすばやく複製するには、モニタするアクセスポイントの設定を保存して、それをスタンバイアクセスポイント上にロードします。コンフィギュレーションファイルのアップロードとダウンロードの方法については、[第 20 章「コンフィギュレーションファイルの操作」](#)を参照してください。

特権 EXEC モードから、次の手順に従ってアクセスポイントでホットスタンバイモードを有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバルコンフィギュレーションモードを開始します。
ステップ 2	<code>iapp standby mac-address</code>	<p>アクセスポイントをスタンバイモードに移行し、モニタするアクセスポイントの無線の MAC アドレスを指定します。</p> <p><b>(注)</b> 2 種類の無線を装備した 1200 シリーズアクセスポイントで 2 種類の無線を装備した 1200 シリーズアクセスポイントをモニタするように設定する場合、モニタする 2.4GHz 無線と 5GHz 無線の両方の MAC アドレスを入力する必要があります。2.4GHz 無線 MAC アドレスを最初に入力し、次に 5GHz MAC アドレスが続きます。</p> <p><b>(注)</b> モニタするユニット上の BSSID が追加または削除されると、モニタするアクセスポイントの MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用する場合は、モニタするアクセスポイント上で BSSID を追加または削除するときに、スタンバイユニットの状態を確認します。必要に応じて、スタンバイユニットを再設定して、BSSID の新しい MAC アドレスを使用するようにします。</p> <p><b>(注)</b> ホットスタンバイは、AP モードに設定されている BR1410 ではサポートされていません。</p>
ステップ 3	<code>interface dot11radio { 0   1 }</code>	<p>無線インターフェイスのインターフェイスコンフィギュレーションモードを開始します。</p> <p>2.4GHz 無線および 2.4GHz 802.11n 無線は 0 です。</p> <p>5GHz 無線および 5GHz 802.11n 無線は 1 です。</p>

	コマンド	目的
ステップ 4	<code>ssid ssid-string</code>	スタンバイアクセスポイントがモニタするアクセスポイントにアソシエートするとき使用する SSID を作成します。次の手順で、この SSID をインフラストラクチャ SSID に指定します。モニタするアクセスポイントにインフラストラクチャ SSID を作成している場合、スタンバイアクセスポイントにも同じ SSID を作成します。
ステップ 5	<code>infrastructure-ssid [optional]</code>	SSID をインフラストラクチャ SSID に指定します。スタンバイはこの SSID を使用して、モニタするアクセスポイントにアソシエートします。モニタするアクセスポイントの役割をスタンバイアクセスポイントが引き継ぐ場合、 <b>optional</b> キーワードを入力している場合を除き、インフラストラクチャ デバイスは、この SSID を使用してスタンバイアクセスポイントにアソシエートする必要があります。
ステップ 6	<code>authentication client username username password password</code>	モニタするアクセスポイントが LEAP 認証を必要とするように設定されている場合、スタンバイアクセスポイントが LEAP 認証を実行するとき使用するユーザ名とパスワードを設定します。このユーザ名とパスワードは、認証サーバでスタンバイアクセスポイントに設定したユーザ名とパスワードに一致する必要があります。
ステップ 7	<code>exit</code>	SSID コンフィギュレーション モードを終了し、無線インターフェイス コンフィギュレーション モードに戻ります。
ステップ 8	<code>iapp standby poll-frequency seconds</code>	スタンバイアクセスポイントが、モニタするアクセスポイントの無線ポートとイーサネット ポートに送信するクエリの間隔を秒数で設定します。デフォルトのポーリング周期は 2 秒です。
ステップ 9	<code>iapp standby timeout seconds</code>	スタンバイアクセスポイントが、モニタするアクセスポイントからの応答を待ち、動作不良だと判断するまでの時間を秒数で設定します。デフォルトのタイムアウト値は 20 秒です。  (注) スタンバイアクセスポイントとモニタするアクセスポイントの間のブリッジパスが 20 秒よりも長い間失われる可能性がある場合 (スパニングツリーの再計算中など)、スタンバイ タイムアウトの設定を延長する必要があります。  (注) モニタするアクセスポイントが、最も混雑の少ないチャンネルを選択するように設定されている場合、スタンバイ タイムアウトの設定の延長が必要になる場合があります。モニタするユニットが最も混雑の少ないチャンネルを選択するまで、最大で 40 秒かかる場合があります。
ステップ 10	<code>iapp standby primary-shutdown</code>	(任意) スタンバイアクセスポイントが、モニタするアクセスポイントに Dumb Device Protocol (DDP) メッセージを送信し、スタンバイユニットが有効になったときに、モニタするアクセスポイントの無線を無効にします。この機能によって、モニタするアクセスポイントにアソシエートされているクライアント デバイスが、障害の発生したユニットにアソシエートしたままになることが回避できます。

	コマンド	目的
ステップ 11	<code>show iapp standby-parms</code>	入力内容を確認します。アクセスポイントがスタンバイモードの場合、このコマンドにより、モニタするアクセスポイントの MAC アドレス、ポーリング周期、タイムアウトの値などのスタンバイパラメータが表示されます。アクセスポイントがスタンバイモード以外の場合、 <code>no iapp standby mac-address</code> が表示されます。
ステップ 12	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

スタンバイモードを有効にした後、モニタするアクセスポイントから記録した設定をスタンバイアクセスポイントの設定と一致するように変更します。

## スタンバイ操作の確認

スタンバイアクセスポイントの状態を確認する場合は、次のコマンドを使用します。

### `show iapp standby-status`

このコマンドは、スタンバイアクセスポイントのステータスを表示します。表 19-2 は、表示されるスタンバイステータスメッセージを示しています。

表 19-2 スタンバイステータスメッセージ

メッセージ	説明
IAPP Standby is Disabled	アクセスポイントがスタンバイモードに設定されていません。
IAPP—AP is in standby mode	アクセスポイントがスタンバイモードになっています。
IAPP—AP is operating in active mode	スタンバイアクセスポイントが、モニタするアクセスポイントを引き継いでおり、ルートアクセスポイントとして機能しています。
IAPP—AP is operating in repeater mode	スタンバイアクセスポイントが、モニタするアクセスポイントを引き継いでおり、リピータアクセスポイントとして機能しています。
Standby status: Initializing	スタンバイアクセスポイントが、モニタするアクセスポイントとのリンクテストを初期化しています。
Standby status: Takeover	スタンバイアクセスポイントがアクティブモードに移行しています。
Standby status: Stopped	スタンバイモードがコンフィギュレーションコマンドによって停止されました。
Standby status: Ethernet Linktest Failed	スタンバイアクセスポイントからモニタするアクセスポイントへのイーサネットリンクテストが失敗しました。
Standby status: Radio Linktest Failed	スタンバイアクセスポイントからモニタするアクセスポイントへの無線リンクテストが失敗しました。
Standby status: Standby Error	未定義のエラーが発生しました。

表 19-2 スタンバイステータス メッセージ (続き)

メッセージ	説明
Standby State: Init	スタンバイアクセスポイントが、モニタするアクセスポイントとのリンクテストを初期化しています。
Standby State: Running	スタンバイアクセスポイントがスタンバイモードで動作しており、モニタするアクセスポイントへのリンクテストを実行しています。
Standby State: Stopped	スタンバイモードがコンフィギュレーションコマンドによって停止されました。
Standby State: Not Running	アクセスポイントはスタンバイモードではありません。

スタンバイ設定を確認する場合は、次のコマンドを使用します。

#### show iapp standby-parms

このコマンドは、スタンバイアクセスポイントの MAC アドレス、スタンバイタイムアウト、ポーリング周期の値を表示します。スタンバイアクセスポイントが設定されていない場合、次のメッセージが表示されます。

```
no iapp standby mac-address
```

スタンバイアクセスポイントが、モニタするアクセスポイントを引き継ぐ場合、スタンバイアクセスポイントが引き継いだ原因を特定するために **show iapp statistics** コマンドを使用できます。

## ワークグループブリッジモードの概要

ワークグループブリッジとして、1040、1100、1130、1200、1230、1240、1250、1260、および 2600 シリーズのアクセスポイントを設定できます。ワークグループブリッジモードのアクセスポイントは、別のアクセスポイントにクライアントとしてアソシエートして、イーサネットポートに接続されたデバイスをネットワークに接続します。たとえば、ネットワークプリンタのグループを無線で接続する必要がある場合は、プリンタをハブまたはスイッチに接続し、ハブまたはスイッチをアクセスポイントのイーサネットポートに接続し、そのアクセスポイントをワークグループブリッジとして設定します。ワークグループブリッジはネットワーク上のアクセスポイントにアソシエートします。

アクセスポイントに2つの無線がある場合、ワークグループブリッジモードで、2.4GHz 無線または 5GHz 無線のいずれかが機能します。一方の無線インターフェイスをワークグループブリッジとして設定すると、他方の無線インターフェイスはアップ状態のままになります。



#### 注意

ワークグループブリッジモードのアクセスポイントでイーサネットポートを有線 LAN に接続すると、ブリッジループが発生することがあります。ネットワークのブリッジループを防止するには、ワークグループブリッジとして設定する前または設定後すぐにワークグループブリッジを有線 LAN から切断します。



  
(注)

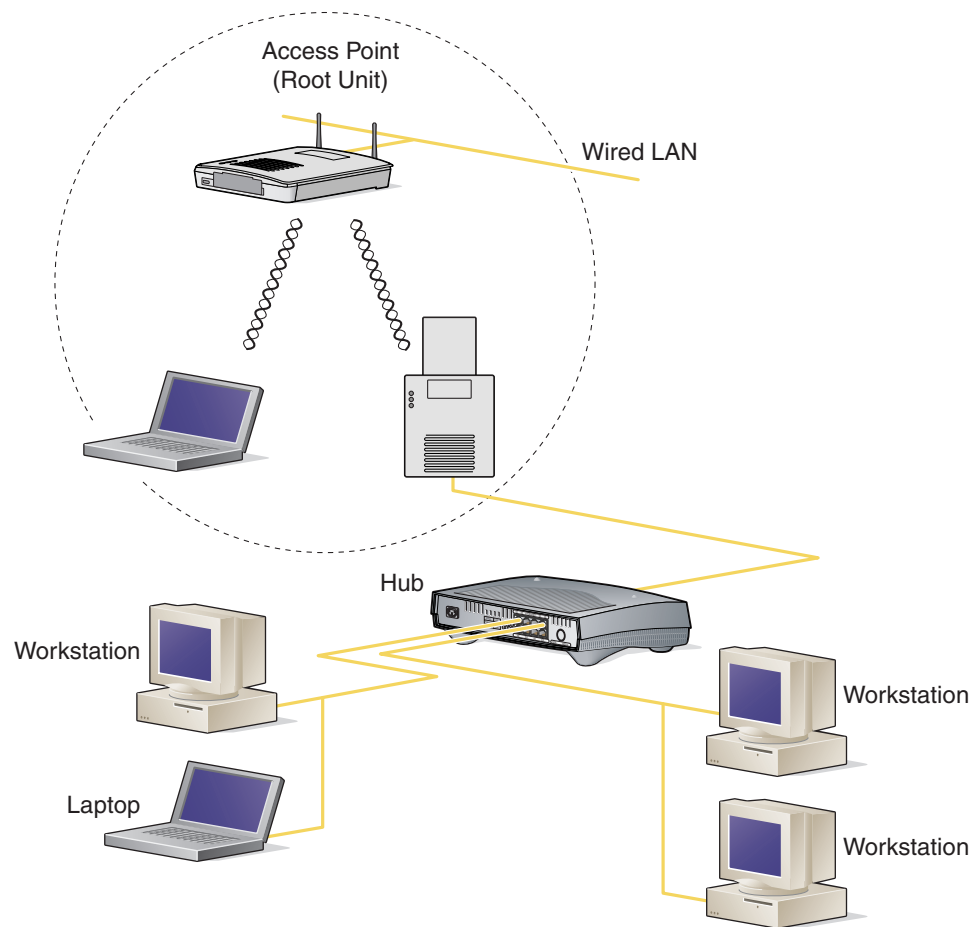
ワークグループブリッジの親として指定されているルート アクセス ポイント上で複数の BSSID が設定されている場合、親アクセスポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。無線 LAN 上で複数の BSSID を使用し、無線 LAN 上のワークグループブリッジが特定の親にアソシエートするように設定されている場合、親アクセスポイント上で BSSID を追加または削除するときは、ワークグループブリッジのアソシエーションの状態を確認します。必要に応じて、ワークグループブリッジを再設定して、BSSID の新しい MAC アドレスを使用するようにします。

  
(注)

ワークグループブリッジモードでのアクセスポイントは、ブリッジとして機能はしますが、無線範囲が限定されています。ワークグループブリッジは、数キロにわたって通信するようにワイヤレスブリッジを設定できる、**distance** 設定をサポートしていません。

図 19-2 は、ワークグループブリッジモードのアクセスポイントを示しています。

図 19-2 ワークグループブリッジモードのアクセスポイント



121646

## インフラストラクチャ デバイスまたはクライアント デバイスとしてのワークグループブリッジの扱い

ワークグループブリッジがアソシエートするアクセスポイントは、そのワークグループブリッジをインフラストラクチャ デバイスまたは単にクライアント デバイスとして扱うことができます。デフォルトでは、アクセスポイントやブリッジはワークグループブリッジをクライアント デバイスとして扱います。

信頼性を向上させるために、ワークグループブリッジをクライアント デバイスとしてではなく、アクセスポイントやブリッジと同じインフラストラクチャ デバイスとして扱うように、アクセスポイントとブリッジを設定できます。ワークグループブリッジがインフラストラクチャ デバイスとして扱われる場合、アクセスポイントはアドレス解決プロトコル (ARP) パケットなどのマルチキャスト パケットを、確実にワークグループブリッジに配信します。ワークグループブリッジをインフラストラクチャ デバイスとして扱うようにアクセスポイントとブリッジを設定するには、設定インターフェイス コマンド **infrastructure-client** を使用します。

ワークグループブリッジをクライアント デバイスとして扱うようにアクセスポイントとブリッジを設定すると、より多くのワークグループブリッジが同じアクセスポイントにアソシエートできます。つまり、より多くのワークグループブリッジが、インフラストラクチャ SSID ではない SSID を使用してアソシエートできます。信頼性の高いマルチキャスト配信のパフォーマンス コストのため (マルチキャスト パケットが各ワークグループブリッジに二重に送信されるので)、アクセスポイントまたはブリッジにアソシエートできるワークグループブリッジなどのインフラストラクチャ デバイスの数は制限されます。アクセスポイントにアソシエートできるワークグループブリッジの数を 21 以上にするには、アクセスポイントがマルチキャスト パケットをワークグループブリッジに配信するときの信頼性を低くする必要があります。信頼性が低くなると、アクセスポイントはマルチキャスト パケットが目的のワークグループブリッジに到達したかどうかを確認できなくなるため、アクセスポイントのカバレッジ領域の端にあるワークグループブリッジでは IP 接続が失われる可能性があります。ワークグループブリッジをクライアント デバイスとして扱うと、パフォーマンスは向上しますが、信頼性は低くなります。ワークグループブリッジを単なるクライアント デバイスとして扱うようにアクセスポイントとブリッジを設定するには、設定インターフェイス コマンド **no infrastructure-client** を使用します。これがデフォルト設定です。

ワークグループブリッジに接続されたデバイスが、アクセスポイントまたはブリッジと同等のネットワークに対する信頼性を必要とする場合には、ワークグループブリッジをインフラストラクチャ デバイスとして使用する必要があります。次の条件を満たす場合には、ワークグループブリッジをクライアント デバイスとして使用します。

- 同じアクセスポイントまたはブリッジに 20 台を超えるワークグループブリッジがアソシエートする。
- ワークグループブリッジがインフラストラクチャ SSID ではない SSID を使用してアソシエートする。
- ワークグループブリッジがモバイルである。

## ローミング用ワークグループブリッジの設定

ワークグループブリッジがモバイルの場合、親アクセスポイントやブリッジへのより良好な無線接続をスキャンするように設定できます。ワークグループブリッジをモバイルステーションとして設定するには、次のコマンドを使用します。

```
ap(config)# mobile station
```

この設定を有効にすると、Received Signal Strength Indicator (RSSI; 受信信号強度表示) の数値が低い、電波干渉が多い、またはフレーム損失率が高いことが検出された場合に、ワークグループブリッジは新しい親アソシエーションをスキャンします。これらの基準を使用して、モバイルステーションとして設定されたワークグループブリッジは新しい親アソシエーションを検索し、現在のアソシエーションが失われる前に新しい親にローミングします。モバイルステーションの設定が無効の場合 (デフォルトの設定)、ワークグループブリッジは現在のアソシエーションを失った後で新しいアソシエーションを検索します。

```
ap(config-if)#mobile station minimum-rate <data rate>
```

これは、WGB が新しいローミング イベントをいつ開始するかを制御するための設定可能なパラメータです。この CLI が設定され、現在のデータレートが設定値より小さい場合、新しいローミングプロセスが開始されます。これにより不要なローミングが減り、所要のレート値が得られます。

## 限定チャネル スキャン用のワークグループブリッジの設定

鉄道などのモバイル環境では、ワークグループブリッジはすべてのチャネルをスキャンする代わりに、限定チャネルのセットのみのスキャンに制限されます。こうすることで、ワークグループブリッジのローミングが1つのアクセスポイントから別のアクセスポイントに切り替わるとき、ハンドオフによる遅延が減少します。ワークグループブリッジがスキャンするチャネル数を必要な数に限定することによって、モバイルワークグループブリッジで高速かつスムーズなローミングが可能な継続的な無線 LAN 接続が実現されて維持されます。

### 限定チャネル セットの設定

この限定チャネル セットは、**mobile station scan <set of channels>** CLI コマンドを使用して設定し、すべてのチャネルまたは指定されたチャネルのスキャンを開始します。設定できるチャネルの最大数に制限はありません。設定できるチャネルの最大数は、無線がサポートできるチャネル数だけに制限されます。スキャンを実行すると、ワークグループブリッジは、この限定チャネル セットだけをスキャンします。この限定チャネル機能は、ワークグループブリッジが現在アソシエートされているアクセスポイントから受け取る既知のチャネル リストにも影響します。チャネルが既知のチャネル リストに追加されるのは、チャネルが限定チャネル セットに含まれる場合に限られます。

次の例は、コマンドを使用する方法を示しています。この例では、チャネル 1、6、および 11 がスキャンに指定されています。

```
ap#
ap#confure terminal
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
ap(config-if)#end
ap#
```

**no mobile station scan** コマンドを使用すると、すべてのチャネルのスキャンが復元されます。

## CCX ネイバー リストの無視

さらにワークグループブリッジは、AP Adjacent レポートや Enhanced Neighbor List レポートなどの CCX レポートを使用して、既知のチャンネル リストを更新します。ただし、ワークグループブリッジが限定チャンネル スキャンに設定されている場合、CCX レポートを処理して既知のチャンネル リストを更新する必要がありません。**mobile station ignore neighbor-list** コマンドを使用して、CCX 近接リスト レポートの処理を無効にします。このコマンドは、ワークグループブリッジが限定チャンネル スキャンに設定されている場合だけ有効です。次の例は、このコマンドを使用する方法を示しています。

```
ap#
ap#confure terminal
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#int d0
ap(config-if)#mobile station ignore neighbor-list
ap(config-if)#end
```

## クライアント VLAN の設定

ワークグループブリッジのイーサネット ポートに接続されたデバイスをすべて特定の VLAN に割り当てる必要がある場合、接続されたデバイスに対して VLAN を設定できます。ワークグループブリッジで、次のコマンドを入力します。

```
ap(config)# workgroup-bridge client-vlan vlan-id
```

ワークグループブリッジのイーサネット ポートに接続されたデバイスが、すべてこの VLAN に割り当てられます。

## ワークグループブリッジのVLAN タギング

ワークグループブリッジ (WGB) の VLAN タギング機能を使用すると、Unified WGB ソリューションに対する VLAN 数に基づいた VLAN トラフィックの分離がイネーブルになります。

この機能がイネーブルの場合、VLAN クライアントから無線 LAN コントローラ (WLC) へのパケットの送信中に、WGB が 802.1q ヘッダーを削除します。WGB は、802.1q ヘッダーなしで VLAN クライアントに向かうパケットを取得します。WGB の背後にあるスイッチにフレームを転送する場合は、802.1q ヘッダーを追加するように、WGB コードを変更する必要があります。

WGB は、Internet Access Point Protocol (IAPP) アソシエーション メッセージの有線クライアント VLAN 情報で WLC を更新します。WLC は WGB クライアントを VLAN クライアントとして扱い、送信元 MAC アドレスに基づき正しい VLAN インターフェイスにパケットを転送します。

アップストリーム方向では、WGB はパケットから 802.1q ヘッダーを削除すると同時にパケットを WLC に送信します。ダウンストリーム方向では、WLC は有線クライアントを接続するスイッチにパケットを転送しながら、802.1q タグなしで、そのパケットを WGB に送信します。WGB は、宛先 MAC アドレスに基づき、4 バイトの 802.1q ヘッダーを追加します。(VLAN の詳細については、第 14 章「VLAN の設定」を参照してください)。

次のコマンドを入力して、WGB の VLAN タギングを有効にします。

```
WGB(config)#workgroup-bridge unified-vlan-client ?
    -replicate  Enable WGB broadcast to all vlans
    <cr>
```

# ワークグループブリッジモードの設定

特権 EXEC モードから、次の手順に従ってアクセスポイントをワークグループブリッジとして設定します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface dot11radio {0   1}</code>	無線インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<code>station-role workgroup-bridge</code>	ワークグループブリッジに無線の役割を設定します。
ステップ 4	<code>ssid ssid-string</code>	ワークグループブリッジが親アクセスポイントまたはブリッジへのアソシエーションに使用する SSID を作成します。
ステップ 5	<code>infrastructure-ssid</code>	SSID をインフラストラクチャ SSID に指定します。  (注) ワークグループブリッジは、ルートアクセスポイントまたはブリッジにアソシエートするために、インフラストラクチャ SSID を使用する必要があります。
ステップ 6	<code>authentication client username username password password</code>	(任意) 親アクセスポイントが LEAP 認証を必要とするように設定されている場合、ワークグループブリッジが LEAP 認証を実行するときに使用するユーザ名とパスワードを設定します。このユーザ名とパスワードは、認証サーバでワークグループブリッジに設定したユーザ名とパスワードに一致する必要があります。
ステップ 7	<code>exit</code>	SSID コンフィギュレーション モードを終了し、無線インターフェイス コンフィギュレーション モードに戻ります。
ステップ 8	<code>parent {1-4} mac-address [timeout]</code>	(任意) ワークグループブリッジがアソシエートするアクセスポイントの MAC アドレスを入力します。  <ul style="list-style-type: none"> <li>最大 4 つの親アクセスポイントの MAC アドレスを入力できます。このポイントには、1 ~ 4 の番号が指定されます。ワークグループブリッジは、必ずその親アクセスポイントのリストから最適なアクセスポイントにアソシエートしようとします。ワークグループブリッジは、「タイムアウト」オプションを設定しない限り、親リストにない MAC アドレスにはアソシエートしません。</li> </ul> (注) 複数の BSSID が親アクセスポイント上で設定されている場合、親アクセスポイントで BSSID が追加または削除されると、親 MAC アドレスが変更される可能性があります。  <ul style="list-style-type: none"> <li>(任意) タイムアウト値は秒単位で入力できますが、これはどれだけの時間、ワークグループブリッジがその親リストにあるアクセスポイントとアソシエートしようとするかを決めています。このタイムアウト期間内にアソシエートできない場合、ワークグループブリッジは親リストにないアクセスポイントにアソシエートしようとします。 0 ~ 65535 秒の範囲のタイムアウト値を入力できます。</li> </ul>

## ■ ワークグループブリッジモードの設定

	コマンド	目的
ステップ 9	<b>exit</b>	無線コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 10	<b>workgroup-bridge client-vlan vlan-id</b>	(任意) ワークグループブリッジのイーサネットポートに接続されたデバイスを割り当てる VLAN を指定します。
ステップ 11	<b>mobile station</b>	(任意) ワークグループブリッジをモバイルステーションとして設定します。この設定を有効にすると、Received Signal Strength Indicator (RSSI; 受信信号強度表示) の数値が低い、電波干渉が多い、またはフレーム損失率が高いことが検出された場合に、ワークグループブリッジは新しい親アソシエーションをスキャンします。この設定が無効の場合 (デフォルトの設定)、ワークグループブリッジは現在のアソシエーションを失った後で新しいアソシエーションを検索します。
ステップ 12	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 13	<b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

次の例は、1100 シリーズのアクセスポイントをワークグループブリッジとして設定する方法を示しています。この例では、ワークグループブリッジは設定されたユーザ名とパスワードを使用して LEAP 認証を実行し、イーサネットポートに接続されたデバイスが VLAN 22 に割り当てられます。

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# station-role workgroup-bridge
AP(config-if)# ssid infra
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# authentication client username wgb1 password cisco123
AP(config-ssid)# exit
AP(config-if)# exit
AP(config)# workgroup-bridge client-vlan 22
AP(config)# end
```

次の例は、1 および 2 の番号が指定された親アクセスポイントを持つワークグループブリッジの設定方法を示しています。

```
AP(config-if)# parent 1 0040.9631.81cf
AP(config-if)# parent 2 0040.9631.81da
```

次の例は、1つの親を親リストから除く方法を示しています。この例では、親 2 を除いています。

```
AP(config-if)# no parent 2
```

次に、親リストに 60 秒のタイムアウトを設定する例を示します。

```
AP(config-if)# parent timeout 60
```

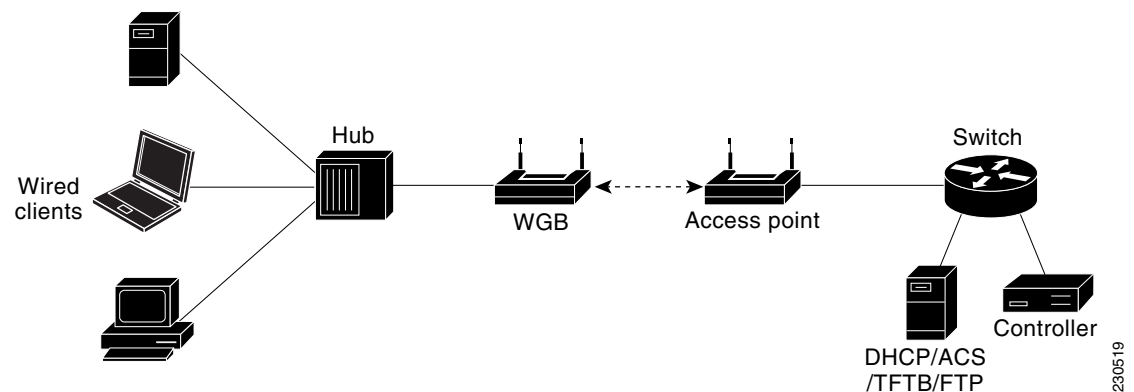
次に、親リストのタイムアウト値をディセーブルにする例を示します。

```
AP(config-if)# no parent timeout
```

## Lightweight 環境でのワークグループブリッジの使用

アクセスポイントをワークグループブリッジとして動作するように設定することで、アクセスポイントはワークグループブリッジアクセスポイントにイーサネットで接続されているクライアントの代理として Lightweight アクセスポイントへの無線接続を提供できます。ワークグループブリッジは、イーサネット インターフェイス側にある有線クライアントの MAC アドレスを学習し、Internet Access Point Protocol (IAPP; インターネット アクセスポイント プロトコル) メッセージングを使用して、MAC アドレスを Lightweight アクセスポイントに報告します。この方法によって、単一の無線セグメントを介して有線ネットワークに接続します。ワークグループブリッジは、Lightweight アクセスポイントへの単一の接続を確立することで、有線クライアントへの無線アクセス接続を提供します。Lightweight アクセスポイントはワークグループブリッジを無線クライアントとして扱います。次の例を参照してください。

図 19-3 Lightweight 環境でのワークグループブリッジ



(注) Lightweight アクセスポイントに障害が発生した場合、ワークグループブリッジは別のアクセスポイントへのアソシエートを試行します。

## ワークグループブリッジを Lightweight 環境で使用する際のガイドライン

ワークグループブリッジを Lightweight ネットワークで使用する場合は、次のガイドラインに従います。

- ワークグループブリッジは、ワークグループブリッジモードをサポートし、Cisco IOS Release JA 以降 (32MB アクセスポイント) または Cisco IOS Release 12.3(8)JEB 以降 (16MB アクセスポイント) を実行する任意の自律アクセスポイントを使用できます。これらのアクセスポイントには、AP1040、AP1121、AP1130、AP1140、AP1231、AP1240、AP1250、AP1260、および AP1310 があります。12.4(3g)JA および 12.3(8)JEB よりも前の Cisco IOS リリースはサポートされません。



(注) アクセスポイントに 2 つの無線がある場合、1 つだけをワークグループブリッジモードに設定できます。この無線は Lightweight アクセスポイントへの接続に使用されます。2 番目の無線は無効にすることをお勧めします。

ワークグループブリッジでワークグループブリッジモードを有効にするには、次のいずれかを実行します。

- ワークグループブリッジアクセスポイントの GUI の [Settings] > [Network Interfaces] ページで、無線ネットワークでの役割について [Workgroup Bridge] を選択します。
- ワークグループブリッジアクセスポイントの CLI で、コマンド **station-role workgroup-bridge** を入力します。
- ワークグループブリッジがアソシエートできるのは、Lightweight アクセスポイントだけです（サポートされていない Cisco Airespace AP1000 シリーズ アクセスポイントを除きます）。
- ワークグループブリッジはクライアントモード（デフォルト値）だけがサポートされます。インフラストラクチャモードはサポートされません。ワークグループブリッジのクライアントモードを有効にするには、次のいずれかを実行します。
  - ワークグループブリッジアクセスポイントの GUI の、ワークグループブリッジへの信頼性のあるマルチキャストのパラメータで、**Disabled** を選択します。
  - ワークグループブリッジアクセスポイントの CLI で、コマンド **no infrastructure client** を入力します。
- ワークグループブリッジでは次の Lightweight 機能の使用がサポートされています。
  - ゲスト N+1 冗長性
  - ローカル EAP
- ワークグループブリッジでは次の Lightweight 機能の使用はサポートされません。
  - Cisco Centralized Key Management (CCKM)
  - ハイブリッド REAP
  - アイドルタイムアウト
  - Web 認証



(注)

ワークグループブリッジが Web 認証 WLAN にアソシエートする場合、ワークグループブリッジは除外リストに追加され、ワークグループブリッジの有線クライアントのすべてが削除されます。

- メッシュネットワークでは、ワークグループブリッジはその役割がルートアクセスポイントかメッシュアクセスポイントかに関係なく、すべてのメッシュアクセスポイントにアソシエートできます。
- ワークグループブリッジに接続する有線クライアントは、セキュリティが認証されません。その代わりに、ワークグループブリッジがアソシエートするアクセスポイントに対してワークグループブリッジが認証されます。したがって、ワークグループブリッジの有線側は物理的に保護することを推奨します。
- レイヤ 3 ローミングで、ワークグループブリッジのローミングが別のコントローラ（外部コントローラなど）に切り替わった後にワークグループブリッジネットワークに有線クライアントを接続する場合、有線クライアントの IP アドレスはアンカーコントローラだけに表示され、外部コントローラには表示されません。
- ワークグループブリッジの記録をコントローラから削除すると、ワークグループブリッジの有線クライアントの記録もすべて削除されます。
- ワークグループブリッジに接続されている有線クライアントは、ワークグループブリッジの QoS および AAA オーバーライド属性を継承します。



- ワークグループブリッジに接続されている有線クライアントでは、次の機能がサポートされません。
  - MAC フィルタリング
  - リンク テスト
  - アイドル タイムアウト
- コントローラに何も設定しなくても、ワークグループブリッジと Lightweight アクセスポイントとの通信を有効にできます。ただし、適切な通信を確保するには、ワークグループブリッジに設定された SSID およびセキュリティ方式と一致する WLAN をコントローラに作成する必要があります。

## ワークグループブリッジの設定例

ここで、WEP キーが 40 ビットの静的 WEP を使用したワークグループブリッジアクセスポイントの設定例です。

```
ap#confure terminal
Enter configuration commands, one per line.End with CNTL/Z.
ap(config)#dot11 ssid WGB_with_static_WEP
ap(config-ssid)#authentication open
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config)#station-role workgroup-bridge
ap(config-if)#encry mode wep 40
ap(config-if)#encry key 1 size 40 0 1234567890
ap(config-if)#WGB_with_static_WEP
ap(config-if)#end
```

ワークグループブリッジがアクセスポイントにアソシエートしていることを確認するには、ワークグループブリッジで次のコマンドを入力します。

### show dot11 association

有線クライアントがトラフィックを長期間送信しない場合、トラフィックがその有線クライアントに連続して送信されている場合でも、ワークグループブリッジはそのクライアントをブリッジテーブルから削除します。その結果、有線クライアントへのトラフィックフローに障害が発生します。トラフィックの損失を避けるには、有線クライアントがブリッジテーブルから削除されないようにします。これを行うには、ワークグループブリッジで次の IOS コマンドを使用して、ワークグループブリッジのエージアウト タイマーを大きな値に設定します。

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

bridge-group-number の値は 1 ~ 255、seconds の値は 10 ~ 1,000,000 秒です。seconds パラメータを有線クライアントのアイドル時間の値よりも大きく設定することをお勧めします。

## ワークグループブリッジでの VideoStream サポートの有効化

VideoStream は、無線経路でユニキャスト フレームにマルチキャスト フレームを変換することによって、IP マルチキャスト ストリームの信頼性を向上させます。Cisco IOS Release 15.2 (2) JA 以降では、ワークグループブリッジに接続された有線デバイス向けに VideoStream サポートを提供しています。リリース 15.2 (2) JA 以降を実行しているアクセスポイントに関しては、ワークグループブリッジが無線 LAN コントローラ (WLC) のマルチキャスト テーブルに追加され、そのワークグループブリッジは VideoStream ユニキャスト フレームをイーサネット マルチキャスト フレームに変換して、それを有線クライアントに送信します。

ワークグループブリッジの VideoStream を有効にするには、WLC で次のコマンドを入力します。

```
config media-stream wired-client enable
```



## ファームウェアと設定の管理

この章では、フラッシュ ファイル システムの操作方法、コンフィギュレーション ファイルのコピー方法、およびソフトウェア イメージのアーカイブ（アップロードとダウンロード）方法について説明します。



(注)

この章で使用されるコマンドの構文と使用方法の詳細については、このリリースの『*Cisco IOS Command Reference for Access Points and Bridges*』、およびリリース 12.4 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章の内容は、次のとおりです。

- 「フラッシュ ファイル システムの操作」 (P.20-1)
- 「コンフィギュレーション ファイルの操作」 (P.20-8)
- 「ソフトウェア イメージの操作」 (P.20-20)

## フラッシュ ファイル システムの操作

アクセスポイントにあるフラッシュ ファイル システムには、ソフトウェア イメージやコンフィギュレーション ファイルを管理しやすくするためのコマンドが用意されています。

フラッシュ ファイル システムは、ファイルを保存できる単独のフラッシュ デバイスです。このフラッシュ デバイスは、*flash:* と呼ばれます。

ここでは、次の情報について説明します。

- 「使用可能なファイル システムの表示」 (P.20-2)
- 「デフォルト ファイル システムの設定」 (P.20-3)
- 「ファイル システム上のファイル情報の表示」 (P.20-3)
- 「ディレクトリの変更および作業ディレクトリの表示」 (P.20-4)
- 「ディレクトリの作成と削除」 (P.20-4)
- 「ファイルのコピー」 (P.20-5)
- 「ファイルの削除」 (P.20-5)
- 「tar ファイルの作成、表示、および抽出」 (P.20-6)
- 「ファイルの内容の表示」 (P.20-8)

## 使用可能なファイルシステムの表示

アクセス ポイントで使用可能なファイルシステムを表示する場合は、次の例に示すように、特権 EXEC コマンド **show file systems** を使用します。

```
ap# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
*    16128000     11118592     flash  rw     flash:
      16128000     11118592     unknown  rw     zflash:
           32768         26363     nvram   rw     nvram:
           -           -     network  rw     tftp:
           -           -     opaque   rw     null:
           -           -     opaque   rw     system:
           -           -     opaque   ro     xmodem:
           -           -     opaque   ro     ymodem:
           -           -     network  rw     rcp:
           -           -     network  rw     ftp:
```

表 20-1 は、**show file systems** コマンドのフィールドの詳細を示しています。

表 20-1 **show file systems** のフィールドの詳細

フィールド	値
Size(b)	ファイルシステムのメモリ サイズ (バイト単位) です。
Free(b)	ファイルシステムの空きメモリ サイズ (バイト単位) です。
Type	ファイルシステムのタイプです。 <b>flash</b> : フラッシュ メモリ デバイス用。 <b>network</b> : ネットワーク デバイス用。 <b>nvram</b> : Nonvolatile RAM (NVRAM; 不揮発性 RAM) デバイス用。 <b>opaque</b> : ファイルシステムはローカルに生成された <i>pseudo</i> ファイルシステム ( <i>system</i> など)、または <i>brimux</i> などのダウンロード インターフェイスです。 <b>unknown</b> : ファイルシステムのタイプは不明です。
Flags	ファイルシステムの権限です。 <b>ro</b> : 読み取り専用です。 <b>rw</b> : 読み取りおよび書き込みです。 <b>wo</b> : 書き込み専用です。

表 20-1 show file systems のフィールドの詳細 (続き)

フィールド	値
Prefixes	<p>ファイルシステムのエイリアスです。</p> <p><b>flash:</b> : フラッシュファイルシステムです。</p> <p><b>ftp:</b> : ファイル転送プロトコル ネットワーク サーバ。ネットワーク デバイス間のファイルの転送に使用されます。</p> <p><b>nvr:</b> : Non-volatile RAM Memory (NVRAM; 不揮発性 RAM メモリ)。</p> <p><b>null:</b> : コピーのヌル宛先です。リモート ファイルをヌルにコピーすると、サイズを確認できます。</p> <p><b>rcp:</b> : Remote Copy Protocol (RCP) ネットワーク サーバです。</p> <p><b>system:</b> : 実行コンフィギュレーションを含むシステム メモリが格納されています。</p> <p><b>tftp:</b> : Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) ネットワーク サーバ。</p> <p><b>zflash:</b> : フラッシュファイルシステムの内容をミラーリングした、読み取り専用ファイル解凍ファイルシステム。</p>

## デフォルト ファイルシステムの設定

デフォルトのファイルシステムとして使用されるファイルシステムまたはディレクトリを指定するには、**cd filesystem:** 特権 EXEC コマンドを使用します。デフォルト ファイルシステムを設定すると、関連するコマンドを実行するときに **filesystem:** 引数を省略できます。たとえば、オプションの **filesystem:** 引数を持つすべての特権 EXEC コマンドでは、**cd** コマンドで指定されたファイルシステムが使用されます。

デフォルトでは、デフォルト ファイルシステムは **flash:** です。

**cd** コマンドで指定された現在のデフォルトのファイルシステムを表示するには、**pwd** 特権 EXEC コマンドを使用します。

## ファイルシステム上のファイル情報の表示

ファイルシステムの内容を操作する前に、そのリストを表示できます。たとえば、新しいコンフィギュレーション ファイルをフラッシュ メモリにコピーする前に、ファイルシステムに同じ名前のコンフィギュレーション ファイルがまだ格納されていないことを確認できます。同様に、フラッシュ コンフィギュレーション ファイルを別の場所にコピーする前に、別のコマンドで使用するファイル名を確認できます。

ファイルシステムのファイルに関する情報を表示するには、表 20-2 に記載された特権 EXEC コマンドのいずれかを使用します。

表 20-2 ファイルに関する情報を表示するためのコマンド

コマンド	説明
<b>dir</b> [/all] [filesystem:][filename]	ファイルシステムのファイル リストを表示します。
<b>show file systems</b>	ファイルシステムのファイルごとの詳細を表示します。

表 20-2 ファイルに関する情報を表示するためのコマンド (続き)

コマンド	説明
<code>show file information file-url</code>	特定のファイルに関する情報を表示します。
<code>show file descriptors</code>	開いているファイルの記述子リストを表示します。ファイル記述子は開いているファイルの内部表現です。このコマンドを使用して、別のユーザによってファイルが開かれているかどうかを調べることができます。

## ディレクトリの変更および作業ディレクトリの表示

ディレクトリの変更や、作業ディレクトリの表示を行うには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>dir filesystem:</code>	指定されたファイル システムのディレクトリを表示します。 <code>filesystem:</code> には、システム ボードのフラッシュ デバイスの <b>flash:</b> を使用します。
ステップ 2	<code>cd new_configs</code>	目的のディレクトリに変更します。 コマンド例では、 <code>new_configs</code> という名前のディレクトリに変更する方法を示します。
ステップ 3	<code>pwd</code>	作業ディレクトリを表示します。

## ディレクトリの作成と削除

特権 EXEC モードを開始して、ディレクトリを作成および削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	<code>dir filesystem:</code>	指定されたファイル システムのディレクトリを表示します。 <code>filesystem:</code> には、システム ボードのフラッシュ デバイスの <b>flash:</b> を使用します。
ステップ 2	<code>mkdir old_configs</code>	新しいディレクトリを作成します。 コマンド例では、 <code>old_configs</code> という名前のディレクトリの作成方法を示します。 ディレクトリ名では、大文字と小文字が区別されます。 スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字です。 ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。
ステップ 3	<code>dir filesystem:</code>	設定を確認します。

ディレクトリを、その内部のすべてのファイルおよびサブディレクトリとともに削除するには、`delete /force/recursive filesystem:file-url` 特権 EXEC コマンドを使用します。

名前指定されたディレクトリを、その内部のすべてのサブディレクトリおよびファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。 **archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

**filesystem** には、システム ボードのフラッシュ デバイスの **flash:** を使用します。 **file-url** には、削除するディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。



注意

ファイルおよびディレクトリが削除された場合、その内容は回復できません。

## ファイルのコピー

ファイルをコピー元からコピー先にコピーするには、特権 EXEC コマンド **copy [/erase] source-url destination-url** を使用します。送信元および宛先の URL には、**running-config** および **startup-config** キーワード ショートカットを使用できます。たとえば、**copy running-config startup-config** コマンドは、現在実行中のコンフィギュレーション ファイルをフラッシュ メモリの NVRAM セクションに保存し、システム初期化の際にコンフィギュレーション ファイルとして使用されるようにします。

ネットワーク ファイル システムの URL には、**ftp:**、**rcp:**、および **tftp:** が含まれ、次のような構文で表されます。

- ファイル転送プロトコル (FTP) : **ftp:[[/username [:password]@location]/directory]/filename**
- リモート コピー プロトコル (RCP) : **rcp:[[/username@location]/directory]/filename**
- 簡易ファイル転送プロトコル (TFTP) : **tftp:[[/location]/directory]/filename**

ローカルにある書き込み可能なファイル システムには **flash:** があります。

送信元および宛先の組み合わせによっては、無効な場合があります。特に、次に示す組み合わせの場合は、コピーできません。

- 実行コンフィギュレーションから実行コンフィギュレーションへ
- スタートアップ コンフィギュレーションからスタートアップ コンフィギュレーションへ
- デバイスから同じ名前のデバイスへ (たとえば、**copy flash: flash:** コマンドは無効)

コンフィギュレーション ファイルによる **copy** コマンドの具体的な使用例については、「[コンフィギュレーション ファイルの操作](#)」(P.20-8) を参照してください。

新しいバージョンをダウンロードするか既存のバージョンをアップロードしてソフトウェア イメージをコピーするには、特権 EXEC コマンド **archive download-sw** または **archive upload-sw** を使用します。詳細については、「[ソフトウェア イメージの操作](#)」(P.20-20) を参照してください。

## ファイルの削除

フラッシュ メモリ デバイス上のファイルが不要になった場合、永続的に削除できます。指定したフラッシュ デバイスからファイルやディレクトリを削除するには、特権 EXEC コマンド **delete [/force] [/recursive] [filesystem:] [file-url]** を使用します。



注意

ファイルが削除された場合、その内容は回復できません。

ディレクトリを、その内部のすべてのサブディレクトリやファイルとともに削除するには、**/recursive** キーワードを使用します。ディレクトリ内のファイルごとに表示される、削除を確認するためのプロンプトを省略するには、**/force** キーワードを使用します。この削除プロセスを実行すると、最初に 1 度だけプロンプトが表示されます。**archive download-sw** コマンドでインストールされ、不要になった古いソフトウェア イメージを削除するには、**/force** キーワードおよび **/recursive** キーワードを使用します。

**filesystem:** オプションを省略した場合、アクセス ポイントは **cd** コマンドで指定されたデフォルト デバイスを使用します。**file-url** には、削除するファイルのパス (ディレクトリ) および名前を指定します。

次の例は、デフォルトのフラッシュ メモリ デバイスからファイル *myconfig* を削除する方法を示しています。

```
ap# delete myconfig
```

## tar ファイルの作成、表示、および抽出

tar ファイルを作成してそこにファイルを書き込んだり、tar ファイル内のファイルをリスト表示したり、tar ファイルからファイルを抽出したりできます (次の項を参照)。

### tar ファイルの作成

tar ファイルを作成してそこにファイルを書き込むには、次の特権 EXEC コマンドを使用します。

```
archive tar/create destination-url flash:/file-url
```

**destination-url** には、ローカルまたはネットワーク ファイル システムの宛先 URL のエイリアス、および作成する tar ファイルの名前を指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。  
**flash:/file-url**
- ファイル転送プロトコル (FTP) の場合、構文は  
**ftp:[//username[:password]@location]/directory/tar-filename.tar** です。
- リモート コピー プロトコル (RCP) の場合、構文は  
**rcp:[//username@location]/directory/tar-filename.tar** です。
- 簡易ファイル転送プロトコル (TFTP) の場合、構文は  
**tftp:[//location]/directory/tar-filename.tar** です。

**tar-filename.tar** は、作成する tar ファイルです。

**flash:/file-url** には、新しい tar ファイルの作成元になるローカル フラッシュ ファイル システム上の場所を指定します。送信元ディレクトリ内に格納されているオプションのファイルまたはディレクトリのリストを指定して、新しい tar ファイルに書き込むこともできます。何も指定しないと、このレベルのすべてのファイルおよびディレクトリが、新しく作成された tar ファイルに書き込まれます。

次の例では、tar ファイルを作成する方法を示します。このコマンドは、ローカル フラッシュ デバイスの *new-configs* ディレクトリの内容を、TFTP サーバの 172.20.10.30 にある *saved.tar* というファイルに書き込みます。

```
ap# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```



## tar ファイルの内容の表示

画面に tar ファイルの内容を表示するには、次の特権 EXEC コマンドを使用します。

### archive tar/table source-url

*source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。  
**flash:**
- ファイル転送プロトコル (FTP) の場合、構文は  
**ftp:[//[username]:password]@location/directory/tar-filename.tar** です。
- リモート コピー プロトコル (RCP) の場合、構文は  
**rcp:[//[username@location]/directory]/tar-filename.tar** です。
- 簡易ファイル転送プロトコル (TFTP) の場合、構文は  
**tftp:[//[location]/directory]/tar-filename.tar** です。

*tar-filename.tar* は、表示する tar ファイルです。

また、tar ファイルの後にファイルまたはディレクトリのオプション リストを指定すると、ファイルの表示を制限できます。リスト内のファイルだけが表示されます。何も指定しなかった場合、すべてのファイルおよびディレクトリが表示されます。

次の例は、フラッシュ メモリにある *c1200-k9w7-mx.122-8.JA.tar* ファイルの内容を表示する方法を示しています。

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
info (219 bytes)
c1200-k9w7-mx.122-8.JA/ (directory)
c1200-k9w7-mx.122-8.JA/html/ (directory)
c1200-k9w7-mx.122-8.JA/html/foo.html (0 bytes)
c1200-k9w7-mx.122-8.JA/c1200-k9w7-mx.122-8.JA.bin (610856 bytes)
c1200-k9w7-mx.122-8.JA/info (219 bytes)
info.ver (219 bytes)
```

次の例は、*c1200-k9w7-mx.122-8.JA/html* ディレクトリとその内容だけを表示する方法を示しています。

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA/html
c1200-k9w7-mx.122-8.JA/html/ (directory)
c1200-k9w7-mx.122-8.JA/html/foo.html (0 bytes)
```

## tar ファイルの抽出

フラッシュ ファイル システムのディレクトリに tar ファイルを抽出するには、次の特権 EXEC コマンドを使用します。

### archive tar /xtract source-url flash:/file-url

*source-url* には、ローカル ファイル システムまたはネットワーク ファイル システムの送信元 URL エイリアスを指定します。次のオプションがサポートされています。

- ローカル フラッシュ ファイル システムの場合の構文は次のとおりです。  
**flash:**
- ファイル転送プロトコル (FTP) の場合、構文は  
**ftp:[//[username]:password]@location/directory/tar-filename.tar** です。
- リモート コピー プロトコル (RCP) の場合、構文は  
**rcp:[//[username@location]/directory]/tar-filename.tar** です。

- 簡易ファイル転送プロトコル (TFTP) の場合、構文は `tftp:[[[location]/directory]/tar-filename.tar` です。

`tar-filename.tar` は、ファイルの抽出元の tar ファイルです。

`flash:file-url` には、tar ファイルの抽出先であるローカルフラッシュファイルシステムの場所を指定します。また、tar ファイル内の抽出するファイルまたはディレクトリのオプション リストを指定できます。何も指定されないと、すべてのファイルとディレクトリが抽出されます。

次に、172.20.10.30 の TFTP サーバ上にある tar ファイルの内容を抽出する例を示します。このコマンドは、`new-configs` ディレクトリだけをローカルフラッシュファイルシステムのルートディレクトリに抽出します。`saved.tar` ファイルの残りのファイルは無視されます。

```
ap# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

## ファイルの内容の表示

リモート ファイル システム上のファイルを含めて、読み取り可能ファイルの内容を表示するには、`more [ascii | binary | ebcdic] file-url` 特権 EXEC コマンドを使用します。

次に、TFTP サーバ上のコンフィギュレーション ファイルの内容を表示する例を示します。

```
ap# more tftp://serverA/hampton/savedconfig
!
!Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenummer
service udp-small-servers
service pt-vty-logging
!
<output truncated>
```

## コンフィギュレーション ファイルの操作

ここでは、コンフィギュレーション ファイルの作成、ロード、およびメンテナンスの手順について説明します。コンフィギュレーション ファイルには、Cisco IOS ソフトウェアの機能をカスタマイズするために入力されたコマンドが格納されています。これらのコマンドをより効果的にするために、アクセス ポイントにはシステム ソフトウェアと対話するための最小限のデフォルト実行コンフィギュレーションが含まれています。

TFTP、FTP、RCP サーバのコンフィギュレーション ファイルは、次の理由でアクセス ポイントの実行コンフィギュレーションにコピー (ダウンロード) できます。

- バックアップ コンフィギュレーション ファイルを復元するため。
- 別のアクセス ポイントのコンフィギュレーション ファイルを使用するため。たとえば、ネットワークにアクセス ポイントを追加して、そのアクセス ポイントを元のアクセス ポイントと同じように設定できます。新しいアクセス ポイントにファイルをコピーすると、ファイル全体を作り直すことなく関連する部分を変更できます。
- ネットワークにあるすべてのアクセス ポイントに同じコンフィギュレーション コマンドをロードするため。これは、すべてのアクセス ポイントを同じように設定するために行います。

TFTP、FTP、または RCP を使用して、アクセス ポイントのコンフィギュレーション ファイルをファイル サーバにコピー（アップロード）できます。内容を変更する前に、現在のコンフィギュレーション ファイルをサーバにバックアップしておく、後でサーバから元のコンフィギュレーション ファイルを復元できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。FTP と RCP が組み込まれたプロトコルであり、接続指向型の伝送制御プロトコル/インターネット プロトコル (TCP/IP) スタックを使用しているため、このような改善が可能なのです。

ここでは、次の情報について説明します。

- 「コンフィギュレーション ファイルの作成および使用上の注意事項」 (P.20-9)
- 「コンフィギュレーション ファイルのタイプおよび場所」 (P.20-10)
- 「テキスト エディタによるコンフィギュレーション ファイルの作成」 (P.20-10)
- 「TFTP によるコンフィギュレーション ファイルのコピー」 (P.20-10)
- 「FTP によるコンフィギュレーション ファイルのコピー」 (P.20-13)
- 「RCP によるコンフィギュレーション ファイルのコピー」 (P.20-16)
- 「設定情報の消去」 (P.20-19)

## コンフィギュレーション ファイルの作成および使用上の注意事項

コンフィギュレーション ファイルの作成によって、アクセス ポイントを設定できます。コンフィギュレーション ファイルには、1 つ以上のアクセス ポイントの設定に必要なコマンドの一部、またはすべてを格納できます。たとえば、同一のハードウェア構成を持つ複数のアクセス ポイントに同一のコンフィギュレーション ファイルをダウンロードできます。

コンフィギュレーション ファイルを作成するときは、次に示す注意事項に従ってください。

- アクセス ポイントにパスワードが設定されていない場合は、グローバル コンフィギュレーション コマンド **enable secret secret-password** を入力して、各アクセス ポイントにパスワードを設定する必要があります。このコマンドには空白行を入力します。パスワードは、クリア テキストとしてコンフィギュレーション ファイルに保存されます。
- パスワードがすでに存在する場合、パスワードの検証に失敗するので、ファイルにグローバル コンフィギュレーション コマンド **enable secret secret-password** を入力できません。コンフィギュレーション ファイルにパスワードを入力すると、アクセス ポイントはファイルを実行するときに誤ってコマンドとしてパスワードを実行しようとします。
- 特権 EXEC コマンド **copy {ftp: | rcp: | tftp:} system:running-config** は、コマンドラインでコマンドを入力するのと同じように、アクセス ポイントでコンフィギュレーション ファイルをロードします。アクセス ポイントは、コマンドを追加する前に既存の実行コンフィギュレーションを消去しません。コピーされたコンフィギュレーション ファイル内のコマンドによって既存のコンフィギュレーション ファイル内のコマンドが置き換えられると、既存のコマンドは消去されます。たとえば、コピーされたコンフィギュレーション ファイルに格納されている特定のコマンドの IP アドレスが、既存のコンフィギュレーションに格納されている IP アドレスと異なる場合は、コピーされたコンフィギュレーション内の IP アドレスが使用されます。ただし、既存のコンフィギュレーション内のコマンドの中には、置き換えたり無効にしたりできないものもあります。このようなコマンドがある場合は、既存のコンフィギュレーション ファイルとコピーされたコンフィギュレーション ファイルが組み合わされた（コピーされたコンフィギュレーション ファイルが優先する）コンフィギュレーション ファイルが作成されます。

コンフィギュレーション ファイルをサーバに保存されたファイルの完全なコピーに復元するには、特権 EXEC コマンド `copy {ftp:|rcp:|tftp:} nvram:startup-config` を使用して、このコンフィギュレーション ファイルをスタートアップ コンフィギュレーションに直接コピーし、アクセス ポイントをリロードします。

## コンフィギュレーション ファイルのタイプおよび場所

スタートアップ コンフィギュレーション ファイルは、ソフトウェアを設定するために、システムの起動中に使用されます。実行コンフィギュレーション ファイルには、ソフトウェアの現在の設定が格納されています。2つのコンフィギュレーション ファイルは別々の設定にできます。たとえば、一時的に設定を変更しなければならない場合があります。この場合は、実行コンフィギュレーションを変更した後、`copy running-config startup-config` 特権 EXEC コマンドによる設定の保存は行わないようにします。

実行コンフィギュレーションは DRAM に保存され、スタートアップ コンフィギュレーションはフラッシュ メモリの NVRAM セクションに保存されます。

## テキスト エディタによるコンフィギュレーション ファイルの作成

コンフィギュレーション ファイルを作成する場合は、システムが適切に応答できるように、コマンドを論理的に並べる必要があります。次に、コンフィギュレーション ファイルの作成方法の一例を示します。

- 
- ステップ 1** 既存のコンフィギュレーション ファイルをアクセス ポイントからサーバにコピーします。  
詳細については、「[TFTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.20-11)、「[FTP によるコンフィギュレーション ファイルのダウンロード](#)」(P.20-14)、または「[RCP によるコンフィギュレーション ファイルのダウンロード](#)」(P.20-17) を参照してください。
  - ステップ 2** UNIX では vi や emacs、PC ではメモ帳などのテキスト エディタでコンフィギュレーション ファイルを開きます。
  - ステップ 3** 目的のコマンドが格納されたコンフィギュレーション ファイルの一部を抽出して、新しいファイルに保存します。
  - ステップ 4** コンフィギュレーション ファイルをサーバ内の適切な場所にコピーします。たとえば、ファイルをワークステーションの TFTP ディレクトリ (UNIX ワークステーションの場合は、通常は /tftpboot) にコピーします。
  - ステップ 5** ファイルに関する権限が world-read に設定されていることを確認します。
- 

## TFTP によるコンフィギュレーション ファイルのコピー

作成したコンフィギュレーション ファイルを使用したアクセス ポイントの設定、別のアクセス ポイントまたは TFTP サーバからのダウンロードが実行できます。また、コンフィギュレーション ファイルを TFTP サーバにコピー (アップロード) して、格納できます。

ここでは、次の情報について説明します。

- 「[TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備](#)」(P.20-11)

- 「TFTP によるコンフィギュレーション ファイルのダウンロード」 (P.20-11)
- 「TFTP によるコンフィギュレーション ファイルのアップロード」 (P.20-12)

## TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

TFTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、`/etc/inetd.conf` ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

`/etc/services` ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



**(注)** `/etc/inetd.conf` および `/etc/services` ファイルを変更した後に、`inetd` デーモンを再起動する必要があります。このデーモンを再起動するには、`inetd` プロセスを終了して再起動するか、または `fastboot` コマンド (SunOS 4.x の場合) や `reboot` コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細は、ご使用のワークステーションの資料を参照してください。

- アクセス ポイントに TFTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと TFTP サーバが同じサブネット内に存在する必要があります。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするコンフィギュレーション ファイルが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 `/tftpboot`)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は `world-read` でなければなりません。
- コンフィギュレーション ファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、`touch filename` コマンドを入力します。`filename` は、サーバにアップロードするとき使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は `world-write` でなければなりません。

## TFTP によるコンフィギュレーション ファイルのダウンロード

TFTP サーバからダウンロードしたコンフィギュレーション ファイルを使用してアクセス ポイントを設定するには、次の手順に従います。

- ステップ 1** コンフィギュレーション ファイルをワークステーションの適切な TFTP ディレクトリにコピーします。
- ステップ 2** 「TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 (P.20-11) を参照して、TFTP サーバが適切に設定されていることを確認します。
- ステップ 3** Telnet セッションでアクセス ポイントにログインします。

**ステップ 4** アクセス ポイントを設定するためのコンフィギュレーション ファイルを TFTP サーバからダウンロードします。

TFTP サーバの IP アドレスまたはホスト名と、ダウンロードするファイルの名前を指定します。次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy tftp:[[//location]/directory]/filename system:running-config**
- **copy tftp:[[//location]/directory]/filename nvram:startup-config**

このコンフィギュレーション ファイルを実行すると、ダウンロードが実行され、ファイルが行単位で解析されてコマンドが実行されます。

次に、IP アドレス 172.16.2.155 上にあるファイル *tokyo-config* からソフトウェアを設定する例を示します。

```
ap# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155?[confirm] y
Booting tokyo-config from 172.16.2.155:!!![OK - 874/16000 bytes]
```

## TFTP によるコンフィギュレーション ファイルのアップロード

アクセス ポイントから TFTP サーバにコンフィギュレーション ファイルをアップロードして保存するには、次の手順に従います。

**ステップ 1** 「[TFTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備](#) (P.20-11) を参照して、TFTP サーバが適切に設定されていることを確認します。

**ステップ 2** Telnet セッションでアクセス ポイントにログインします。

**ステップ 3** アクセス ポイントの設定を、TFTP サーバにアップロードします。TFTP サーバの IP アドレスまたはホスト名と、アップロード先のファイル名を指定します。

次に示す特権 EXEC コマンドのいずれかを使用します。

- **copy system:running-config tftp:[[//location]/directory]/filename]**
- **copy nvram:startup-config tftp:[[//location]/directory]/filename]**

TFTP サーバにファイルがアップロードされます。

次の例は、コンフィギュレーション ファイルをアクセス ポイントから TFTP サーバにアップロードする方法を示しています。

```
ap# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155?[confirm] y
#
Writing tokyo-config!!![OK]
```

## FTP によるコンフィギュレーション ファイルのコピー

FTP サーバから、または FTP サーバに、コンフィギュレーション ファイルをコピーできます。FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してコンフィギュレーション ファイルをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは、次のリストで最初に有効なユーザ名を送信します。

- **copy** コマンドで指定されたユーザ名 (ユーザ名が指定されている場合)
- **ip ftp username *username*** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- Anonymous

アクセス ポイントは、次のリストで最初に有効なパスワードを送信します。

- **copy** コマンドで指定されたパスワード (パスワードが指定されている場合)
- **ip ftp password *password*** グローバル コンフィギュレーション コマンドで設定されたパスワード (このコマンドが設定されている場合)
- アクセス ポイントが作成するパスワード ***username@apname.domain***。変数 ***username*** は現在のセッションと関連付けられたユーザ名、***apname*** は設定済みホスト名、***domain*** はアクセス ポイントのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。特定のコピー操作にのみ使用するユーザ名を指定する場合は、**copy** コマンド内でユーザ名を指定します。

サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリに置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

詳細は、ご使用の FTP サーバの資料を参照してください。

ここでは、次の情報について説明します。

- 「[FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備](#)」 (P.20-13)
- 「[FTP によるコンフィギュレーション ファイルのダウンロード](#)」 (P.20-14)
- 「[FTP によるコンフィギュレーション ファイルのアップロード](#)」 (P.20-15)

## FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

FTP を使用してコンフィギュレーション ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- アクセス ポイントに FTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと FTP サーバが同じサブネット内に存在する必要があります。**ping** コマンドを使用して、FTP サーバへの接続をチェックします。



- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の FTP ユーザ名が、FTP ダウンロードで使用したいユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、ip ftp username username グローバル コンフィギュレーション コマンドを使用して、すべてのコピー処理中に使用する新しい FTP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、FTP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、copy コマンド内でユーザ名を指定します。
- FTP サーバにコンフィギュレーション ファイルをアップロードする場合、アクセス ポイントのユーザからの書き込み要求を受け付けるように FTP サーバを適切に設定しておく必要があります。

詳細は、ご使用の FTP サーバの資料を参照してください。

## FTP によるコンフィギュレーション ファイルのダウンロード

FTP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-13) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	configure terminal	アクセス ポイントでグローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ 4	ip ftp username username	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	ip ftp password password	(任意) デフォルトのパスワードを変更します。
ステップ 6	end	特権 EXEC モードに戻ります。
ステップ 7	copy ftp:[[ <i>[/username[:password]@]location[/directory]/filename</i> ]] system:running-config  または  copy ftp:[[ <i>[/username[:password]@]location[/directory]/filename</i> ]] nvram:startup-config	FTP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次の例は、コンフィギュレーション ファイル *host1-config* を IP アドレス 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからコピーし、アクセス ポイントでそのコマンドをロードして実行する方法を示しています。

```
ap# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
```



```
ap#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-conf* は、IP アドレス 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからアクセスポイントのスタートアップ コンフィギュレーションにコピーされます。

```
ap# configure terminal
ap(config)# ip ftp username netadmin1
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]?172.16.101.101
Name of configuration file[rtr2-config]?host2-conf
Configure using host2-conf from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-conf:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

## FTP によるコンフィギュレーション ファイルのアップロード

FTP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-13)を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセスポイントにログインします。
ステップ 3	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ 4	<b>ip ftp username <i>username</i></b>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	<b>ip ftp password <i>password</i></b>	(任意) デフォルトのパスワードを変更します。
ステップ 6	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>copy system:running-config ftp:[[//]<i>username</i>[:<i>password</i>]@]<i>location</i>/<i>directory</i>/<i>filename</i>]</b> または <b>copy nvram:startup-config ftp:[[//]<i>username</i>[:<i>password</i>]@]<i>location</i>/<i>directory</i>/<i>filename</i>]</b>	FTP を使用して、アクセスポイントの実行中のコンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルを指定された場所に保存します。

次の例は、実行コンフィギュレーション ファイル *ap2-conf* を、IP アドレス 172.16.101.101 のリモート ホストにある *netadmin1* ディレクトリにコピーする方法を示しています。

```
ap# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/ap2-conf
```

```
Write file ap2-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

次に、FTP を使用してスタートアップ コンフィギュレーション ファイルをサーバに格納して、ファイルをコピーする例を示します。

```
ap# configure terminal
ap(config)# ip ftp username netadmin2
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy nvram:startup-config ftp:
Remote host[?]172.16.101.101
Name of configuration file to write [ap2-config]?
Write file ap2-config on host 172.16.101.101?[confirm]
![OK]
```

## RCP によるコンフィギュレーション ファイルのコピー

Remote Copy Protocol (RCP) を使用すると、リモート ホストとアクセス ポイントの間でコンフィギュレーション ファイルを別の方式でダウンロード、アップロード、コピーできます。コネクションレス プロトコルであるユーザ データグラム プロトコル (UDP) を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の `copy` コマンドは、リモート システム上の `rsh` サーバ (またはデーモン) を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは `rsh` をサポートするサーバにアクセスするだけでかまいません (ほとんどの UNIX システムは `rsh` をサポートしています)。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。コンフィギュレーション ファイルをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは次のリストで最初に有効なユーザ名を送信します。

- `copy` コマンドで指定されたユーザ名 (ユーザ名が指定されている場合)
- `ip rcmd remote-username username` グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが設定されている場合)
- 現在の TTY (端末) プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続され、`username` コマンドによって認証されている場合、アクセス ポイント ソフトウェアは Telnet ユーザ名をリモート ユーザ名として送信します。
- アクセス ポイント ホスト名。

RCP コピー要求を正常に終了させるには、ネットワーク サーバ上にリモート ユーザ名用のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、コンフィギュレーション ファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、コンフィギュレーション ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

ここでは、次の情報について説明します。

- [「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」\(P.20-17\)](#)

- 「RCP によるコンフィギュレーション ファイルのダウンロード」 (P.20-17)
- 「RCP によるコンフィギュレーション ファイルのアップロード」 (P.20-18)

## RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備

RCP を使用してコンフィギュレーション ファイルのダウンロードまたはアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、`rsh` がサポートされていることを確認します。
- アクセス ポイントに RCP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントとサーバが同じサブネット内に存在する必要があります。`ping` コマンドを使用して、RCP サーバへの接続を確認します。
- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の RCP ユーザ名が RCP ダウンロードで使いたいユーザ名であることを確認します。`show users` 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのコピー処理中に `ip rcmd remote-username username` グローバル コンフィギュレーション コマンドを使用し、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、RCP ユーザ名を設定する必要はありません。特定のコピー操作にのみ使用するユーザ名を指定する場合は、`copy` コマンド内でユーザ名を指定します。
- RCP サーバにファイルをアップロードする場合、アクセス ポイントのユーザからの RCP 書き込み要求を受け付けるようにこのサーバを適切に設定しておく必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の `.rhosts` ファイルにエントリを追加する必要があります。たとえば、アクセス ポイントに次の設定行が設定されているとします。

```
hostname ap1
ip rcmd remote-username User0
```

アクセス ポイントの IP アドレスが `ap1.company.com` に変換された場合、RCP サーバの `User0` の `.rhosts` ファイルに次の行を追加する必要があります。

```
ap1.company.com ap1
```

詳細は、ご使用の RCP サーバの資料を参照してください。

## RCP によるコンフィギュレーション ファイルのダウンロード

RCP を使用してコンフィギュレーション ファイルをダウンロードするには、特権 EXEC モードで次の手順を実行します。

ステップ	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」 (P.20-17) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。

	コマンド	目的
ステップ 3	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです（ステップ 4 および 5 を参照）。
ステップ 4	<b>ip rcmd remote-username username</b>	(任意) リモート ユーザ名を指定します。
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>copy rcp:[[//[username@]location]/directory]/filename] system:running-config</b>  または <b>copy rcp:[[//[username@]location]/directory]/filename] nvram:startup-config</b>	RCP を使用して、コンフィギュレーション ファイルをネットワーク サーバから実行コンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルにコピーします。

次の例は、コンフィギュレーション ファイル *host1-config* を IP アドレス 172.16.101.101 のリモート サーバにある *netadmin1* ディレクトリからコピーし、アクセス ポイントでそのコマンドをロードして実行する方法を示しています。

```
ap# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

次に、*netadmin1* というリモート ユーザ名を指定する例を示します。コンフィギュレーション ファイル *host2-config* が、IP アドレスが 172.16.101.101 であるリモート サーバ上のディレクトリ *netadmin1* からスタートアップ コンフィギュレーションにコピーされます。

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin1
ap(config)# end
ap# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]?172.16.101.101
Name of configuration file[rtr2-config]?host2-config
Configure using host2-config from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

## RCP によるコンフィギュレーション ファイルのアップロード

RCP を使用してコンフィギュレーション ファイルをアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-17)を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ 4	<b>ip rcmd remote-username username</b>	(任意) リモート ユーザ名を指定します。
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>copy system:running-config rcp:[[[//[username@] location]/directory]/filename]</b>  または <b>copy nvram:startup-config rcp:[[[//[username@] location]/directory]/filename]</b>	RCP を使用して、アクセス ポイントの実行中のコンフィギュレーション ファイルまたはスタートアップ コンフィギュレーション ファイルからネットワーク サーバにコンフィギュレーション ファイルをコピーします。

次の例は、実行コンフィギュレーション ファイル *ap2-config* を、IP アドレス 172.16.101.101 のリモート ホストにある *netadmin1* ディレクトリにコピーする方法を示しています。

```
ap# copy system:running-config rcp://netadmin1@172.16.101.101/ap2-config
Write file ap-config on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

次に、スタートアップ コンフィギュレーション ファイルをサーバ上に格納する例を示します。

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin2
ap(config)# end
ap# copy nvram:startup-config rcp:
Remote host[ ]?172.16.101.101
Name of configuration file to write [ap2-config]?
Write file ap2-config on host 172.16.101.101?[confirm]
![OK]
```

## 設定情報の消去

この項では、設定情報をクリアする方法を説明します。

## 格納されたコンフィギュレーション ファイルの削除

**注意**

削除されたファイルは復元できません。

保存されたコンフィギュレーション ファイルをフラッシュ メモリから削除するには、特権 EXEC コマンド **delete flash:filename** を使用します。**file prompt** グローバル コンフィギュレーション コマンドの設定に応じて、ファイルを削除する前に確認を求めるプロンプトが表示されます。デフォルトでは、ファイルを削除するかどうか確認を求めるプロンプトが表示されません。**file prompt** コマンドの詳細は、リリース 12.4 の『Cisco IOS Command Reference』を参照してください。

## ソフトウェア イメージの操作

この項では、システム ソフトウェア、Cisco IOS ソフトウェア、無線ファームウェア、および Web 管理 HTML ファイルを含むソフトウェア イメージ ファイルのアーカイブ（ダウンロードとアップロード）の方法を説明します。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルを、TFTP、FTP、または RCP サーバからダウンロードします。バックアップ用に、アクセス ポイント イメージ ファイルを TFTP、FTP、または RCP サーバにアップロードします。アップロードしたこのイメージは、今後同じアクセス ポイントまたは同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

使用するプロトコルは、使用中のサーバのタイプに応じて異なります。FTP および RCP トランスポート メカニズムを使用すると、TFTP よりもパフォーマンスが速く、データがより確実に配信されます。FTP と RCP が組み込まれたプロトコルであり、接続指向型の伝送制御プロトコル/インターネット プロトコル (TCP/IP) スタックを使用しているため、このような改善が可能です。

ここでは、次の情報について説明します。

- 「アクセス ポイントのイメージの場所」 (P.20-21)
- 「サーバまたは Cisco.com 上のイメージの tar ファイル形式」 (P.20-21)
- 「TFTP によるイメージ ファイルのコピー」 (P.20-21)
- 「FTP によるイメージ ファイルのコピー」 (P.20-25)
- 「RCP によるイメージ ファイルのコピー」 (P.20-30)
- 「Web ブラウザ インターフェイスによるイメージのリロード」 (P.20-35)

**(注)**

ソフトウェア イメージとサポートされているアップグレード パスのリストについては、アクセス ポイントのリリース ノートを参照してください。

## アクセスポイントのイメージの場所

Cisco IOS イメージは、バージョン番号を表示したディレクトリに保存されています。サブディレクトリには、Web 管理に必要な HTML ファイルが入っています。イメージは、システムボードのフラッシュメモリ (flash:) に格納されています。

特権 EXEC コマンド **show version** を使用して、アクセスポイントで現在実行中のソフトウェアのバージョンを確認できます。System image file is... で始まる行をディスプレイで確認します。この行には、イメージが保存されているフラッシュメモリ内のディレクトリ名が表示されます。

また、特権 EXEC コマンド **dir filesystem:** を使用して、フラッシュメモリに保存したその他のソフトウェアイメージのディレクトリ名を表示することもできます。



(注) Cisco Aironet 3600 シリーズ AP の Cisco IOS release 15.2 (4) JB および 12.4 (25e) JAO 以降では、新しいイメージがシステムボードのフラッシュメモリにダウンロードされると、フラッシュメモリにあるバックアップ IOS イメージが削除されます。システムボードのフラッシュメモリサイズの合計は 31 MB であり、リカバリ イメージ、新しいイメージ、およびバックアップ イメージを格納するのに十分な領域があるため、このような設計になっています。

## サーバまたは Cisco.com 上のイメージの tar ファイル形式

サーバ上にあるソフトウェア イメージまたは Cisco.com からダウンロードされたソフトウェア イメージは、次のファイルを含む tar ファイル形式で提供されます。

- *info* ファイル  
info ファイルは、常に tar ファイルの先頭にあり、その tar ファイルに含まれるファイルの情報が入っています。
- Cisco IOS イメージ
- アクセスポイントの HTTP サーバで要求される Web 管理ファイル
- 無線ファームウェア 5000.img ファイル
- *info.ver* ファイル  
info.ver ファイルは、常に tar ファイルの末尾にあり、info ファイルと同じ情報が入っています。info.ver ファイルは tar ファイルの最後のファイルであるため、このファイルが存在すればイメージ内のすべてのファイルがダウンロードされたこととなります。



(注) tar ファイルには .tar 以外の拡張子が付いていることがあります。

## TFTP によるイメージファイルのコピー

TFTP サーバからアクセスポイント イメージをダウンロードしたり、アクセスポイントから TFTP サーバにイメージをアップロードしたりできます。

アクセスポイントソフトウェアをアップグレードするには、アクセスポイント イメージファイルをサーバからダウンロードします。現在のイメージを新しいイメージで上書きできます。

バックアップのために、アクセスポイントのイメージファイルをサーバにアップロードします。アップロードされたこのイメージは、今後同じアクセスポイントや同じ種類の別のアクセスポイントにダウンロードする際に使用できます。

ここでは、次の情報について説明します。

- 「TFTP によるイメージファイルのダウンロードまたはアップロードの準備」(P.20-22)
- 「TFTP によるイメージファイルのダウンロード」(P.20-23)
- 「TFTP によるイメージファイルのアップロード」(P.20-24)

## TFTP によるイメージファイルのダウンロードまたはアップロードの準備

TFTP を使用してイメージファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- TFTP サーバとして機能しているワークステーションが適切に設定されていることを確認します。Sun ワークステーションの場合、`/etc/inetd.conf` ファイル内に次の行が含まれていることを確認します。

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

`/etc/services` ファイルに次の行が含まれていることを確認します。

```
tftp 69/udp
```



**(注)** `/etc/inetd.conf` および `/etc/services` ファイルを変更した後に、`inetd` デーモンを再起動する必要があります。このデーモンを再起動するには、`inetd` プロセスを終了して再起動するか、または **fastboot** コマンド (SunOS 4.x の場合) や **reboot** コマンド (Solaris 2.x または SunOS 5.x の場合) を入力します。TFTP デーモンの詳細は、ご使用のワークステーションの資料を参照してください。

- アクセスポイントに TFTP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセスポイントと TFTP サーバが同じサブネット内に存在する必要があります。ping コマンドを使用して、TFTP サーバへの接続をチェックします。
- ダウンロードするイメージが TFTP サーバ上の正しいディレクトリ内にあることを確認します (UNIX ワークステーションの場合は、通常 `/tftpboot`)。
- ダウンロードを行う場合は、ファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は `world-read` でなければなりません。
- イメージファイルをアップロードする前に、TFTP サーバに空のファイルを作成する必要があります。空のファイルを作成するには、**touch filename** コマンドを入力します。`filename` は、イメージをサーバにアップロードするときに使用するファイルの名前です。
- アップロード処理中に、サーバの既存のファイル (空のファイルを作成する必要があった場合は、空のファイルを含む) を上書きする場合は、そのファイルに関する権限が正しく設定されていることを確認します。ファイルの権限は `world-write` でなければなりません。



## TFTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。



### 注意

ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

TFTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1 ~ 3 を実行します。

	コマンド	目的
ステップ 1	.	イメージをワークステーション上の適切な TFTP ディレクトリにコピーします。「 <a href="#">TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備</a> 」(P.20-22)を参照して、TFTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	<code>archive download-sw /overwrite /reload tftp:[//location]/directory/image-name</code>	<p>イメージ ファイルを TFTP サーバからアクセス ポイントにダウンロードし、現在のイメージを上書きします。</p> <ul style="list-style-type: none"> <li>• <code>/overwrite</code> オプションを指定すると、フラッシュ内のソフトウェア イメージが、ダウンロードしたイメージで上書きされます。</li> <li>• <code>/reload</code> オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。</li> <li>• <code>//location</code> には、TFTP サーバの IP アドレスを指定します。</li> <li>• <code>/directory/image-name</code> には、ディレクトリ (任意) とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> </ul>
ステップ 4	<code>archive download-sw /leave-old-sw /reload tftp:[//location]/directory/image-name</code>	<p>イメージ ファイルを TFTP サーバからアクセス ポイントにダウンロードし、現在のイメージを維持します。</p> <ul style="list-style-type: none"> <li>• <code>/leave-old-sw</code> オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。</li> <li>• <code>/reload</code> オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。</li> <li>• <code>//location</code> には、TFTP サーバの IP アドレスを指定します。</li> <li>• <code>/directory/image-name</code> には、ディレクトリ (任意) とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> </ul>



(注) ダウンロードの失敗を回避するには、**archive download-sw /safe** コマンドを使用します。このコマンドによって、まずイメージがダウンロードされ、ダウンロードが正常に終了するまで現在実行中のバージョンは削除されません。

ダウンロード アルゴリズムにより、イメージがアクセス ポイント モデルに適していること、および DRAM が十分あることが確認されます。不備があった場合はプロセスが中止され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによりフラッシュ デバイス上の既存イメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注) アクセス ポイント IOS をダウングレードする手順は IOS アップグレードを実行する手順と同じです。アクセス ポイント IOS をダウングレードするには、**archive download-sw /overwrite /reload tftp:[[/location]/directory]/image-name** と入力します。**overwrite** パラメータを指定すると、現在の IOS イメージが消去され、新しくダウングレードされたバージョンの IOS がアクセス ポイントにロードされます。**/reload** オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。



(注) フラッシュ デバイスに 2 つのイメージを保存できる容量があり、同じバージョンでこれらのイメージの 1 つを上書きする場合、**/overwrite** オプションを指定する必要があります。

**/leave-old-sw** を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に、現在稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

このアルゴリズムによって、ダウンロードされたイメージはシステム ボードのフラッシュ デバイス (**flash:**) にインストールされます。イメージは、ソフトウェア バージョンのストリングで名付けられた新しいディレクトリに保存され、新しくインストールされたイメージをポイントするように、システム ブート パス変数が更新されます。

ダウンロード プロセス中に古いイメージを保存した場合は (**/leave-old-sw** キーワードを指定した場合は)、**delete /force/recursive filesystem:/file-url** 特権 EXEC コマンドを入力して、そのイメージを削除できます。**filesystem** には、システム ボードのフラッシュ デバイスの **flash:** を使用します。**file-url** には、古いイメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

## TFTP によるイメージ ファイルのアップロード

イメージをアクセス ポイントから TFTP サーバにアップロードできます。後でこのイメージを同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードできます。



注意

ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

イメージを TFTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

コマンド	目的
ステップ 1	「TFTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-22) を参照して、TFTP サーバが適切に設定されていることを確認します。
ステップ 2	Telnet セッションでアクセス ポイントにログインします。
ステップ 3 <b>archive upload-sw</b> <b>ftftp:[[/location]/directory]/image-name.tar</b>	<p>現在実行中のアクセス ポイント イメージを TFTP サーバにアップロードします。</p> <ul style="list-style-type: none"> <li>• <i>//location</i> には、TFTP サーバの IP アドレスを指定します。</li> <li>• <i>/directory/image-name.tar</i> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。<i>image-name.tar</i> は、サーバ上に格納するソフトウェア イメージの名前です。</li> </ul>

特権 EXEC コマンド **archive upload-sw** は、info ファイル、Cisco IOS イメージ ファイル、HTML ファイル、および info.ver ファイルの順にアップロードして、サーバにイメージ ファイルを構築します。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

## FTP によるイメージ ファイルのコピー

FTP サーバからアクセス ポイント イメージをダウンロードしたり、アクセス ポイントから FTP サーバにイメージをアップロードしたりできます。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルをサーバからダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップ用に、アクセス ポイント イメージ ファイルをサーバにアップロードします。アップロードしたイメージは、今後同じアクセス ポイントまたは同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

ここでは、次の情報について説明します。

- 「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-25)
- 「FTP によるイメージ ファイルのダウンロード」(P.20-26)
- 「FTP によるイメージ ファイルのアップロード」(P.20-29)

## FTP によるイメージ ファイルのダウンロードまたはアップロードの準備

FTP サーバから、または FTP サーバに、イメージ ファイルをコピーできます。

FTP プロトコルでは、FTP 要求ごとにリモート ユーザ名およびパスワードを、クライアントがサーバに送信する必要があります。FTP を使用してイメージ ファイルをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは次のリストで最初に有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)。

- **ip ftp username *username*** グローバル コンフィギュレーション コマンドで設定されたユーザ名（このコマンドが設定されている場合）
- Anonymous

アクセス ポイントは、次のリストで最初に有効なパスワードを送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されたパスワード（パスワードが指定されている場合）
- **ip ftp password *password*** グローバル コンフィギュレーション コマンドで設定されたパスワード（このコマンドが設定されている場合）
- アクセス ポイントが作成するパスワード *username@apname.domain*。変数 *username* は現在のセッションと関連付けられたユーザ名、*apname* は設定済みホスト名、*domain* はアクセス ポイントのドメインです。

ユーザ名およびパスワードは、FTP サーバのアカウントに関連付けられている必要があります。サーバに書き込む場合は、ユーザからの FTP 書き込み要求が許可されるように FTP サーバを適切に設定する必要があります。

すべてのコピー操作に使用するユーザ名およびパスワードを指定するには、**ip ftp username** および **ip ftp password** コマンドを使用します。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。

サーバがディレクトリ構造である場合、イメージ ファイルはサーバ上のユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージ ファイルがサーバ上のユーザのホーム ディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

FTP を使用してイメージ ファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- アクセス ポイントに FTP サーバへのルートが設定されていることを確認します。サブ ネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントと FTP サーバが同じサブネット内に存在する必要があります。ping コマンドを使用して、FTP サーバへの接続を確認します。
- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の FTP ユーザ名が、FTP ダウンロードで使いたいユーザ名であることを確認します。show users 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、**ip ftp username *username*** グローバル コンフィギュレーション コマンドを使用して、新しい FTP ユーザ名を作成します。新しい名前は、すべてのアーカイブ処理中に使用されます。新しいユーザ名は NVRAM に格納されません。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、FTP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、**archive download-sw** または **archive upload-sw** 特権 EXEC コマンドでユーザ名を指定します。
- FTP サーバにイメージ ファイルをアップロードする場合、アクセス ポイントのユーザからの書き込み要求を受け付けるように FTP サーバを適切に設定しておく必要があります。

詳細は、ご使用の FTP サーバの資料を参照してください。

## FTP によるイメージ ファイルのダウンロード

新しいイメージ ファイルをダウンロードして、現在のイメージを上書きしたり、保存したりできます。

**注意**

ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

FTP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1～7 の手順を実行します。現在のイメージをそのまま維持するには、ステップ 7 をスキップします。

コマンド	目的
ステップ 1	「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-25) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2	Telnet セッションでアクセス ポイントにログインします。
ステップ 3 <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。 このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ 4 <b>ip ftp username <i>username</i></b>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5 <b>ip ftp password <i>password</i></b>	(任意) デフォルトのパスワードを変更します。
ステップ 6 <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7 <b>archive download-sw /overwrite /reload ftp:[//<i>username[:password]@location]/directory/image-name.tar</i></b>	イメージ ファイルを FTP サーバからアクセス ポイントにダウンロードし、現在のイメージを上書きします。 <ul style="list-style-type: none"> <li><b>/overwrite</b> オプションを指定すると、フラッシュ内のソフトウェア イメージが、ダウンロードしたイメージで上書きされます。</li> <li><b>/reload</b> オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。</li> <li><b>//username[:password]</b> には、ユーザ名およびパスワードを指定します。これらは FTP サーバ上のアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-25) を参照してください。</li> <li><b>@location</b> には、FTP サーバの IP アドレスを指定します。</li> <li><b>directory/image-name.tar</b> には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> </ul>

コマンド	目的
<b>ステップ 8</b> <code>archive download-sw /leave-old-sw /reload ftp:[[/username[:password]@location]/directory]/image-name.tar</code>	<p>イメージファイルをFTPサーバからアクセスポイントにダウンロードし、現在のイメージを維持します。</p> <ul style="list-style-type: none"> <li>• <code>/leave-old-sw</code> オプションを指定すると、ダウンロード後に古いソフトウェアバージョンが保存されます。</li> <li>• <code>/reload</code> オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。</li> <li>• <code>//username[:password]</code> には、ユーザ名およびパスワードを指定します。これらは、FTPサーバのアカウントに関連付けられている必要があります。詳細については、「<a href="#">FTPによるイメージファイルのダウンロードまたはアップロードの準備</a>」(P.20-25)を参照してください。</li> <li>• <code>@location</code> には、FTPサーバのIPアドレスを指定します。</li> <li>• <code>directory/image-name.tar</code> には、ディレクトリ（任意）およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> </ul>



(注) ダウンロードの失敗を回避するには、`archive download-sw /safe` コマンドを使用します。このコマンドによって、まずイメージがダウンロードされ、ダウンロードが正常に終了するまで現在実行中のバージョンは削除されません。

ダウンロード アルゴリズムにより、イメージがアクセスポイントモデルに適していること、および DRAM が十分あることが確認されます。不備があった場合はプロセスが中止され、エラーが報告されます。`/overwrite` オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによりフラッシュデバイス上の既存イメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注) フラッシュ デバイスに2つのイメージを保存できる容量があり、同じバージョンでこれらのイメージの1つを上書きする場合、`/overwrite` オプションを指定する必要があります。

`/leave-old-sw` を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分なスペースがない場合に稼働中のイメージを保存しようとする、ダウンロードプロセスが停止して、エラーメッセージが表示されます。

このアルゴリズムによって、ダウンロードされたイメージはシステムボードのフラッシュデバイス (flash:) にインストールされます。イメージは、ソフトウェアバージョンのストリングで名付けられた新しいディレクトリに保存され、新しくインストールされたイメージをポイントするように、BOOT パスリストが更新されます。ブート属性を表示するには、特権 EXEC モード コマンド `show boot` を使用し、ブート属性を変更するには、グローバル コンフィギュレーション コマンド `boot` を使用します。

ダウンロード プロセス中に古いイメージを保存した場合は (`/leave-old-sw` キーワードを指定した場合は)、`delete /force/recursive filesystem:/file-url` 特権 EXEC コマンドを入力して、そのイメージを削除できます。`filesystem` には、システムボードのフラッシュデバイスの `flash:` を使

用します。 *file-url* には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

## FTP によるイメージ ファイルのアップロード

イメージをアクセス ポイントから FTP サーバにアップロードできます。後でこのイメージを同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードできます。



### 注意

ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

アップロード機能が使用できるのは、Cluster Management Suite (CMS) と関連付けられた HTML ページが既存のイメージとともにインストールされている場合だけです。

イメージを FTP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「FTP によるコンフィギュレーション ファイルのダウンロードまたはアップロードの準備」(P.20-13) を参照して、FTP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名またはパスワードを上書きする場合のみです (ステップ 4、5、および 6 を参照)。
ステップ 4	<code>ip ftp username <i>username</i></code>	(任意) デフォルトのリモート ユーザ名を変更します。
ステップ 5	<code>ip ftp password <i>password</i></code>	(任意) デフォルトのパスワードを変更します。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>archive upload-sw ftp:[//[<i>username</i>[:<i>password</i>]]@]<i>location</i>]/<i>directory</i>]/<i>image-name.tar</i></code>	現在実行中のアクセス ポイント イメージを FTP サーバにアップロードします。  <ul style="list-style-type: none"> <li><code>//<i>username:password</i></code> には、ユーザ名およびパスワードを指定します。これらは、FTP サーバのアカウントに関連付けられている必要があります。詳細については、「FTP によるイメージ ファイルのダウンロードまたはアップロードの準備」(P.20-25) を参照してください。</li> <li><code>@<i>location</i></code> には、FTP サーバの IP アドレスを指定します。</li> <li><code>/<i>directory</i>/<i>image-name.tar</i></code> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。<code><i>image-name.tar</i></code> は、サーバ上に格納するソフトウェア イメージの名前です。</li> </ul>



**archive upload-sw** コマンドは、**info** ファイル、Cisco IOS イメージ ファイル、HTML ファイル、**info.ver** ファイルの順にアップロードして、サーバにイメージ ファイルを構築します。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって **tar** ファイル形式が作成されます。

## RCP によるイメージ ファイルのコピー

RCP サーバからアクセス ポイント イメージをダウンロードしたり、アクセス ポイントから RCP サーバにイメージをアップロードしたりできます。

アクセス ポイント ソフトウェアをアップグレードするには、アクセス ポイント イメージ ファイルをサーバからダウンロードします。現在のイメージを新しいイメージで上書きしたり、ダウンロード後に現在のファイルを保存したりできます。

バックアップ用に、アクセス ポイント イメージ ファイルをサーバにアップロードします。アップロードしたこのイメージは、今後同じアクセス ポイントまたは同じ種類の別のアクセス ポイントにダウンロードする際に使用できます。

ここでは、次の情報について説明します。

- 「RCP によるイメージ ファイルのダウンロードまたはアップロードの準備」 (P.20-30)
- 「RCP によるイメージ ファイルのダウンロード」 (P.20-31)
- 「RCP によるイメージ ファイルのアップロード」 (P.20-34)

## RCP によるイメージ ファイルのダウンロードまたはアップロードの準備

RCP によって、リモート ホストとアクセス ポイントの間でイメージ ファイルをダウンロードおよびアップロードする別の方法が提供されます。コネクションレス プロトコルであるユーザ データグラム プロトコル (UDP) を使用する TFTP と異なり、RCP ではコネクション型の TCP が使用されます。

RCP を使用してファイルをコピーする場合は、ファイルのコピー元またはコピー先のサーバで RCP がサポートされている必要があります。RCP の **copy** コマンドは、リモート システム上の **rsh** サーバ (またはデーモン) を利用します。RCP を使用してファイルをコピーする場合は、TFTP の場合のようにファイル配信用サーバを作成する必要がありません。ユーザは **rsh** をサポートするサーバにアクセスするだけでかまいません (ほとんどの UNIX システムは **rsh** をサポートしています)。ある場所から別の場所へファイルをコピーするので、コピー元ファイルに対して読み取り権限、コピー先ファイルに対して書き込み権限が必要です。コピー先ファイルが存在しない場合は、RCP によって作成されます。

RCP では、RCP 要求ごとのリモート ユーザ名をクライアントがサーバに送信する必要があります。RCP を使用してイメージをアクセス ポイントからサーバにコピーする場合、Cisco IOS ソフトウェアは次のリストで最初に有効なユーザ名を送信します。

- **archive download-sw** または **archive upload-sw** 特権 EXEC コマンドで指定されているユーザ名 (ユーザ名が指定されている場合)。
- **ip rcmd remote-username username** グローバル コンフィギュレーション コマンドで設定されたユーザ名 (このコマンドが入力されている場合)。
- 現在の TTY (端末) プロセスに関連付けられたリモート ユーザ名。たとえば、ユーザが Telnet 経由でルータに接続され、**username** コマンドによって認証されている場合、アクセス ポイント ソフトウェアは Telnet ユーザ名をリモート ユーザ名として送信します。
- アクセス ポイント ホスト名。



RCP コピー要求を正常に実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。サーバがディレクトリ構造である場合、イメージファイルはサーバ上のリモート ユーザ名に関連付けられたディレクトリに書き込まれたり、そこからコピーされたりします。たとえば、イメージファイルがサーバ上のユーザのホームディレクトリ内に置かれている場合は、ユーザの名前をリモート ユーザ名として指定します。

RCP を使用してイメージファイルのダウンロードやアップロードを開始する前に、次の作業を実行します。

- RCP サーバとして機能しているワークステーションで、`rsh` がサポートされていることを確認します。
- アクセス ポイントに RCP サーバへのルートが設定されていることを確認します。サブネット間のトラフィックをルータでルート設定していない場合は、アクセス ポイントとサーバが同じサブネット内に存在する必要があります。`ping` コマンドを使用して、RCP サーバへの接続を確認します。
- Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っていない場合は、現在の RCP ユーザ名が RCP ダウンロードで使用したいユーザ名であることを確認します。`show users` 特権 EXEC コマンドを使用して、有効なユーザ名を表示できます。このユーザ名を使用しない場合は、すべてのアーカイブ処理中に使用される `ip rcmd remote-username username` グローバル コンフィギュレーション コマンドを使用して、新しい RCP ユーザ名を作成します。新しいユーザ名は NVRAM に格納されます。Telnet セッションを使用してアクセス ポイントにアクセスしていて、有効なユーザ名を持っている場合は、このユーザ名が使用されるため、RCP ユーザ名を設定する必要はありません。この処理のためだけにユーザ名を指定する場合は、`archive download-sw` または `archive upload-sw` 特権 EXEC コマンドでユーザ名を指定します。
- RCP サーバにイメージをアップロードする場合、アクセス ポイントのユーザからの RCP 書き込み要求を受け付けるように、このサーバを設定しておく必要があります。UNIX システムの場合は、RCP サーバ上のリモート ユーザ用の `.rhosts` ファイルにエントリを追加する必要があります。たとえば、アクセス ポイントに次の設定行が設定されているとします。

```
hostname ap1
ip rcmd remote-username User0
```

アクセス ポイントの IP アドレスが `ap1.company.com` に変換された場合、RCP サーバの `User0` の `.rhosts` ファイルに次の行を追加する必要があります。

```
ap1.company.com ap1
```

詳細は、ご使用の RCP サーバの資料を参照してください。

## RCP によるイメージファイルのダウンロード

新しいイメージファイルをダウンロードして、現在のイメージを置き換えたり、保存したりできます。



### 注意

ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

RCP サーバから新しいイメージをダウンロードして、既存のイメージを上書きするには、特権 EXEC モードでステップ 1～6 の手順を実行します。現在のイメージをそのまま維持するには、ステップ 6 をスキップします。

	コマンド	目的
ステップ 1		「RCPによるイメージファイルのダウンロードまたはアップロードの準備」(P.20-30)を参照して、RCPサーバが適切に設定されていることを確認します。
ステップ 2		Telnetセッションでアクセスポイントにログインします。
ステップ 3	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ 4	<code>ip rcmd remote-username username</code>	(任意) リモート ユーザ名を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>archive download-sw /overwrite /reload rcp:[[//[username@]location]/directory]/image- name.tar]</code>	イメージファイルを RCP サーバからアクセスポイントにダウンロードし、現在のイメージを上書きします。  <ul style="list-style-type: none"> <li>• <code>/overwrite</code> オプションを指定すると、フラッシュ内のソフトウェア イメージが、ダウンロードしたイメージで上書きされます。</li> <li>• <code>/reload</code> オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。</li> <li>• <code>//username</code> には、ユーザ名を指定します。RCP コピー要求を正常に実行するためには、ネットワークサーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「RCPによるイメージファイルのダウンロードまたはアップロードの準備」(P.20-30)を参照してください。</li> <li>• <code>@location</code> には、RCP サーバの IP アドレスを指定します。</li> <li>• <code>/directory/image-name.tar</code> には、ディレクトリ (任意) およびダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> </ul>

コマンド	目的
<b>ステップ 7</b> <b>archive download-sw /leave-old-sw /reload</b> <b>rcp:[[//][username@]location]/directory/image-name.tar]</b>	<p>イメージ ファイルを RCP サーバからアクセス ポイントにダウンロードし、現在のイメージを維持します。</p> <ul style="list-style-type: none"> <li>• <b>/leave-old-sw</b> オプションを指定すると、ダウンロード後に古いソフトウェア バージョンが保存されます。</li> <li>• <b>/reload</b> オプションを指定すると、設定を変更して保存していない場合を除き、イメージのダウンロード後、システムがリロードされます。</li> <li>• <b>//username</b> には、ユーザ名を指定します。RCP コピー要求を実行するためには、ネットワーク サーバ上にリモート ユーザ名のアカウントを定義する必要があります。詳細については、「<a href="#">RCP によるイメージ ファイルのダウンロードまたはアップロードの準備</a>」(P.20-30) を参照してください。</li> <li>• <b>@location</b> には、RCP サーバの IP アドレスを指定します。</li> <li>• <b>/directory/image-name.tar</b> には、ディレクトリ (任意) とダウンロードするイメージを指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> </ul>



(注) ダウンロードの失敗を回避するには、**archive download-sw /safe** コマンドを使用します。このコマンドによって、まずイメージがダウンロードされ、ダウンロードが正常に終了するまで現在実行中のバージョンは削除されません。

ダウンロード アルゴリズムにより、イメージがアクセス ポイント モデルに適していること、および DRAM が十分あることが確認されます。不備があった場合はプロセスが中止され、エラーが報告されます。**/overwrite** オプションを指定した場合、新しいイメージと同じであるかどうかにかかわらず、ダウンロード アルゴリズムによりフラッシュ デバイス上の既存イメージが削除され、新しいイメージがダウンロードされて、ソフトウェアがリロードされます。



(注) フラッシュ デバイスに 2 つのイメージを保存できる容量があり、同じバージョンでこれらのイメージの 1 つを上書きする場合、**/overwrite** オプションを指定する必要があります。

**/leave-old-sw** を指定すると、既存のファイルは削除されません。新しいイメージをインストールする十分な余裕がない場合に稼働中のイメージを保存しようとする、ダウンロード プロセスが停止して、エラー メッセージが表示されます。

このアルゴリズムによって、ダウンロードされたイメージはシステム ボードのフラッシュ デバイス (flash:) にインストールされます。このイメージはソフトウェア バージョン スtring の名前が付いた新しいディレクトリに格納されます。また、新しくインストールされたイメージを示すように、BOOT 環境変数が更新されます。

ダウンロード プロセス中に古いソフトウェアを保存した場合は (`/leave-old-sw` キーワードを指定した場合は)、`delete /force/recursive filesystem:/file-url` 特権 EXEC コマンドを入力して、そのイメージを削除できます。 `filesystem` には、システム ボードのフラッシュ デバイスの **flash:** を使用します。 `file-url` には、古いソフトウェア イメージのディレクトリ名を入力します。ディレクトリ内のすべてのファイルおよびディレクトリが削除されます。

## RCP によるイメージファイルのアップロード

イメージをアクセス ポイントから RCP サーバにアップロードできます。後でこのイメージを同じアクセス ポイントや同じ種類の別のアクセス ポイントにダウンロードできます。



**注意**

ダウンロード アルゴリズムおよびアップロード アルゴリズムを適切に動作させるために、イメージ ディレクトリの名前を変更しないでください。

アップロード機能が使用できるのは、Cluster Management Suite (CMS) と関連付けられた HTML ページが既存のイメージとともにインストールされている場合だけです。

イメージを RCP サーバにアップロードするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		「RCP によるイメージファイルのダウンロードまたはアップロードの準備」(P.20-30) を参照して、RCP サーバが適切に設定されていることを確認します。
ステップ 2		Telnet セッションでアクセス ポイントにログインします。
ステップ 3	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。  このステップが必要になるのは、デフォルトのリモート ユーザ名を上書きする場合のみです (ステップ 4 および 5 を参照)。
ステップ 4	<code>ip rcmd remote-username username</code>	(任意) リモート ユーザ名を指定します。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>archive upload-sw rcp:[[/[username@] location]/directory]/image-name.tar]</code>	現在実行中のアクセス ポイント イメージを RCP サーバにアップロードします。  <ul style="list-style-type: none"> <li>• <code>//username</code> にはユーザ名を指定します。RCP コピー要求を実行するには、ネットワーク サーバ上でリモート ユーザ名にアカウントを定義する必要があります。詳細については、「RCP によるイメージファイルのダウンロードまたはアップロードの準備」(P.20-30) を参照してください。</li> <li>• <code>@location</code> には、RCP サーバの IP アドレスを指定します。</li> <li>• <code>/directory/image-name.tar</code> には、ディレクトリ (任意) およびアップロードするソフトウェア イメージの名前を指定します。ディレクトリ名およびイメージ名では大文字と小文字が区別されます。</li> <li>• <code>image-name.tar</code> は、サーバに保存するソフトウェア イメージの名前です。</li> </ul>

特権 EXEC コマンド **archive upload-sw** は、info ファイル、Cisco IOS イメージ ファイル、HTML ファイル、および info.ver ファイルの順にアップロードして、サーバにイメージ ファイルを構築します。これらのファイルがアップロードされた後に、アップロード アルゴリズムによって tar ファイル形式が作成されます。

## Web ブラウザ インターフェイスによるイメージのリロード

アクセス ポイントのイメージ ファイルをリロードするには、Web ブラウザ インターフェイスも使用できます。Web ブラウザ インターフェイスでは、HTTP または TFTP インターフェイスを使用したイメージ ファイルのロードがサポートされています。



(注) ブラウザを使用してイメージ ファイルをリロードする場合、アクセス ポイントの設定は変更されません。

### ブラウザ HTTP インターフェイス

HTTP インターフェイスを使用すると、PC 上にあるアクセス ポイント イメージ ファイルを参照し、アクセス ポイントにイメージをダウンロードできます。HTTP インターフェイスを使用する手順は、次のとおりです。

- ステップ 1** インターネット ブラウザを開きます。Microsoft Internet Explorer (バージョン 5.x 以降) または Netscape Navigator (バージョン 4.x) を使用してください。
  - ステップ 2** ブラウザのアドレス入力用ボックスにアクセス ポイントの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。
  - ステップ 3** [User Name] フィールドにユーザ名を入力します。
  - ステップ 4** [Password] フィールドにアクセス ポイントのパスワードを入力し、Enter を押します。[Summary Status] ページが表示されます。
  - ステップ 5** [System Software] タブをクリックして、[Software Upgrade] をクリックします。[HTTP Upgrade] 画面が表示されます。
  - ステップ 6** [Browse] ボタンをクリックして、PC 内のイメージ ファイルを探します。
  - ステップ 7** [Upgrade] ボタンをクリックします。
- 詳細は、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。

### ブラウザ TFTP インターフェイス

TFTP インターフェイスを使用すると、ネットワーク デバイスの TFTP サーバを使用してアクセス ポイントのイメージ ファイルをロードできます。TFTP サーバを使用する手順は、次のとおりです。

- ステップ 1** インターネット ブラウザを開きます。Microsoft Internet Explorer (バージョン 5.x 以降) または Netscape Navigator (バージョン 4.x) を使用してください。
- ステップ 2** ブラウザのアドレス入力用ボックスにアクセス ポイントの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

- ステップ 3** [User Name] フィールドにユーザ名を入力します。
- ステップ 4** [Password] フィールドにアクセス ポイントのパスワードを入力し、Enter を押します。  
[Summary Status] ページが表示されます。
- ステップ 5** [System Software] タブをクリックして、[Software Upgrade] をクリックします。[HTTP Upgrade] 画面が表示されます。
- ステップ 6** [TFTP Upgrade] タブをクリックします。
- ステップ 7** [TFTP Server] フィールドに、TFTP サーバの IP アドレスを入力します。
- ステップ 8** [Upload New System Image Tar File] フィールドに、アクセス ポイントのイメージ ファイル名を入力します。TFTP サーバのルート ディレクトリ下のサブディレクトリ内にファイルがある場合は、TFTP サーバのルート ディレクトリに対する相対パスとファイル名を指定します。ファイルが TFTP サーバのルート ディレクトリにある場合は、ファイル名だけを入力します。
- ステップ 9** [Upgrade] ボタンをクリックします。  
詳細については、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。
-



# 第 21 章

## システム メッセージ ログिंगの設定

---

この章では、アクセス ポイントにシステム メッセージ ログिंगを設定する方法について説明します。



(注)

---

この章で使用されるコマンドの構文と使用方法の詳細については、*Release 12.3* の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

---

この章の内容は、次のとおりです。

- 「システム メッセージ ログिंगの概要」 (P.21-2)
- 「システム メッセージ ログिंगの設定」 (P.21-2)
- 「ログング設定の表示」 (P.21-12)

## システム メッセージ ログイングの概要

デフォルトでは、アクセス ポイントはシステム メッセージと **debug** 特権 EXEC コマンドからの出力をログイング プロセスに送信します。ログイング プロセスはログ メッセージを各宛先（設定に応じて、ログ バッファ、端末回線、UNIX Syslog サーバなど）に配信する処理を制御します。ログイング プロセスは、コンソールにもメッセージを送信します。



(注) Syslog フォーマットは 4.3 Berkeley Standard Distribution (BSD) UNIX と互換性があります。

ログイング プロセスがディセーブルの場合、メッセージはコンソールにのみ送信されます。メッセージは生成時に送信されるため、メッセージおよびデバッグ出力にはプロンプトや他のコマンドの出力が割り込みます。メッセージがコンソールに表示されるのは、メッセージを生成したプロセスが終了してからです。

コンソールと各送信先に表示されるメッセージのタイプを制御する場合、メッセージの重大度レベルを設定できます。ログ メッセージにタイムスタンプを適用したり、syslog 送信元アドレスを設定したりすると、リアルタイムのデバッグと管理を強化できます。

ログイングされたシステム メッセージにアクセスするには、アクセス ポイントのコマンドライン インターフェイス (CLI) を使用するか、適切に設定された syslog サーバに保存します。アクセス ポイントのソフトウェアは、syslog メッセージを内部バッファに保存します。Telnet を通じてアクセス ポイントにアクセスしたり、syslog サーバでログを表示したりすることでシステム メッセージをリモートにモニタできます。

## システム メッセージ ログイングの設定

この項では、システム メッセージ ログイングを設定する方法について説明します。内容は次のとおりです。

- 「システム ログ メッセージのフォーマット」 (P.21-2)
- 「システム メッセージ ログイングのデフォルト設定」 (P.21-3)
- 「メッセージ ログイングのディセーブル化とイネーブル化」 (P.21-4)
- 「メッセージ表示宛先デバイスの設定」 (P.21-5)
- 「ログ メッセージのタイムスタンプのイネーブル化とディセーブル化」 (P.21-6)
- 「ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化」 (P.21-7)
- 「メッセージ重大度の定義」 (P.21-7)
- 「履歴テーブルおよび SNMP に送信される Syslog メッセージの制限」 (P.21-9)
- 「ログイング レート制限の設定」 (P.21-10)
- 「UNIX Syslog サーバの設定」 (P.21-10)

## システム ログ メッセージのフォーマット

システム ログ メッセージは最大 80 文字と 1 つのパーセント記号 (%) で構成され、設定されている場合にはその前に、オプションとしてシーケンス番号またはタイムスタンプ情報が付加されます。メッセージは次の形式で表示されます。

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```



パーセント記号の前のメッセージ部分は、**service sequence-numbers**、**service timestamps log datetime**、**service timestamps log datetime [localtime] [msec] [show-timezone]**、または **service timestamps log uptime** グローバル コンフィギュレーション コマンドの設定によって変わります。

表 21-1 に、Syslog メッセージの要素を示します。

表 21-1 システム ログ メッセージの要素

要素	説明
<i>seq no:</i>	<b>service sequence-numbers</b> グローバル コンフィギュレーション コマンドが設定されている場合だけ、ログ メッセージにシーケンス番号をスタンプします。 詳細については、「 <a href="#">ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化</a> 」(P.21-7) を参照してください。
<i>timestamp</i> のフォーマット： <i>mm/dd hh:mm:ss</i> または <i>hh:mm:ss</i> (短時間) または <i>d h</i> (長時間)	メッセージまたはイベントの日時です。この情報が表示されるのは、グローバル コンフィギュレーション コマンド <b>service timestamps log [datetime   log]</b> が設定されている場合だけです。 詳細については、「 <a href="#">ログ メッセージのタイムスタンプのイネーブル化とディセーブル化</a> 」(P.21-6) を参照してください。
<i>facility</i>	メッセージが参照する機能 (SNMP、SYS など) です。ファシリティはハードウェア デバイス、プロトコル、またはシステム ソフトウェアのモジュールである可能性があります。システム メッセージのソースまたは原因を表します。
<i>severity</i>	メッセージの重大度を示す 0 ~ 7 の 1 桁のコードです。重大度の詳細については、 <a href="#">表 21-3 (P.21-8)</a> を参照してください。
<i>MNEMONIC</i>	メッセージを一意に示すテキスト ストリングです。
<i>description</i>	レポートされているイベントの詳細を示すテキスト ストリングです。

次の例は、アクセス ポイントの部分的なシステム メッセージを示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channell1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

## システム メッセージ ログिंगのデフォルト設定

表 21-2 に、システム メッセージ ログिंगのデフォルト設定を示します。

表 21-2 システム メッセージ ログイングのデフォルト設定

機能	デフォルト設定
コンソールへのシステム メッセージ ログイング	イネーブル
コンソールの重大度	debugging (および数値の低いレベル。 表 21-3 (P.21-8) を参照)
ログ バッファ サイズ	4096 バイト
ログ履歴サイズ	1 メッセージ
タイムスタンプ	ディセーブル
同期ログイング	ディセーブル
ログイング サーバ	ディセーブル
Syslog サーバの IP アドレス	未設定
サーバ機能	Local7 (表 21-4 (P.21-12) を参照)
サーバの重大度	informational (および数値の低いレベル。 表 21-3 (P.21-8) を参照)

## メッセージ ログイングのディセーブル化とイネーブル化

メッセージ ログイングはデフォルトでイネーブルに設定されています。コンソール以外のいずれかの宛先にメッセージを送信する場合は、メッセージ ログイングをイネーブルにする必要があります。メッセージ ログイングがイネーブルの場合、ログ メッセージはログイングプロセスに送信されます。ログイングプロセスは、メッセージを生成元プロセスと同期しないで指定場所に記録します。

特権 EXEC モードから、次の手順に従ってメッセージ ログイングをディセーブルにします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>no logging on</code>	メッセージ ログイングをディセーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code> または <code>show logging</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ログイングプロセスを無効にすると、アクセス ポイントの速度が遅くなる場合があります。これはメッセージがコンソールに書き込まれるまで待ってからプロセスで次の動作が行われるためです。ログイングプロセスがディセーブルになると、メッセージは作成されるとすぐにコンソールに表示され、コマンド出力の途中で表示されることが多くなります。

**logging synchronous** グローバル コンフィギュレーション コマンドも、コンソールへのメッセージ表示に影響します。このコマンドをイネーブルにすると、Return を押さなければメッセージが表示されません。詳細については、「[ログメッセージのタイムスタンプのイネーブル化とディセーブル化](#)」(P.21-6) を参照してください。

メッセージロギングをディセーブルにした後に再びイネーブルにするには、**logging on** グローバル コンフィギュレーション コマンドを使用します。

## メッセージ表示宛先デバイスの設定

メッセージロギングがイネーブルの場合、コンソールだけでなく特定の場所にもメッセージを送信できます。特権 EXEC モードから、次のコマンドの1つ以上を使用してメッセージを受信する場所を指定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>logging buffered [size] [level]</b>	内部バッファへのメッセージを記録します。デフォルトのバッファサイズは 4096 です。指定できる範囲は 4096 ~ 2147483647 バイトです。レベルには emergencies 0、alerts 1、critical 2、errors 3、warnings 4、notifications 5、informational 6、debugging 7 を指定します。  (注) バッファサイズは大きくしすぎないでください。これは、アクセスポイントが他の作業の分のメモリを消費してしまうためです。アクセスポイントのプロセッサの空きメモリを表示する場合は <b>show memory</b> 特権 EXEC コマンドを使用します。ただし、この値は使用可能な最大メモリ量です。バッファサイズをこの数値に設定しないでください。
ステップ 3	<b>logging host</b>	UNIX Syslog サーバホストにメッセージを記録します。  <i>host</i> には、Syslog サーバとして使用するホストの名前または IP アドレスを指定します。  ログメッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。  Syslog サーバの設定手順については、「 <a href="#">UNIX Syslog サーバの設定</a> 」(P.21-10) を参照してください。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>terminal monitor</b>	現在のセッション中にコンソール以外の端末にメッセージをロギングします。  端末パラメータ コンフィギュレーション コマンドはローカルに設定され、セッションの終了後は無効になります。デバッグメッセージを表示する場合は、セッションごとにこのステップを実行する必要があります。
ステップ 6	<b>show running-config</b>	入力内容を確認します。
ステップ 7	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

**logging buffered** グローバル コンフィギュレーション コマンドを実行すると、ログメッセージが内部バッファにコピーされます。循環バッファであるため、バッファがいっぱいになると、古いメッセージが新しいメッセージで置き換えられます。バッファに記録されたメッセージを表示するには、**show logging** 特権 EXEC コマンドを使用します。最初に表示されるメッセージは、バッファ内で最も古いメッセージです。バッファの内容をクリアするには、**clear logging** 特権 EXEC コマンドを使用します。

コンソールへのロギングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。

## ログメッセージのタイムスタンプのイネーブル化とディセーブル化

デフォルトでは、ログメッセージにはタイムスタンプが設定されていません。

特権 EXEC モードから、次の手順に従ってログメッセージのタイムスタンプをイネーブルにします。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>service timestamps log uptime</b> または <b>service timestamps log datetime [msec] [localtime] [show-timezone]</b>	ログ タイムスタンプをイネーブルにします。 最初のコマンドにより、ログメッセージへのタイムスタンプがイネーブルになり、システムがリブートしてからの時間が表示されます。 2 番目のコマンドにより、ログメッセージへのタイムスタンプがイネーブルになります。選択したオプションに応じて、タイムスタンプに日付、時間（ローカル時間帯を基準、ミリ秒単位）、タイムゾーン名を指定できます。
ステップ 3	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b>	入力内容を確認します。
ステップ 5	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

デバッグとログメッセージの両方に対してタイムスタンプをディセーブルにするには、グローバル コンフィギュレーション コマンド **no service timestamps** を使用します。

次に、**service timestamps log datetime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

次に、**service timestamps log uptime** グローバル コンフィギュレーション コマンドをイネーブルにした場合のログ表示の一部を示します。

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

## ログ メッセージのシーケンス番号のイネーブル化およびディセーブル化

複数のログ メッセージが同じタイムスタンプを持つ可能性があるため、シーケンス番号を表示すると確実に 1 つのメッセージを参照できます。デフォルトでは、ログ メッセージにシーケンス番号は表示されません。

特権 EXEC モードから、次の手順に従ってログ メッセージのシーケンス番号をイネーブルにします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>service sequence-numbers</code>	シーケンス番号をイネーブルにします。
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	入力内容を確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

シーケンス番号をディセーブルにするには、`no service sequence-numbers` グローバル コンフィギュレーション コマンドを使用します。

次に、シーケンス番号をイネーブルにした場合のログ表示の一部を示します。

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

## メッセージ重大度の定義

選択したデバイスに表示されるメッセージを制限するには、メッセージの重大度を指定します (表 21-3 を参照)。

特権 EXEC モードから、次の手順に従ってメッセージの重大度を定義します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>logging console level</code>	コンソールに記録されるメッセージを制限します。 デフォルトで、コンソールはデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 21-3 (P.21-8) を参照)。
ステップ 3	<code>logging monitor level</code>	端末回線に記録されるメッセージを制限します。 デフォルトで、端末はデバッグ メッセージ、および数値的により低いレベルのメッセージを受信します (表 21-3 (P.21-8) を参照)。

	コマンド	目的
ステップ 4	<code>logging trap level</code>	Syslog サーバに記録されるメッセージを制限します。 デフォルトで、Syslog サーバは通知メッセージ、および数値的により低いレベルのメッセージを受信します (表 21-3 (P.21-8) を参照)。 Syslog サーバの設定手順については、「UNIX Syslog サーバの設定」(P.21-10) を参照してください。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code> または <code>show logging</code>	入力内容を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。



(注) `level` を指定すると、この数値以下のレベルのメッセージが出力先に表示されます。

コンソールへのログイングをディセーブルにするには、**no logging console** グローバル コンフィギュレーション コマンドを使用します。コンソール以外の端末へのログイングをディセーブルにするには、**no logging monitor** グローバル コンフィギュレーション コマンドを使用します。Syslog サーバへのログイングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを使用します。

表 21-3 に `level` キーワードを示します。また、対応する UNIX Syslog 定義を、重大度の最も高いものから順に示します。

表 21-3 メッセージ ログイング level キーワード

level キーワード	レベル	説明	syslog 定義
<b>emergencies</b>	0	システムが不安定	LOG_EMERG
<b>alerts</b>	1	即時処理が必要	LOG_ALERT
<b>critical</b>	2	クリティカルな状態	LOG_CRIT
<b>errors</b>	3	エラー状態	LOG_ERR
<b>warnings</b>	4	警告状態	LOG_WARNING
<b>notifications</b>	5	正常だが注意を要する状態	LOG_NOTICE
<b>informational</b>	6	情報メッセージだけ	LOG_INFO
<b>debugging</b>	7	デバッグ メッセージ	LOG_DEBUG

ソフトウェアは、これ以外の 4 つのカテゴリのメッセージを生成します。

- ソフトウェアまたはハードウェアの誤動作に関するエラー メッセージ：**warnings** ~ **emergencies** の重大度で表示されます。これらのタイプのメッセージは、アクセス ポイントの機能に影響することを意味しています。
- debug** コマンドの出力：**debugging** の重大度で表示されます。**debug** コマンドは通常は、Technical Assistance Center (TAC) だけで使用されます。

- インターフェイスのアップまたはダウン トランジション メッセージおよびシステム再起動メッセージ：**notifications** の重大度で表示されます。このメッセージは情報専用です。アクセス ポイントの機能には影響しません。
- リロード要求と低プロセス スタック メッセージ：**informational** の重大度で表示されます。このメッセージは情報専用です。アクセス ポイントの機能には影響しません。



(注) 認証要求ログ メッセージは **syslog** サーバにログングされません。この機能は Cisco Aironet アクセス ポイントでサポートされません。

## 履歴テーブルおよび SNMP に送信される Syslog メッセージの制限

グローバル コンフィギュレーション コマンド **snmp-server enable trap** を使用して、**syslog** メッセージトラップを SNMP ネットワーク管理ステーションへ送信するように設定している場合は、アクセス ポイント履歴テーブルに送信されて保存されるメッセージのレベルを変更できます。また履歴テーブルに保存されるメッセージ数も変更できます。

SNMP トラップは宛先への到達が保証されていないため、メッセージは履歴テーブルに格納されます。デフォルトでは、**Syslog** トラップがイネーブルでない場合も、重大度が **warnings** のメッセージ、および数値的により低いメッセージ（表 21-3 (P.21-8) を参照）が、履歴テーブルに 1 つ格納されます。

特権 EXEC モードから、次の手順に従ってレベルと履歴テーブルのサイズのデフォルトを変更します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>logging history level<sup>1</sup></b>	履歴ファイルに格納され、SNMP サーバに送信される Syslog メッセージのデフォルトの重大度を変更します。  <i>level</i> キーワードのリストについては、表 21-3 (P.21-8) を参照してください。  デフォルトでは、 <b>warnings</b> 、 <b>errors</b> 、 <b>critical</b> 、 <b>alerts</b> 、および <b>emergencies</b> のメッセージが送信されます。
ステップ 3	<b>logging history size number</b>	履歴テーブルに格納できる Syslog メッセージ数を指定します。  デフォルトでは 1 つのメッセージが格納されます。指定範囲は 1 ~ 500 メッセージです。
ステップ 4	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b>	入力内容を確認します。
ステップ 6	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

1. 表 21-3 に、*level* キーワードおよび重大度を示します。SNMP を使用している場合は、重大度の値が 1 だけ増えます。たとえば、**emergencies** は 0 ではなく 1 に、**critical** は 2 ではなく 3 になります。

履歴テーブルがいっぱいの場合（**logging history size** グローバル コンフィギュレーション コマンドで指定した最大メッセージ エントリ数が格納されている場合）は、新しいメッセージ エントリを格納できるように、最も古いエントリがテーブルから削除されます。

Syslog メッセージのログングをデフォルトの重大度に戻すには、**no logging history** グローバル コンフィギュレーション コマンドを使用します。履歴テーブル内のメッセージ数をデフォルト値に戻すには、**no logging history size** グローバル コンフィギュレーション コマンドを使用します。



## ログイング レート制限の設定

アクセス ポイントが 1 秒あたりにログイングするメッセージ数への制限を有効にできます。すべてのメッセージ、またはコンソールに送信されるメッセージに対して制限を有効にできます。また特定の重大度のメッセージを制限から除外することを指定できます。

特権 EXEC モードから、次の手順に従ってログイング レート制限を有効にします。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>logging rate-limit seconds</code> [all   console] [except severity]	ログイング レート制限を秒単位で有効にします。 <ul style="list-style-type: none"> <li>(任意) すべてのログイング、またはコンソールにログイングされるメッセージにのみ制限を適用します。</li> <li>(任意) 特定の重大度を制限から除外します。</li> </ul>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

レート制限を無効にするには、グローバル コンフィギュレーション コマンド `no logging rate-limit` を使用します。

## UNIX Syslog サーバの設定

次の項では、4.3 BSD UNIX サーバの syslog デーモンを設定し、UNIX システム ログイング ファシリティを定義する方法を説明します。

### UNIX Syslog デーモンへのメッセージのログイング

システム ログ メッセージを UNIX Syslog サーバに送信する前に、UNIX サーバ上で Syslog デーモンを設定する必要があります。root としてログインし、次のステップを実行します。



(注)

最新バージョンの UNIX Syslog デーモンの中には、デフォルトでネットワークからの Syslog パケットを受け入れないものがあります。ご使用のシステムがこれに該当する場合、UNIX の `man syslogd` コマンドを使用して、リモート syslog メッセージのログイングをイネーブルにするために `syslog` コマンド ラインに追加または削除する必要のあるオプションを確認してください。

ステップ 1 /etc/syslog.conf ファイルに次のような行を 1 行追加します。

```
local7.debug /usr/adm/logs/cisco.log
```

`local7` キーワードは、使用するログイング機能を指定します。機能の詳細については、表 21-4 (P.21-12) を参照してください。`debug` キーワードは、Syslog の重大度を指定します。重大度の詳細については、表 21-3 (P.21-8) を参照してください。`syslog` デーモンは、次のフィールドで指定されたファイルに、このレベルまたはより重大なレベルのメッセージを送信します。このファイルは、`syslog` デーモンに書き込み権限がある既存ファイルである必要があります。



**ステップ 2** UNIX シェル プロンプトに次のコマンドを入力して、ログ ファイルを作成します。

```
$ touch /usr/adm/log/cisco.log
$ chmod 666 /usr/adm/log/cisco.log
```

**ステップ 3** 次のコマンドを入力して、syslog デーモンが新しい変更を読み取ることを確認します。

```
$ kill -HUP `cat /etc/syslog.pid`
```

詳細については、ご使用の UNIX システムの **man syslog.conf** および **man syslogd** コマンドを参照してください。

## UNIX システム ログング機能の設定

外部デバイスにシステム ログ メッセージを送信するときに、そのメッセージを UNIX syslog ファシリティのいずれかから発信されたものとしてアクセス ポイントが特定するように設定できます。

特権 EXEC モードから、次の手順に従って UNIX システム ファシリティのメッセージ ログングを設定します。

	コマンド	目的
ステップ 1	<b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>logging host</b>	IP アドレスを入力して、UNIX Syslog サーバ ホストにメッセージを記録します。 ログ メッセージを受信する Syslog サーバのリストを作成するには、このコマンドを複数回入力します。
ステップ 3	<b>logging trap level</b>	Syslog サーバに記録されるメッセージを制限します。 デフォルトでは、Syslog サーバは通知メッセージおよびそれより下のレベルのメッセージを受信します。level キーワードについては、表 21-3 (P.21-8) を参照してください。
ステップ 4	<b>logging facility facility-type</b>	Syslog 機能を設定します。facility-type キーワードについては、表 21-4 (P.21-12) を参照してください。 デフォルトは <b>local7</b> です。
ステップ 5	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b>	入力内容を確認します。
ステップ 7	<b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

Syslog サーバを削除するには、**no logging host** グローバル コンフィギュレーション コマンドを使用して、Syslog サーバの IP アドレスを指定します。Syslog サーバへのログングをディセーブルにするには、**no logging trap** グローバル コンフィギュレーション コマンドを入力します。

表 21-4 は、Cisco IOS ソフトウェアでサポートされる 4.3 BSD UNIX システム ファシリティを示しています。これらの機能の詳細については、ご使用の UNIX オペレーティング システムの操作マニュアルを参照してください。

表 21-4 ログイング facility-type キーワード

ファシリティ タイプの キーワード	説明
auth	許可システム
cron	cron 機能
daemon	システム デーモン
kern	カーネル
local0 ~ local7	ローカルに定義されたメッ セージ
lpr	ライン プリンタ システム
mail	メール システム
news	USENET ニュース
sys9	システムで使用
sys10	システムで使用
sys11	システムで使用
sys12	システムで使用
sys13	システムで使用
sys14	システムで使用
syslog	システム ログ
user	ユーザ プロセス
uucp	UNIX から UNIX へのコピー システム

## ログイング設定の表示

現在のログイング設定とログ バッファの内容を表示する場合は、**show logging** 特権 EXEC コマンドを使用します。この表示のフィールドについては、リリース 12.2 の『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

ログイング履歴ファイルを表示するには、**show logging history** 特権 EXEC コマンドを使用します。



## トラブルシューティング

---

この章では、ワイヤレス デバイスに発生する可能性のある基本的な問題に対するトラブルシューティングの手順を説明します。トラブルシューティングの最新の詳細情報は、次の URL で、シスコの TAC Web サイト（[Top Issues]、[Wireless Technologies] の順に選択）を参照してください。

<http://www.cisco.com/tac>

この章の内容は、次のとおりです。

- 「LED インジケータ」 (P.22-2)
- 「電力チェック」 (P.22-2)
- 「低電力状態」 (P.22-2)
- 「基本設定の確認」 (P.22-3)
- 「デフォルト設定へのリセット」 (P.22-4)
- 「アクセス ポイントのイメージのリロード」 (P.22-7)
- 「1520 アクセス ポイントでのイメージの復元」 (P.22-12)

## LED インジケータ

使用しているワイヤレス デバイスが通信していない場合は、まずデバイスの LED インジケータを確認して、そのデバイスのステータスを評価します。

LED インジケータの設定は、すべての Cisco Aironet シリーズのアクセス ポイントで同じであるわけではありません。シリーズによって、アクセス ポイントには、1つのステータス LED インジケータ、または3種類のインジケータ（イーサネット LED、ステータス LED、および無線 LED）があります。LED インジケータの設定情報については、ご使用のアクセス ポイントのスタートアップガイド、またはハードウェア設置ガイド（屋外アクセス ポイント向け）を参照してください。



(注) LED の色の強さや見え方は、装置によって多少異なります。これは想定どおりのことであり、LED メーカーの仕様の正常範囲内であって、不具合ではありません。

## 電力チェック

パワー インジェクタの LED インジケータをチェックして、アクセス ポイント/ブリッジへの給電を確認できます。

- 緑色は、入力パワーがブリッジに給電されていることを示します。
- 赤色は、過電流または過電圧エラー状況を示します。パワー インジェクタの電源を抜いて、すべての同軸ケーブルで短絡がないことをチェックし、約 1 分間待機してから入力電源をパワー インジェクタに差し込み直します。これで再度 LED が赤色に変わった場合は、テクニカル サポートにお問い合わせください。



(注) パワー インジェクタが過電流または過電圧状況から回復するには、約 50 秒かかります。

LED がオフの場合は入力パワーが利用できないことを示します。電源モジュールがパワー インジェクタに接続されていること、および AC 電力が使用可能であること、または 12 ~ 40VDC 入力パワーがパワー インジェクタに接続されていることを確認してください。

## 低電力状態

アクセス ポイントには、48VDC 電源モジュールまたはインライン電源から給電できます。1040、1130、1140、1240、1250、および 1260 のアクセス ポイントは、IEEE 802.3af 電源規格、Cisco 準規格 PoE プロトコル、およびインライン電源用 Cisco Intelligent Power Management をサポートしています。

フル動作の場合、1040、1130、1140、1240、1250、および 1260 シリーズのアクセス ポイントには 12.95 W の電力が必要です。電源モジュールおよび Cisco Aironet パワー インジェクタは、フル動作に必要な電力を給電できますが、インライン電源によっては 12.95 W を給電できないものもあります。また、一部の大電力インライン電源では、すべてのポートに同時に 12.95 W の電力を供給できない場合もあります。



(注)

802.3af 準拠スイッチ（シスコ製またはシスコ以外の製品）では、フル動作に十分な電力を供給できます。

電源を投入すると、1040、1130、1140、1240、1250、および 1260 シリーズのアクセス ポイントは、低電力モードになり（いずれも無線は無効化）、Cisco IOS ソフトウェアのロードおよび実行が行われ、電力ネゴシエーションによって、十分な電力が利用できるかどうか判定されます。十分な電力がある場合は、無線がオンになります。それ以外の場合は、過電流状態が発生しないように、アクセス ポイントは無線が無効の状態では低電力モードに保持されます。低電力モードでは、アクセス ポイントのステータス LED の低電力エラー表示が有効化され、ブラウザおよびシリアル インターフェイスに低電力メッセージが表示され、イベント ログ入力が作成されます。

## 基本設定の確認

無線クライアントとの接続が失われる最も一般的な原因は、基本設定の不一致です。ワイヤレス デバイスでクライアント デバイスとの通信が行われない場合は、この項に記載された項目を確認します。

## SSID

ワイヤレス デバイスにアソシエートしようとする無線クライアントは、ワイヤレス デバイスと同じ SSID を使用する必要があります。クライアント デバイスの SSID が無線範囲のワイヤレス デバイスの SSID と一致しない場合、クライアント デバイスはアソシエートしません。

## WEP キー

データ送信に使用する WEP キーは、ワイヤレス デバイス、およびにアソシエートするすべての無線デバイスでまったく同じように設定する必要があります。たとえば、クライアント アダプタの WEP Key 3 を 0987654321 に設定し、送信キーとして選択した場合、ワイヤレス デバイスの WEP Key 3 もまったく同じ値に設定する必要があります。ただし、ワイヤレス デバイスでは、Key 3 を送信キーとして使用する必要はありません。

無線デバイスの WEP キーの設定方法については、第 10 章「暗号スイートと WEP の設定」を参照してください。

## セキュリティ設定

ワイヤレス デバイスによる認証を求める無線クライアントは、そのワイヤレス デバイスで設定されているのと同じセキュリティ オプションをサポートする必要があります。たとえば、Extensible Authentication Protocol (EAP; 拡張認証プロトコル) または Light Extensible Authentication Protocol (LEAP; 拡張認証プロトコル)、MAC アドレス認証、Message Integrity Check (MIC; メッセージ完全性チェック)、WEP キー ハッシュ、および 802.1X プロトコルバージョンなどです。

無線クライアントが EAP-FAST 認証を使用している場合は、Open 認証 + EAP を設定する必要があります。Open 認証 + EAP を設定しないと、警告メッセージが表示されます。CLI を使用している場合は、次の警告メッセージが表示されます。

「SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.」

GUIを使用している場合は、次の警告メッセージが表示されます。

「WARNING:

「Network EAP is used for LEAP authentication only.If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured.」

無線クライアントがワイヤレス デバイスから認証されない場合には、クライアント アダプタの適切なセキュリティ設定、および現在のワイヤレス デバイスの設定で使用可能なクライアントのアダプタ ドライバおよびファームウェアのバージョンをシステム管理者に問い合わせてください。



(注) Aironet Client Utility (ACU) で [Status] ページに表示されるワイヤレス デバイスの MAC アドレスは、ワイヤレス デバイスの無線ポートの MAC アドレスです。アクセス ポイントのイーサネット ポートの MAC アドレスは、アクセス ポイントの背面のラベルに記載されています。

## デフォルト設定へのリセット

ワイヤレス デバイスの設定に必要なパスワードを忘れてしまった場合は、設定を完全にリセットする必要があることもあります。1040、1100、および 1200 シリーズのアクセス ポイントでは、アクセス ポイントの MODE ボタンまたは Web ブラウザ インターフェイスを使用します。350 シリーズのアクセス ポイントでは、Web ブラウザ インターフェイスまたは CLI を使用します。



(注) 次の手順では、パスワード、WEP キー、IP アドレス、SSID などのすべての設定をデフォルトにリセットします。デフォルトのユーザ名とパスワードは両方とも **Cisco** で、大文字と小文字が区別されます。

## MODE ボタンの使用

次の手順に従って現在の設定を削除し、MODE ボタンを使用してアクセス ポイントのすべての設定をデフォルトに戻します。



(注) 設定をデフォルトにリセットするには、MODE ボタンを使用する代わりに「[Web ブラウザ インターフェイスの使用](#)」(P.22-5) の手順または「[CLI の使用](#)」(P.22-6) の手順に従います。350 シリーズのアクセス ポイントでは、MODE ボタンを使用して設定をデフォルトにリセットすることはできません。

- ステップ 1 アクセス ポイントの電源（外部電源用の電源ジャックまたはインライン パワー用のイーサネット ケーブル）を切ります。
- ステップ 2 MODE ボタンを押しながら、アクセス ポイントに電源を再接続します。
- ステップ 3 MODE ボタンを押し続けて、ステータス LED がオレンジに変わったら（約 1～2 秒かかります）ボタンを放します。



(注) Cisco Aironet 1140 シリーズ アクセス ポイントでは、ステータス LED が青になるまで、MODE ボタンを押したままにします。

**ステップ 4** アクセス ポイントをリブートした後で、Web ブラウザ インターフェイスまたは CLI を使用して、アクセス ポイントを再設定する必要があります。



(注) アクセス ポイントは、IP アドレスも含めてデフォルト値に設定されます (DHCP を使用して IP アドレスを受信するように設定されます)。デフォルトのユーザ名とパスワードは **Cisco** で、大文字と小文字が区別されます。

## Web ブラウザ インターフェイスの使用方法

Web ブラウザ インターフェイスを使用して、現在の設定を削除してワイヤレス デバイスのすべての設定をデフォルトに戻す手順は、次のとおりです。

- ステップ 1** インターネット ブラウザを開きます。Microsoft Internet Explorer (バージョン 6.x 以降) または Netscape Navigator (バージョン 7.x) を使用してください。
- ステップ 2** ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。
- ステップ 3** [User Name] フィールドにユーザ名を入力します。
- ステップ 4** [Password] フィールドにワイヤレス デバイスのパスワードを入力し、**Enter** を押します。[Summary Status] ページが表示されます。
- ステップ 5** [System Software] をクリックして、[System Software] 画面を表示します。
- ステップ 6** [System Configuration] をクリックして、[System Configuration] 画面を表示します。
- ステップ 7** [Reset to Defaults] または [Reset to Defaults (Except IP)] ボタンをクリックします。



(注) 静的 IP アドレスを保持する場合は、[Reset to Defaults (Except IP)] を選択します。

- ステップ 8** [Restart] をクリックします。システムがリブートします。
- ステップ 9** ワイヤレス デバイスをリブートした後で、Web ブラウザ インターフェイスまたは CLI を使用して、ワイヤレス デバイスを再設定する必要があります。デフォルトのユーザ名とパスワードは **Cisco** で、大文字と小文字が区別されます。

## CLI の使用

CLI を使用して、現在の設定を削除してワイヤレス デバイスのすべての設定をデフォルトに戻す手順は、次のとおりです。

**ステップ 1** Telnet セッションまたはワイヤレス デバイス コンソール ポートへの接続を使用して、CLI を開きます。

**ステップ 2** 電源を切って再度電源を入れ、ワイヤレス デバイスをリブートします。

**ステップ 3** コマンド プロンプトが表示され、ワイヤレス デバイスによってイメージの拡大が開始されるまで、ワイヤレス デバイスのブートを続けます。CLI に次の行が表示されたら、Esc を押します。

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...#####
#####
#####
#####
```

**ステップ 4** ap: プロンプトに対して **flash\_init** コマンドを入力し、フラッシュを初期化します。

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

**ステップ 5** **dir flash:** コマンドを使用して、フラッシュのコンテンツを表示させ、コンフィギュレーション ファイル **config.txt** を検索します。

```
ap: dir flash:
Directory of flash:/
 3 .rwx 223 <date> env_vars
 4 .rwx 2190 <date> config.txt
 5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

**ステップ 6** **rename** コマンドを使用して、**config.txt** ファイルの名前を **config.old** に変更します。

```
ap: rename flash:config.txt flash:config.old
```

**ステップ 7** **reset** コマンドを入力してワイヤレス デバイスをリブートします。

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
  using eeprom values
WRDTR,CLKTR: 0x80000800 0x80000000
RQDC ,RFDC : 0x80000033 0x000001cb
  ddr init done
IOS Bootloader - Starting system.
Xmodem file system is available.
DDR values used from system serial eeprom.
WRDTR,CLKTR: 0x80000800, 0x80000000
RQDC, RFDC : 0x80000033, 0x000001cb
```

**ステップ 8** アクセス ポイントでソフトウェアのリブートが終了したら、アクセス ポイントに対して新しい Telnet セッションを開始します。





(注) ワイヤレス デバイスは、IP アドレス (DHCP を使用して IP アドレスを受信するように設定) およびデフォルトのユーザ名とパスワード (Cisco) の設定など、デフォルト値に設定されています。

**ステップ 9** IOS ソフトウェアがロードされると、特権 EXEC コマンド **del** を使用してフラッシュから config.old ファイルを削除できます。

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

## アクセスポイントのイメージのリロード

ワイヤレス デバイスでファームウェアの障害が生じた場合は、Web ブラウザ インターフェイスを使用してイメージファイルをリロードする必要があります。または、1040、1100、および 1200 シリーズのアクセスポイントでは MODE ボタンを約 30 秒押し続けます。ワイヤレス デバイスのファームウェアが完全に動作している間に、ファームウェア イメージをアップグレードする場合、ブラウザ インターフェイスを使用します。ただし、アクセスポイントのファームウェア イメージが壊れている場合は MODE ボタンを使用します。350 シリーズのアクセスポイントでは、MODE ボタンを使用してイメージファイルをリロードすることはできませんが、Telnet またはコンソールポート接続を経由して CLI を使用できます。

## MODE ボタンの使用

1040、1100、および 1200 シリーズのアクセスポイントで MODE ボタンを使用すると、ネットワーク上またはアクセスポイントのイーサネットポートに接続した PC 上のアクティブな簡易ファイル転送プロトコル (TFTP) サーバから、アクセスポイントのイメージファイルをリロードできます。



(注) 350 シリーズのアクセスポイントでは、MODE ボタンを使用してイメージファイルをリロードすることはできません。350 シリーズのアクセスポイントでイメージファイルをリロードするには、「CLI の使用」(P.22-10) の手順に従ってください。

ワイヤレス デバイスの 3 つの LED インジケータが赤色になり、ファームウェア障害、またはファームウェア イメージの破壊が発生した場合、接続した TFTP サーバからイメージをリロードする必要があります。



(注) その結果、パスワード、WEP キー、ワイヤレス デバイスの IP アドレス、SSID などすべての設定がデフォルトにリセットされます。

## ■ アクセスポイントのイメージのリロード

アクセスポイントのイメージファイルのリロードする手順は、次のとおりです。

- 
- ステップ 1** 使用する PC は、静的 IP アドレスが 10.0.0.2 ~ 10.0.0.30 の範囲で設定されている必要があります。
  - ステップ 2** PC の TFTP サーバフォルダにアクセスポイントのイメージファイル（1040 または 1100 シリーズのアクセスポイントの場合は `c1100-k9w7-tar.123-8.JA.tar`、1200 シリーズのアクセスポイントの場合は `c1200-k9w7-tar.123-8.JA.tar` など）が格納され、TFTP サーバが起動していることを確認します。詳細については、「[アクセスポイントのイメージファイルの入手](#)」および「[TFTP サーバソフトウェアの入手](#)」の各項を参照してください。
  - ステップ 3** TFTP サーバフォルダのアクセスポイントイメージファイルの名前を変更します。たとえば、1100 シリーズのアクセスポイントのイメージファイルが `c1100-k9w7-tar.123-8.JA.tar` の場合、`c1100-k9w7-tar.default` のように名前を変更します。
  - ステップ 4** Category 5 (CAT 5; カテゴリ 5) のイーサネットケーブルを使用して、PC をアクセスポイントに接続します。
  - ステップ 5** アクセスポイントの電源（外部電源用の電源ジャックまたはインラインパワー用のイーサネットケーブル）を切ります。
  - ステップ 6** MODE ボタンを押しながら、アクセスポイントに電源を再接続します。
  - ステップ 7** MODE ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ~ 30 秒かかります）、MODE ボタンを放します。
  - ステップ 8** アクセスポイントがリブートしてすべての LED が緑色に変わった後、ステータス LED が緑色に点滅するまで待ちます。
  - ステップ 9** アクセスポイントをリブートした後で、Web ブラウザ インターフェイスまたは CLI を使用して、アクセスポイントを再設定する必要があります。
- 

## Web ブラウザ インターフェイスの使用法

ワイヤレスデバイスのイメージファイルのリロードするには、Web ブラウザ インターフェイスも使用できます。Web ブラウザ インターフェイスでは、HTTP または TFTP インターフェイスを使用したイメージファイルのロードがサポートされています。



**(注)** ブラウザを使用してイメージファイルのリロードする場合、ワイヤレスデバイスの設定は変更されません。

---

## ブラウザ HTTP インターフェイス

HTTP インターフェイスを使用すると、PC にあるワイヤレスデバイスのイメージファイルを参照し、ワイヤレスデバイスにイメージをダウンロードできます。HTTP インターフェイスを使用する手順は、次のとおりです。

- 
- ステップ 1** インターネット ブラウザを開きます。Microsoft Internet Explorer（バージョン 6.x 以降）または Netscape Navigator（バージョン 7.x）を使用してください。
  - ステップ 2** ブラウザのアドレス入力用ボックスにワイヤレスデバイスの IP アドレスを入力し、**Enter** を押します。[Enter Network Password] 画面が表示されます。

- ステップ3 [User Name] フィールドにユーザ名を入力します。
  - ステップ4 [Password] フィールドにワイヤレス デバイスのパスワードを入力し、Enter を押します。  
[Summary Status] ページが表示されます。
  - ステップ5 [System Software] タブをクリックして、[Software Upgrade] をクリックします。[HTTP Upgrade] 画面が表示されます。
  - ステップ6 [Browse] をクリックして PC 内のイメージ ファイルを検索します。
  - ステップ7 [Upload] をクリックします。  
詳細は、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。
- 

## ブラウザ TFTP インターフェイス

TFTP インターフェイスを使用すると、ネットワーク デバイスの TFTP サーバを使用してワイヤレス デバイスのイメージ ファイルをロードできます。TFTP サーバを使用する手順は、次のとおりです。

- ステップ1 インターネット ブラウザを開きます。Microsoft Internet Explorer (バージョン 6.x 以降) または Netscape Navigator (バージョン 7.x) を使用してください。
  - ステップ2 ブラウザのアドレス入力用ボックスにワイヤレス デバイスの IP アドレスを入力し、Enter を押します。[Enter Network Password] 画面が表示されます。
  - ステップ3 [User Name] フィールドにユーザ名を入力します。
  - ステップ4 [Password] フィールドにワイヤレス デバイスのパスワードを入力し、Enter を押します。  
[Summary Status] ページが表示されます。
  - ステップ5 [System Software] タブをクリックして、[Software Upgrade] をクリックします。[HTTP Upgrade] 画面が表示されます。
  - ステップ6 [TFTP Upgrade] タブをクリックします。
  - ステップ7 [TFTP Server] フィールドに、TFTP サーバの IP アドレスを入力します。
  - ステップ8 [Upload New System Image Tar File] フィールドに、イメージ ファイル名を入力します。TFTP サーバのルート ディレクトリ下のサブディレクトリ内にファイルがある場合は、TFTP サーバのルート ディレクトリに対する相対パスとファイル名を指定します。ファイルが TFTP サーバのルート ディレクトリにある場合は、ファイル名だけを入力します。
  - ステップ9 [Upload] をクリックします。  
詳細については、[Software Upgrade] 画面で [Help] アイコンをクリックしてください。
-

## CLI の使用

CLI を使用してワイヤレス デバイスのイメージをリロードする手順は、次のとおりです。ワイヤレス デバイスがブートを開始したら、ブート プロセスを中断させ、ブートローダ コマンドを使用して TFTP サーバからイメージをロードして、ワイヤレス デバイス内のイメージを置き換えます。



(注) CLI を使用してイメージ ファイルをリロードする場合、ワイヤレス デバイスの設定は変更されません。

- ステップ 1** ワイヤレス デバイス コンソール ポートへの接続を使用して、CLI を開きます。
- ステップ 2** 電源を切って再度電源を入れ、ワイヤレス デバイスをリブートします。
- ステップ 3** イメージの拡大が開始されるまで、ワイヤレス デバイスのブートを続けます。CLI に次の行が表示されたら、Esc を押します。

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...#####
#####
#####
#####
#####
```

- ステップ 4** ap: コマンド プロンプトが表示されたら、**set** コマンドを入力して、ワイヤレス デバイスに IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを割り当てます。



(注) **set** コマンドを使用して **IP-ADDR**、**NETMASK**、および **DEFAULT\_ROUTER** オプションを入力する場合は、大文字を使用する必要があります。

たとえば、次のように入力します。

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

- ステップ 5** **tftp\_init** コマンドを入力して、ワイヤレス デバイスを TFTP 用に準備します。

```
ap: tftp_init
```

- ステップ 6** **tar** コマンドを入力して、TFTP サーバから新しいイメージをロードおよび拡大します。このコマンドには次の情報を含む必要があります。

- **-xtract** オプション。ロード時にイメージを拡大します。
- TFTP サーバの IP アドレス。
- イメージが格納されている TFTP サーバのディレクトリ。
- イメージの名前。
- イメージの保存先（ワイヤレス デバイスのフラッシュ）。

たとえば、次のように入力します。

```
ap: tar -xtract tftp://192.168.130.222/images/c350-k9w7-tar.122-13.JA1.tar flash:
```

**ステップ 7** 画面の一番下まで出力が表示され、CLI がポーズして --MORE-- と表示されたら、スペースバーを押して続けます。

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
-- MORE --
```



**(注)** スペースバーを押して続行しない場合、プロセスはタイムアウトとなり、ワイヤレスデバイスはイメージの拡大を停止します。

**ステップ 8** **set BOOT** コマンドを入力して、ワイヤレス デバイスがリブートするときに使用するイメージに新しいイメージを指定します。ワイヤレス デバイスによって、イメージと同じ名前のイメージ用ディレクトリが作成されます。このディレクトリをコマンドに含める必要があります。たとえば、次のように入力します。

```
ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

**ステップ 9** **set** コマンドを入力して、ブートローダのエントリを確認します。

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

**ステップ 10** **boot** コマンドを入力して、ワイヤレス デバイスをリブートします。ワイヤレス デバイスがリブートすると、新しいイメージがロードされます。

```
ap: boot
```

## アクセスポイントのイメージファイルの入手

ワイヤレス デバイスのイメージ ファイルは、次の手順に従って Cisco.com から入手できます。

- ステップ 1** インターネット ブラウザを使用して、[Tools and Resources Downloads] ページにアクセスします。URL は、次のとおりです。  
<http://tools.cisco.com/support/downloads/pub/MDFTree.x?butype=wireless>
- ステップ 2** Wireless LAN Access フォルダを展開します。
- ステップ 3** 適切なアクセス ポイント フォルダを展開します。
- ステップ 4** 適切なアクセス ポイントを選択します。
- ステップ 5** 使用する CCO ログイン ユーザ名とパスワードを入力します。[Select Software] ページが表示されます。
- ステップ 6** [IOS] をクリックします。提供されている Cisco IOS バージョンの一覧が表示されます。
- ステップ 7** ダウンロードするバージョンを選択します。選択したバージョンのダウンロード ページが表示されます。
- ステップ 8** [WIRELESS LAN] をクリックします。
- ステップ 9** 要求された場合は、ユーザ名とパスワードを入力します。[Encryption Software Export Distribution Authorization] ページが表示されます。
- ステップ 10** ページに表示された質問に回答して [Submit] をクリックします。[Download] ページが表示されます。
- ステップ 11** [DOWNLOAD] をクリックします。[Software Download Rules] ページが表示されます。
- ステップ 12** [Software Download Rules] をよく読んで、[Agree] をクリックします。
- ステップ 13** 要求された場合は、ユーザ名とパスワードを入力します。[File Download] ウィンドウが表示されます。
- ステップ 14** ファイルを、使用するハード ドライブのディレクトリに保存します。

## TFTP サーバソフトウェアの入手

TFTP サーバソフトウェアは、いくつかの Web サイトからダウンロードできます。次の URL から入手できるシェアウェアの TFTP ユーティリティを推奨します。

<http://tftpd32.jounin.net>

ユーティリティのインストール方法と使用方法については、Web サイトの指示に従ってください。

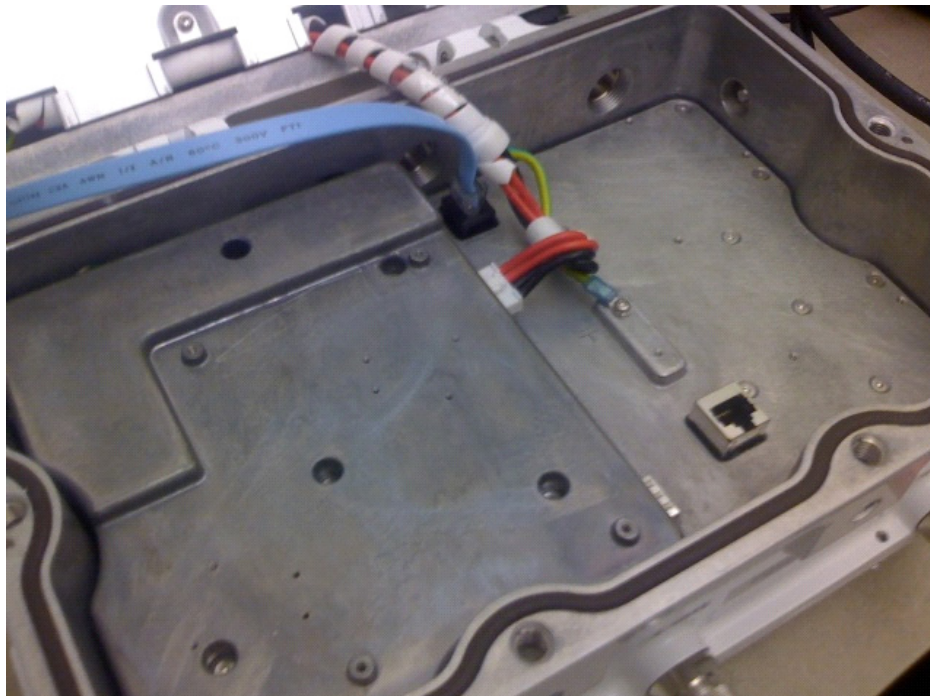
## 1520 アクセスポイントでのイメージの復元

1520 アクセスポイントでイメージを復元するプロセスは、コンソールポートを持つ IOS アクセスポイントでのプロセスと同様です。

1520 アクセス ポイントでイメージの復元を実行するには、次の手順に従います。

- ステップ 1** アクセス ポイントの電源をオフにした状態で、RJ45 コンソール ケーブルをコンソール ポートに接続します。コンソール ポートは、ユニット内部にある黒いプラスチック製の RJ45 ジャックです。

図 22-1 コンソール ポートへの RJ45 コンソール ケーブルの接続



- ステップ 2** 8 データビット、パリティなし、フロー制御なし、9600 bps に対応するようにターミナルエミュレータを設定します。
- ステップ 3** アクセス ポイントに電力を供給します。
- ステップ 4** ブートローダに「Base Ethernet MAC Address」と表示されたら、Esc キーを押して **ap:** プロンプトを開始します。

```
IOS Bootloader - Starting system.
Xmodem file system is available.
flashfs[0]: 13 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31868928
flashfs[0]: Bytes used: 9721344
flashfs[0]: Bytes available: 22147584
flashfs[0]: flashfs fsck took 20 seconds.
Reading cookie from flash parameter block...done.
Base Ethernet MAC address: 00:1f:27:75:db:00
```

```
The system boot has been aborted.The following
commands will finish loading the operating system
software:
```

```
    ether_init
    tftp_init
    boot
```

```
ap:
```



(注) **ENABLE\_BREAK=no environmental** 変数が設定されている場合、ブートローダにエスケープできません。

- ステップ 5** 1520 アクセスポイントの LAN ポート (「PoE In」) と TFTP サーバをケーブルで接続します。たとえば、tftpd32 がインストールされた Windows PC に接続します。
- ステップ 6** **c1520 k9w8 IOS** イメージの正常なコピーを TFTP サーバにインストールします。
- ステップ 7** 静的 IP アドレスで、TFTP サーバの LAN インターフェイスを設定します。たとえば、10.1.1.1 と指定します。
- ステップ 8** アクセスポイントで、次のように入力します。

```
ap: dir flash:
```

新しいコードを保持するのに十分な空きスペースがフラッシュに存在すること (またはフラッシュ ファイル システムが破損しているかどうか) を確認して、次のように入力します。

```
ap: format flash:
```

- ステップ 9** TFTP を使用して 1520 アクセスポイントのフラッシュにイメージをコピーします。

```
ap: set IP_ADDR 10.1.1.2
```

```
ap: set NETMASK 255.255.255.0
```

```
ap: ether_init
Initializing ethernet port 0...
```

```
ap: tftp_init
tftp_init success: You can now use tftp file system!
```

```
ap: tar -xtract tftp://10.1.1.1/c1520-k9w8-tar.124-21a.JA2 flash:
```

```
extracting info (293 bytes)
c1520-k9w8-mx.124-21a.JA2/ (directory) 0 (bytes)
extracting c1520-k9w8-mx.124-21a.JA2/c1520-k9w8-mx.124-21a.JA2 (5197365 bytes)..
.....
extracting c1520-k9w8-mx.124-21a.JA2/8001.img (97896 bytes).....
extracting c1520-k9w8-mx.124-21a.JA2/c1520_avr_1.img (10368 bytes)..
extracting c1520-k9w8-mx.124-21a.JA2/c1520_avr_2.img (10624 bytes)..
extracting c1520-k9w8-mx.124-21a.JA2/c1520_avr_3.img (14720 bytes)...
extracting c1520-k9w8-mx.124-21a.JA2/info (293 bytes)
extracting info.ver (293 bytes)
ap: set
49_RADIO_CARRIER_SET=0x0024
49_RADIO_MAX_TX_POWER=400
58_RADIO_CARRIER_SET=0x0027
58_RADIO_MAX_TX_POWER=640
5G_RADIO_ANTENNA_DIVERSITY=0x01
5G_RADIO_CARRIER_SET=0x000B
5G_RADIO_ENCRYPTION_CONFIG=0x0002
5G_RADIO_MAX_TX_POWER=250
BOOT=flash:/c1520-k9w8-mx.124-18a.JA1/c1520-k9w8-mx.124-18a.JA1
CRASH_LOG=yes
DEFAULT_ROUTER=10.0.0.1
DOT11G_RADIO_MODE=0xFF
DOT11_DEVICE_TYPE=4C
DOT11_ENCRYPTION_CONFIG=0x0002
DOT11_MAX_ASSOCIATION_NUM=2007
ENABLE_BREAK=yes
FAB_PART_NUM=1c 1f 44 03
```



```

IP_ADDR=10.1.1.2
MAC_ADDR=00:1F:27:75:DB:00
MAC_ADDR_BLOCK_SIZE=01 00
NETMASK=255.255.255.0
NEW_IMAGE=yes
PCA_ASSY_NUM_800=03 20 00 70 ed 03
PCA_PART_NUM_73=49 2a a6 03
PCA_REVISION_NUM=B0
PCA_REVISION_NUM_800=B0
PCB_SERIAL_NUM=FOC1213496Z
PEP_PRODUCT_ID=AIR-LAP1524PS-A-K9
PEP_VERSION_ID=V01
PRODUCT_MODEL_NUM=AIR-LAP1524PS-A-K9
RADIO_ANTENNA_DIVERSITY=0x01
RADIO_CARRIER_SET=0x0000
RADIO_MAX_TX_POWER=640
RELOAD_REASON=23
SYSTEM_REVISION_NUM_800=A0
TERMLINES=0
TOP_ASSY_NUM_800=03 20 00 77 2e 01
TOP_ASSY_SERIAL_NUM=FTX1218P080

ap:

ap: dir flash:
Directory of flash:/

 2  -rwx  63      <date>          mesh_cfg.txt
 3  -rwx 4515840  <date>          c1520-img-tar
 4  -rwx  213    <date>          mesh_port_cfg.txt
 9  drwx  384    <date>          c1520-k9w8-mx.124-18a.JA1
 5  -rwx 1008    <date>          env_vars
 6  -rwx  293    <date>          info
 7  -rwx  9240   <date>          private-multiple-fs
 8  -rwx  90439  <date>          event.log
15  drwx  384    <date>          c1520-k9w8-mx.124-21a.JA2
10  -rwx  3564   <date>          private-config
24  -rwx  293    <date>          info.ver

16813056 bytes available (15055872 bytes used)

ap: set BOOT flash:/c1520-k9w8-mx.124-21a.JA2/c1520-k9w8-mx.124-21a.JA2

ap: boot
Loading "flash:/c1520-k9w8-mx.124-21a.JA2/c1520-k9w8-mx.124-21a.JA2" ...#####
#####
[ ... ]
*Mar  1 00:00:14.047: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C1520 Software (C1520-K9W8-M), Version 12.4(21a)JA2, RELEASE SOFTWARE
(fc1)

```





## プロトコルフィルタ

---

この付録の表では、アクセス ポイントでフィルタの可能なプロトコルを示します。各表の内容は、次のとおりです。

- 表 A-1 : 「EtherType プロトコル」
- 表 A-2 : 「IP プロトコル」
- 表 A-3 : 「IP ポート プロトコル」

いずれの表でも、「プロトコル」の列にプロトコル名、「別の識別名」の列にプロトコルの別名、「ISO 識別番号」の列にプロトコルの ISO 識別番号を示します。

表 A-1 EtherType プロトコル

プロトコル	別の識別名	ISO 識別番号
ARP	—	0x0806
RARP	—	0x8035
IP	—	0x0800
Berkeley Trailer Negotiation	—	0x1000
LAN Test	—	0x0708
X.25 Level3	X.25	0x0805
Banyan	—	0x0BAD
CDP	—	0x2000
DEC XNS	XNS	0x6000
DEC MOP Dump/Load	—	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	—	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	—	0x00E0
IPX 802.3	—	0x00FF
Novell IPX (old)	—	0x8137
Novell IPX (new)	IPX	0x8138
EAPOL (old)	—	0x8180
EAPOL (new)	—	0x888E
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet Config Test	—	0x9000
NetBUI	—	0xF0F0

表 A-2 IP プロトコル

プロトコル	別の識別名	ISO 識別番号
dummy	—	0
Internet Control Message Protocol	ICMP	1
Internet Group Management Protocol	IGMP	2
Transmission Control Protocol	TCP	6
Exterior Gateway Protocol	EGP	8
PUP	—	12
CHAOS	—	16
User Datagram Protocol	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
Encapsulation Header	encap_hdr	98
Spectralink Voice Protocol	SVP Spectralink	119
raw	—	255

表 A-3 IP ポート プロトコル

プロトコル	別の識別名	ISO 識別番号
TCP port service multiplexer	tcpmux	1
echo	—	7
discard (9)	—	9
systat (11)	—	11
daytime (13)	—	13
netstat (15)	—	15
Quote of the Day	qotd quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	。
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
Simple Mail Transport Protocol	SMTP mail	25
time	timserver	37
Resource Location Protocol	RLP	39
IEN 116 Name Server	name	42
whois	nickname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101

表 A-3 IP ポート プロトコル (続き)

プロトコル	別の識別名	ISO 識別番号
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
Network Time Protocol	nntp	123
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
Simple Network Management Protocol	SNMP	161
SNMP Traps	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
Border Gateway Protocol	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194

表 A-3 IP ポート プロトコル (続き)

プロトコル	別の識別名	ISO 識別番号
SNMP Unix Multiplexer	smux	199
AppleTalk Routing	at-rtmp	201
AppleTalk name binding	at-nbp	202
AppleTalk echo	at-echo	204
AppleTalk Zone Information	at-zis	206
NISO Z39.50 database	z3950	210
IPX	—	213
Interactive Mail Access Protocol v3	imap3	220
Unix Listserv	ulistserv	372
syslog	—	514
Unix spooler	spooler	515
talk	—	517
ntalk	—	518
route	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	—	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-privileged	prospero-np	1525
RADIUS	—	1812
Concurrent Versions System	CVS	2401
Cisco IAPP	—	2887
Radio Free Ethernet	RFE	5002





## サポート対象 MIB

この付録では、アクセスポイントがこのソフトウェアリリースでサポートする簡易ネットワーク管理プロトコル (SNMP) 管理情報ベース (MIB) を示します。Cisco IOS SNMP エージェントは、SNMPv1、SNMPv2、および SNMPv3 をサポートします。この付録の内容は、次のとおりです。

- [「MIB の一覧」 \(P.B-1\)](#)
- [「FTP による MIB ファイルへのアクセス」 \(P.B-2\)](#)

### MIB の一覧

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-LBS-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB

- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI-MIB
- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- CISCO-WDS-INFO-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

## FTP による MIB ファイルへのアクセス

FTP を使用して各 MIB ファイルを取得する手順は、次のとおりです。

- 
- ステップ 1** FTP を使用してサーバ **ftp.cisco.com** にアクセスします。
  - ステップ 2** ユーザ名 **anonymous** を使用してログインします。
  - ステップ 3** パスワードが要求されたら、Eメールのユーザ名を入力します。
  - ステップ 4** `ftp>` プロンプトで、ディレクトリを **/pub/mibs/v1** または **/pub/mibs/v2** に変更します。
  - ステップ 5** `get MIB_filename` コマンドを使用して、MIB ファイルのコピーを入手します。
- 



(注)

シスコの Web サイトでも、MIB に関する情報にアクセスできます。  
<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

---



# エラーメッセージおよびイベントメッセージ

この付録では、CLI のエラーメッセージおよびイベントメッセージの一覧を示します。この付録の構成は、次のとおりです。

- 「表記法」 (P.C-2)
- 「ソフトウェア自動アップグレードメッセージ」 (P.C-3)
- 「アソシエーション管理メッセージ」 (P.C-5)
- 「解凍メッセージ」 (P.C-7)
- 「システム ログメッセージ」 (P.C-7)
- 「802.11 サブシステムメッセージ」 (P.C-8)
- 「アクセスポイント間プロトコルメッセージ」 (P.C-22)
- 「ローカル認証サーバメッセージ」 (P.C-23)
- 「WDSメッセージ」 (P.C-25)
- 「ミニ IOSメッセージ」 (P.C-26)
- 「アクセスポイントまたはブリッジについてのメッセージ」 (P.C-27)
- 「Cisco Discovery Protocolメッセージ」 (P.C-28)
- 「外部 RADIUS サーバエラーメッセージ」 (P.C-28)
- 「LWAPP エラーメッセージ」 (P.C-28)
- 「センサーメッセージ」 (P.C-29)
- 「SNMP エラーメッセージ」 (P.C-30)
- 「SSH エラーメッセージ」 (P.C-31)

# 表記法

システム エラー メッセージは、表 C-1 に示す形式で表示されます。

**表 C-1 システム エラー メッセージの形式**

メッセージのコンポーネント	説明	例
エラー ID	エラーをカテゴリ分けするストリング。	STATION-ROLE
ソフトウェア コンポーネント	エラーのソフトウェア コンポーネントを識別するためのストリング。	AUTO_INSTALL
重大度	エラーの重大度を示す数値ストリング。	0-LOG-EMERG：緊急事態。何も機能していない 1-LOG-ALERT：ユーザに非常に深刻な問題であることを知らせる 2-LOG-CRIT：深刻で重大なエラーの可能性を警告する 3-LOG-ERR：エラー状態の警告。大半の機能は正常に動作しているが、ユーザは注意を払うべきである 4-LOG-WARNING：必要であれば、無視してもよい警告 5-LOG-NOTICE：ユーザの懸念事項になる可能性のある通告 6-LOG-INFO：情報（深刻ではない） 7-LOG-DEBUG：デバッグ情報（深刻ではない）
動作フラグ	追加処理の表示対象であるコードが内部的に使用。	0：アクション不要を示すフラグ MSG-TRACEBACK：メッセージにトレースバックを含める MSG-PROCESS：メッセージにプロセス情報を含める MSG-CLEAR：問題のある状態が解消されたことを示す MSG-SECURITY：セキュリティ メッセージとして表示する MSG-NOSCAN：EEM パターン スクリーニングを抑制する
%d	整数値。	2450
%e	MAC アドレス。	000b.fcff.b04e
%s	エラーの詳細を示すメッセージストリング。	「Attempt to protect port 1640 failed.」
%x	16 進数値。	0x001

# ソフトウェア自動アップグレード メッセージ

**エラーメッセージ** SW-AUTO-UPGRADE-2-FATAL\_FAILURE: Attempt to upgrade software failed, software on flash may be deleted. Please copy software into flash.

**説明** ソフトウェアの自動アップグレードに失敗しました。フラッシュのソフトウェアが削除されている可能性があります。ソフトウェアをフラッシュにコピーしてください。

**推奨処置** ソフトウェアをコピーしてから装置をリブートしてください。

**エラーメッセージ** SW-AUTO-UPGRADE-7-DHCP\_CLIENT\_FAILURE: "%s": Auto upgrade of the software failed.

**説明** ソフトウェアの自動アップグレードに失敗しました。

**推奨処置** Dynamic Host Configuration Protocol (DHCP) クライアントが実行されていることを確認してください。

**エラーメッセージ** SW-AUTO-UPGRADE-7-DHCP\_SERVER\_FAILURE: ["%s": Auto upgrade of the software failed.]

**説明** ソフトウェアの自動アップグレードに失敗しました。

**推奨処置** DHCP サーバが正しく設定されていることを確認してください。

**エラーメッセージ** SW-AUTO-UPGRADE-7\_BOOT\_FAILURE: ["%s": Auto upgrade of the software failed.]

**説明** ソフトウェアの自動アップグレードに失敗しました。

**推奨処置** 装置をリブートしてください。再度メッセージが表示される場合、表示されているエラーメッセージを正確にコピーし、テクニカルサポート担当者に報告してください。

**エラーメッセージ** DOT11-4-UPGRADE: [Send your company name and the following report to migrateapj52w52@cisco.com.] The following AP has been migrated from J(j52) to U(w52) Regulatory Domain: AP name AP Model Ethernet MAC %s %s %e \U\Regulatory Doman

**説明** J から U への日本の規制分野フィールド アップグレードが完了しました。

**推奨処置** なし。

**エラーメッセージ** AUTO-INSTALL-4-STATION\_ROLE: ["%s": The radio is operating in automatic install mode.]

**説明** 自動インストール モードで無線が動作しています。

**推奨処置** 設定インターフェイス コマンド **station-role** は、無線をインストール モード以外の役割に設定するために使用します。

**エラーメッセージ** AUTO-INSTALL-4-IP\_ADDRESS\_DHCP: 「The radio is operating in automatic install mode and has set ip address dhcp.」

**説明** 無線は自動インストールモードで動作しており、DHCPを介してIPアドレスを受信するように設定されています。

**推奨処置** 設定インターフェイスコマンド **station-role** は、無線をインストールモード以外の役割に設定するために使用します。

**エラーメッセージ** AUTO-INSTALL-6\_STATUS: "%s" %s.RSSI=-%d dBm.: 「The radio is operating in install mode.」

**説明** 自動インストールモードで無線が動作しています。

**推奨処置** 設定インターフェイスコマンド **station-role** は、無線をインストールモード以外の役割に設定するために使用します。

**エラーメッセージ** AVR\_IMAGE\_UPDATE-7-UPDATE\_COMPLETE: 「The AVR "\$d" firmware was successfully updated.」

**説明** アクセスポイントAVRファームウェアは正常に更新されました。

**推奨処置** なし。

**エラーメッセージ** AVR\_IMAGE\_UPDATE-2-UPDATE\_FAILURE: 「The AVR "\$d" firmware is not current.Update error: "\$s".」

**説明** AVRファームウェアは最新の状態ではありません。アップデートに失敗しました

**推奨処置** エラーメッセージを書き写し、テクニカルサポート担当者に報告してください。

**エラーメッセージ** AVR\_IMAGE\_UPDATE-4-UPDATE\_SKIPPED: 「AVR "\$d" update processing was skipped:"\$s".」

**説明** エラーのため、AVRアップデートの処理がスキップされました。

**推奨処置** なし。

**エラーメッセージ** AVR\_IMAGE\_UPDATE-4-UPDATE\_START: 「The system is updating the AVR "\$d" firmware.Please wait ...」

**説明** システムは、AVRファームウェアをアップデートしています。

**推奨処置** なし。

# アソシエーション管理メッセージ

**エラーメッセージ** DOT11-3-BADSTATE: 「%s %s ->%s.」

**説明** 802.11 アソシエーションと管理では、テーブル方式ステートマシンを使用してアソシエーションのさまざまなステートへの移行を追跡します。ステート移行は、アソシエーションが多くの可能性のあるイベントのいずれかを受け取ったときに起こります。このエラーが発生した場合、移行前のステートでは予測できなかったイベントをアソシエーションが受け取ったことを意味します。

**推奨処置** システムは稼働し続けますが、このエラーを発生させたアソシエーションは損失する場合があります。表示されているエラーメッセージを正確にコピーし、サービス担当者に報告してください。

**エラーメッセージ** DOT11-6-ASSOC: 「Interface %s, Station %s e% %s KEY\_MGMT (%s), MSGDEF\_LIMIT\_MEDIUM.」

**説明** 表示されているステーションは、表示されているインターフェイスのアクセスポイントにアソシエートされています。

**推奨処置** なし。

**エラーメッセージ** DOT11-6-ADD: 「Interface %s, Station %e associated to parent %e.」

**説明** 表示されているステーションは、表示されているインターフェイスの親アクセスポイントにアソシエートされています。

**推奨処置** なし。

**エラーメッセージ** DOT11-6-DISASSOC: Interface %s, Deauthenticating Station %e #s

**説明** ステーションがアクセスポイントからアソシエーションを解除されました。

**推奨処置** なし。

**エラーメッセージ** DOT11-6-ROAMED: 「Station %e roamed to %e.」

**説明** 表示されているステーションは、表示されている新しいアクセスポイントにローミングしました。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-ENCRYPT\_MISMATCH: 「Possible encryption key mismatch between interface %s and station %e.」

**説明** 表示されているインターフェイスとステーションの暗号化設定が一致していない可能性があります。

**推奨処置** このインターフェイスの暗号化設定と、エラーを起こしているステーションの暗号化設定が一致することを確認してください。

**エラーメッセージ** DOT11-4-DIVER\_USED: Interface \$s, Mcs rates 8-15 disabled due to only one transmit or receive antenna enabled

**説明** これらのレートでは、少なくとも2つの送受信アンテナを有効にする必要があります。

**推奨処置** コンソールまたはシステムログに出力されたエラーメッセージをそのままコピーします。Output Interpreter (<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>) を使用して、エラーについて調査し、解決を試みます。また、<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> にアクセスして、Bug Toolkit を検索してください。それでもサポートが必要である場合は、インターネット経由で、Technical Assistance Center ([http://www.cisco.com/cgi-bin/front.x/case\\_tools/caseOpen.pl](http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl)) でケースを開くか、シスコのテクニカルサポート担当者に連絡し、収集した情報を報告します。

**エラーメッセージ** DOT11-4-NO\_HT: Interface %s, Mcs rates disabled on vlan %d due to %s

**説明** 正しい設定が使用されていなかったため、HT レートを使用できませんでした。

**推奨処置** コンソールまたはシステムログに出力されたエラーメッセージをそのままコピーします。Output Interpreter (<https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>) を使用して、エラーについて調査し、解決を試みます。また、<http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl> にアクセスして、Bug Toolkit を検索してください。それでもサポートが必要である場合は、インターネット経由で、Technical Assistance Center ([http://www.cisco.com/cgi-bin/front.x/case\\_tools/caseOpen.pl](http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl)) でケースを開くか、シスコのテクニカルサポート担当者に連絡し、収集した情報を報告します。

**エラーメッセージ** DOT11-4-NO\_MBSSID\_BACKUP\_VLAN: Backup VLANs cannot be configured if MBSSID is not enabled: "\$s" not started

**説明** VLAN のバックアップを有効にするには、MBSSID モードを設定する必要があります。

**推奨処置** このデバイスで MBSSID を設定します。



## 解凍メッセージ

**エラーメッセージ** SOAP-4-UNZIP\_OVERFLOW: 「Failed to unzip %s, exceeds maximum uncompressed html size.」

**説明** HTTP サーバが HTTP GET 要求に対して圧縮ファイルを取り出すことができません。これは、ファイルが圧縮解除プロセスで使用されるバッファよりも大きすぎるためです。

**推奨処置** ファイルが有効な HTML ページであることを確認します。有効である場合、圧縮する前のファイルをフラッシュにコピーして、HTTP を通じて取り出します。

## システム ログ メッセージ

**エラーメッセージ** %DOT11-4-LOADING\_RADIO: Interface [chars], loading the radio firmware ([chars])

**説明** 新しいファームウェアをロードするために、無線が停止されました。

**推奨処置** なし。

**エラーメッセージ** %LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]

**説明** データ リンク レベル ライン プロトコルの状態が変わりました。

**推奨処置** なし。

**エラーメッセージ** %SYS-5-RESTART: System restarted --[chars]

**説明** リロードまたは再起動が要求されました。

**推奨処置** 単なる通知メッセージです。なし。

**エラーメッセージ** %SYS-5-CONFIG\_I: Configured from [chars] by [chars]

**説明** ルータの設定が変更されています。

**推奨処置** これは単なる通知メッセージです。なし。

**エラーメッセージ** %LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]

**説明** 表示されているインターフェイスのデータ リンク レベル ライン プロトコルの状態が変わりました。

**推奨処置** なし。

**エラーメッセージ** %SNMP-5-COLDSTART: SNMP agent on host [chars] is undergoing a cold start

**説明** SNMP サーバがコールドスタートを完了しました。

**推奨処置** 単なる通知メッセージです。なし。

**エラーメッセージ** %SYS-6-CLOCKUPDATE: System clock has been updated from [chars] to [chars], configured from [chars] by [chars].

**説明** システムクロックが変更されました。

**推奨処置** これは単なる情報メッセージです。なし。

## 802.11 サブシステム メッセージ

**エラーメッセージ** DOT11-6-FREQ\_USED: 「Interface %s, frequency %d selected.」

**説明** 未使用の周波数をスキャンした後に、表示されたインターフェイスにより、表示された周波数が選択されました。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-NO-VALID\_INFRA\_SSID: 「No infrastructure SSID configured.%s not started.」

**説明** インフラストラクチャ SSID は設定されていませんでした。また、表示されたインターフェイスは開始されていませんでした。

**推奨処置** 無線の設定に 1 つ以上のインフラストラクチャ SSID を追加します。

**エラーメッセージ** DOT11-4-VERSION\_UPGRADE: 「Interface %d, upgrading radio firmware.」

**説明** 表示されたインターフェイスの起動時に、アクセスポイントで誤ったバージョンのファームウェアが見つかりました。無線は要求されたバージョンでロードされます。

**推奨処置** なし。

**エラーメッセージ** DOT11-2-VERSION\_INVALID: 「Interface %d, unable to find required radio version %x.%x/ %d/」

**説明** 表示されたインターフェイスの無線ファームウェアを再フラッシュしているときに、アクセスポイントが表示された無線ファームウェア (Cisco IOS ソフトウェアに同梱されているもの) のバージョンが誤っていることを検出しました。

**推奨処置** なし。

**エラーメッセージ** DOT11-3-RADIO\_OVER\_TEMPERATURE: 「Interface %s Radio over temperature detected.」

**説明** 無線の内部温度が、表示された無線インターフェイスの上限を超えました。

**推奨処置** 内部温度を下げるために必要な処理を実行してください。この処理は、使用しているインストラクションによって異なります。

**エラーメッセージ** DOT11-6-RADIO\_TEMPERATURE\_NORMAL: 「Interface %s radio temperature returned to normal.」

**説明** 無線の内部温度が、表示された無線インターフェイスの正常な制限範囲内に戻りました。

**推奨処置** なし。

**エラーメッセージ** DOT11-3-TX\_PWR\_OUT\_OF\_RANGE: 「Interface %s Radio transmit power out of range.」

**説明** 送信電力レベルが、表示された無線インターフェイスの正常範囲外にあります。

**推奨処置** ネットワークおよびサービスから装置を取り外してください。

**エラーメッセージ** DOT11-3-RADIO\_RF\_LO: 「Interface %s Radio cannot lock RF freq.」

**説明** 無線の Phase Lock Loop (PLL) 回線は、表示されたインターフェイスで正しい周波数にロックできません。

**推奨処置** ネットワークおよびサービスから装置を取り外してください。

**エラーメッセージ** DOT11-3-RADIO\_IF\_LO: 「Interface %s Radio cannot lock IF freq.」

**説明** 無線の Intermediate Frequency (IF; 中間周波数) PLL は、表示されたインターフェイスで正しい周波数にロックできません。

**推奨処置** ネットワークおよびサービスから装置を取り外してください。

**エラーメッセージ** DOT11-6-FREQ\_SCAN: 「Interface %s Scanning frequencies for %d seconds.」

**説明** 表示されたインターフェイスで Least Congested Frequency のスキャンが開始され、表示された期間、実行されます。

**推奨処置** なし。

**エラー メッセージ** DOT11-2-NO\_CHAN\_AVAIL: 「Interface %s, no channel available.」

**説明** 使用可能な周波数がありません。過去 30 分間のうちに、レーダーが検出された可能性があります。

**推奨処置** なし。

**エラー メッセージ** DOT11-6-CHAN\_NOT\_AVAIL: 「DFS configured frequency %d Mhz unavailable for %d minute(s).」

**説明** 現在のチャンネルでレーダーが検出されました。Dynamic Frequency Selection (DFS; 動的周波数選択) の規制では、このチャンネルで 30 秒間、送信しないこととされています。

**推奨処置** なし。

**エラー メッセージ** DOT11-6-DFS\_SCAN\_COMPLETE: 「DFS scan complete on frequency %d MHz.」

**説明** デバイスは、表示された周波数で Dynamic Frequency Selection (DFS; 動的周波数選択) 周波数スキャンプロセスを完了しました。

**推奨処置** なし。

**エラー メッセージ** DOT11-6-DFS\_SCAN\_START: 「DFS: Scanning frequency %d MHz for %d seconds.」

**説明** デバイスは、DFS スキャンプロセスを開始しました。

**推奨処置** なし。

**エラー メッセージ** DOT11-6-DFS\_TRIGGERED: 「DFS: triggered on frequency %d MHz.」

**説明** DFS は、表示された周波数でレーダー信号を検出しました。

**推奨処置** なし。このチャンネルは Non-Occupancy List に 30 分間載せられ、新しいチャンネルが選択されます。

**エラー メッセージ** DOT11-4-DFS\_STORE\_FAIL: 「DFS: could not store the frequency statistics.」

**説明** DFS 統計情報をフラッシュに書き込むときにエラーが発生しました。

**推奨処置** なし。

**エラー メッセージ** DOT11-4-NO\_SSID: 「No SSIDs configured, %d not started.」

**説明** すべての SSID が設定から削除されています。無線の実行には SSID が少なくとも 1 つは設定されている必要があります。

**推奨処置** アクセス ポイントに 1 つ以上の SSID を設定します。

**エラーメッセージ** DOT11-4-NO\_SSID\_VLAN: 「No SSID with VLAN configured.%s not started.」

**説明** VLAN 用に設定された SSID はありません。表示されたインターフェイスは開始されていませんでした。

**推奨処置** VLAN 1 つにつき、少なくとも 1 つの SSID を設定する必要があります。表示されたインターフェイス上の VLAN に対して、SSID を少なくとも 1 つ追加してください。

**エラーメッセージ** DOT11-4-NO\_MBSSID\_VLAN: 「No VLANs configured in MBSSID mode.%s not started.」

**説明** MBSSID モードで設定されている VLAN はありません。表示されたインターフェイスは開始されていませんでした。

**推奨処置** 表示されたインターフェイス設定に、VLAN を持つ SSID を少なくとも 1 つ追加してください。

**エラーメッセージ** DOT11-4-NO\_MBSSID\_SHR\_AUTH: 「More than 1 SSID with shared authentication method in non-MBSSID mode % is down.」

**説明** MBSSID が有効にされていない場合、複数の SSID で認証方式は共有できません。

**推奨処置** 設定を開くには、Dot11Radio 無線インターフェイスを削除するか、SSID の認証モードを変更します。

**エラーメッセージ** DOT114-NO\_MBSSID\_BACKUP\_VLAN: 「Backup VLANs cannot be configured if MBSSID is not enabled.%s not started.」

**説明** バックアップ VLAN を有効にするには、MBSSID モードを設定する必要があります。

**推奨処置** このデバイスで MBSSID を設定します。

**エラーメッセージ** IF-4-MISPLACED\_VLAN\_TAG: 「Detected a misplaced VLAN tag on source Interface %. Dropping packet.」

**説明** 受信された 802.1Q VLAN タグは表示されたインターフェイスで検出されましたが、正しく解析できませんでした。受信されたパケットのカプセル化、またはカプセル化解除は正しく行われていませんでした。

**推奨処置** なし。

**エラーメッセージ** DOT11-2-FW\_LOAD\_NET: 「Interface %s cannot load on boot.Place image in flash root directory and reload.」

**説明** アクセスポイントをブートしているときには、ネットワークから無線イメージはロードできません。

**推奨処置** このイメージを、フラッシュ ファイルシステムのルート ディレクトリに格納します。

**エラー メッセージ** DOT11-4-FW\_LOAD\_DELAYED: 「Interface %s, network filesys not ready.Delaying firmware (%s) load.」

**説明** 表示されたインターフェイスに新しいファームウェアをフラッシュしようとしたときに、ネットワーク ファイルシステムが実行されていなかったか、準備ができていませんでした。表示されたファームウェア ファイルのロードが遅れています。

**推奨処置** 新しいファームウェアのフラッシュを再試行する前に、ネットワークが立ち上がり、準備できていることを確認してください。

**エラー メッセージ** DOT11-3-FLASH\_UNKNOWN\_RADIO: 「Interface %s has an unknown radio.」

**説明** ユーザが新しいファームウェアを、表示されたインターフェイスにフラッシュしようとしたときに、無線のタイプを判断できませんでした。

**推奨処置** システムをリブートし、ファームウェアのアップグレードが完了するかどうかを確認してください。

**エラー メッセージ** DOT11-4-UPLINK\_ESTABLISHED: 「Interface %s associated to AP %s %e %s.」

**説明** 表示されたリピータは、表示されたルート アクセス ポイントにアソシエートされています。これで、表示されたリピータにクライアントをアソシエートし、トラフィックを通過させることができます。

**推奨処置** なし。

**エラー メッセージ** DOT11-2-UPLINK\_FAILED: 「Uplink to parent failed: %s.」

**説明** 表示された理由で親アクセス ポイントとの接続が失敗しました。アップリンクは接続の試行を停止します。

**推奨処置** アップリンク インターフェイスをリセットしてください。それでも問題が解決されない場合は、テクニカル サポートにお問い合わせください。

**エラー メッセージ** DOT11-4-CANT\_ASSOC: 「Interface %, cannot associate %s.」

**説明** 表示されたインターフェイス デバイスを、表示された親アクセス ポイントにアソシエートできませんでした。

**推奨処置** 親アクセス ポイントの設定とこの装置の設定が一致していることを確認してください。

**エラー メッセージ** DOT11-4-CANT\_ASSOC: 「Interface Dot11Radio 0, cannot associate.」

**説明** 親はクライアント MFP をサポートしていません。このエラー メッセージがアクセス ポイントに表示されるのは、ワークグループブリッジ、リピータ、または非ルートブリッジモードだけです。また、WGB、リピータ、非ルートが Client MFP SD 必須（または、強制）と設定されているが、ルート Client MFP が無効になっている場合に表示されます。

**推奨処置** 親アクセスポイントの設定とこの装置の設定が一致していることを確認してください。

**エラー メッセージ** DOT11-2-PROCESS\_INITIALIZATION\_FAILED: 「The background process for the radio could not be started: %s」

**説明** 表示されたインターフェイスで使用されている初期化プロセスが何らかの理由により失敗しました。一時的なエラーである可能性があります。

**推奨処置** アクセスポイントをリロードします。この操作により問題が解決されなかった場合は、電源を再投入します。それでも問題が解決されない場合は、アクセスポイントのファームウェアを前のバージョンにダウングレードします。

**エラー メッセージ** DOT11-2-RADIO\_HW\_RESET: 「Radio subsystem is undergoing hardware reset to recover from problem.」

**説明** ソフトリセットでは解決できない修復不可能なエラーが発生しました。

**推奨処置** なし。

**エラー メッセージ** DOT11-2-RESET\_RADIO: 「Interface %s, Radio %s, Trying hardware reset on radio.」

**説明** ソフトウェアリセットにより無線を起動しようとしたましたが、失敗しました。装置の無線すべてをリセットするために、ハードウェアリセットを試行しています。

**推奨処置** なし。

**エラー メッセージ** DOT11-4-MAXRETRIES: 「Packet to client %e reached max retries, removing the client.」

**説明** パケット送信試行回数の上限に達したため、クライアントの削除が行われています。このエラーメッセージは、アクセスポイントが、ある特定の回数、クライアントのポーリングを試みたが、応答を受信できなかったことを表しています。したがって、このクライアントはアソシエーションテーブルから削除されます。この問題は、クライアントとアクセスポイントがノイズの多い RF 環境で通信を試みたときによく発生します。

**推奨処置** この問題を解決するには、アクセスポイントでキャリア話中検索を実行して、スナップショットの無線スペクトラムにノイズが現れるかどうかを確認します。不要なノイズの軽減を試行します。詳細については、「[キャリア話中検索の実行](#)」(P.6-37)の手順を参照してください。1つのエリアに複数のアクセスポイントがある場合、チャンネル信号や、このエリアを取り囲むエリアにある他の無線デバイスとオーバーラップしている可能性があります。ネットワークインターフェイスの下のチャンネルを変更し、Radio-802.11 を選択します。オーバーラップしないチャンネルには、1、6、および 11 の 3 種類があります。

**エラー メッセージ** DOT11-4-RM\_INCAPABLE: 「Interface %s」

**説明** 表示されたインターフェイスは、無線管理機能をサポートしていません。

**推奨処置** なし。

**エラー メッセージ** DOT11-4-RM\_INCORRECT\_INTERFACE: 「Invalid interface, either not existing or non-radio.」

**説明** 無線管理要求により、このインターフェイスは存在しないか、無線インターフェイスではないことが検出されました。

**推奨処置** なし。

**エラー メッセージ** DOT11-3-POWERS\_INVALID: 「Interface %s, no valid power levels available.」

**説明** 無線ドライバは、有効な電力レベル設定を検出できませんでした。

**推奨処置** 電源および設定を調べ、訂正してください。

**エラー メッセージ** DOT11-4-RADIO\_INVALID\_FREQ: 「Operating frequency (%d) invalid - performing a channel scan.」

**説明** 表示された周波数は、操作には無効です。有効な周波数を選択するためにチャンネルスキャンが行われています。

**推奨処置** なし。

**エラー メッセージ** DOT11-4-RADIO\_NO\_FREQ: 「Interface &s, all frequencies have been blocked, interface not started.」

**説明** この操作に対して設定された周波数は無効です。有効な操作周波数を選択するために、チャンネルスキャンが行われています。

**推奨処置** なし。

**エラー メッセージ** DOT11-4-BCN\_BURST\_NO\_MBSSID: 「Beacon burst mode is enabled but MBSSID is not enabled, %s is down.」

**説明** ビーコンバーストモードは、表示されたインターフェイスで MBSSID が有効にされている場合にだけ有効にできます。

**推奨処置** 表示されたインターフェイスで MBSSID を有効にするか、ビーコンバーストを無効にしてください。



**エラーメッセージ** DOT11-4-BCN\_BURST\_TOO\_MANY\_DTIMS: 「Beacon burst mode is enabled and there are too many different DTIM periods defined.%s is down.」

**説明** ビーコンバーストモードでサポートできるのは最大4個の一意のDTIM値だけです。DTIM値1個につき、最大4個のBSSがあります。

**推奨処置** このインターフェイスで設定されているSSIDに対する一意のDTIM数をより妥当な値に変更します。

**エラーメッセージ** DOT11-2-RADIO\_INITIALIZATION\_ERROR: 「The radio subsystem could not be initialized (%s).」

**説明** 無線サブシステムの初期化を試みているときに、重大なエラーが検出されました。

**推奨処置** システムをリロードします。

**エラーメッセージ** DOT11-4-UPLINK\_NO\_ID\_PWD: 「Interface %s, no username/password supplied for uplink authentication.」

**説明** ユーザ名またはパスワード、もしくはその両方の入力に失敗しました。

**推奨処置** ユーザ名またはパスワード、もしくはその両方を入力して、もう一度実行してください。

**エラーメッセージ** DOT11-5-NO\_IE\_CFG: 「No IEs configured for %s (ssid index %u).」

**説明** 無線にビーコン、またはプローブ応答を適用しようとしたのですが、表示されたSSIDインデックスではこのビーコン、またはプローブは定義されていませんでした。

**推奨処置** IE設定を確認してください。

**エラーメッセージ** DOT11-4-FLASHING\_RADIO: 「Interface %s, flashing radio firmware (%s).」

**説明** 表示された新しいファームウェアをロードするために、表示されたインターフェイス無線が停止されました。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-LOADING\_RADIO: 「Interface %s, loading the radio firmware (%s).」

**説明** 表示された新しいファームウェアをロードするために、表示されたインターフェイス無線が停止されました。

**推奨処置** なし。

**エラーメッセージ** DOT11-2-NO\_FIRMWARE: 「Interface %s, no radio firmware file (%s) was found.」

**説明** 新しいファームウェアをフラッシュしようとしたますが、無線のファイルがフラッシュファイルシステムに見つかりませんでした。または、アクセスポイントのIOSが破損しています。

**推奨処置** 装置に誤ったイメージがロードされました。使用している無線のタイプに基づき、正しいイメージを探してください。この問題を解決するために、新しいCisco IOSイメージを使用して、アクセスポイントのリロードが必要な場合があります。イメージのリロード手順については、「[アクセスポイントのイメージのリロード](#)」(P.22-7)を参照してください。

アクセスポイントのIOSが破損している場合は、MODEボタン方式を使用して、アクセスポイントイメージをリロードします。「[MODEボタンの使用](#)」(P.22-4)を参照してください。

**エラーメッセージ** DOT11-2-BAD\_FIRMWARE: 「Interface %s, radio firmware file (%s) is invalid.」

**説明** 新しいファームウェアを、表示されたインターフェイスにフラッシュしようとしたときに、表示された無線ファームウェアファイルが無効であることがわかりました。

**推奨処置** 装置が予期している場所に、正しいファームウェアイメージファイルが存在することを確認します。

**エラーメッセージ** DOT11-2-RADIO\_FAILED: 「Interface %s, failed - %s.」

**説明** 表示されたインターフェイスの無線ドライバは重大なエラーを検出しました。表示された理由によりシャットダウンしています。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-FLASH\_RADIO\_DONE: 「Interface %s, flashing radio firmware completed.」

**説明** 表示されたインターフェイスの無線ファームウェアのフラッシュが終了しました。この無線は新しいファームウェアで再起動されます。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-UPLINK\_LINK\_DOWN: 「Interface %s, parent lost: %s.」

**説明** 表示されたインターフェイス上の親アクセスポイントへの接続は、表示された理由により失われました。装置は新しい親アクセスポイントを探そうとしています。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-CANT\_ASSOC: Cannot associate: \$s

**説明** 表示された理由により、装置は親アクセスポイントとの接続を確立できませんでした。

**推奨処置** 親アクセスポイントと装置の基本設定 (SSID、WEP など) が一致していることを確認します。

**エラーメッセージ** DOT11-4-CLIENT\_NOT\_FOUND: 「Client was not found.」

**説明** mic の確認中に、クライアントが見つかりませんでした。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client

**説明** クライアントに送信したパケットが何度も正常に届かず、最大再試行回数に達しました。このため、アソシエーションテーブルからこのクライアントが削除されました。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-BRIDGE\_LOOP: 「Bridge loop detected between WGB %e and device %e.」

**説明** 表示されたワークグループブリッジは、表示されたイーサネットクライアントのいずれか 1 つのアドレスを報告しましたが、アクセスポイントではこのアドレスはネットワーク上の別の場所としてすでにマークされています。

**推奨処置** アクセスポイントの GUI において [Associations] ページで [Refresh] をクリックするか、CLI で **clear dot11 statistics** コマンドを入力します。

**エラーメッセージ** DOT11-4-ANTENNA\_INVALID: 「Interface %s, current antenna position not supported, radio disabled.」

**説明** 表示された AIR-RM21A 無線モジュールは、高ゲイン位置の外部アンテナをサポートしません (高ゲイン位置のアンテナはアクセスポイントに対して平らに折り返します)。アクセスポイントは、アンテナが高ゲイン位置にあると自動的に無線を無効にします。

**推奨処置** AIR-RM21A 無線モジュールのアンテナを、アクセスポイントの本体に直角になるように折り返します。

**エラーメッセージ** DOT11-6-ANTENNA\_GAIN: 「Interface %s, antenna position/gain changed, adjusting transmitter power.」

**説明** アンテナゲインが変更されたため、許可される電力レベルのリストを調節する必要があります。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-DIVER\_USED: 「Interface %s Mcs rates 8-15 disabled due to only one transmit or receive antenna enabled.」

**説明** リストされているレートでは、少なくとも 2 つの送受信アンテナを有効にする必要があります。

**推奨処置** アクセス ポイントに少なくとも 2 つの送受信アンテナを設置し、有効にします。

**エラーメッセージ** DOT11-3-RF-LOOPBACK\_FAILURE: 「Interface %s Radio failed to pass RF loopback test.」

**説明** 表示されたインターフェイスに対する無線ループバック テストが失敗しました。

**推奨処置** なし。

**エラーメッセージ** DOT11-3-RF-LOOPBACK\_FREQ\_FAILURE: 「Interface %s failed to pass RF loopback test.」

**説明** 表示されたインターフェイスに対する、指定された周波数での無線ループバック テストが失敗しました。

**推奨処置** なし。

**エラーメッセージ** DOT11-7-AUTH\_FAILED: 「Station %e Authentication failed」

**説明** 表示されたステーションは、認証に失敗しました。

**推奨処置** 入力したユーザ名とパスワードが正しいこと、および認証サーバがオンラインであることを確認します。

**エラーメッセージ** DOT11-7-CCKM\_AUTH\_FAILED: 「Station %e CCKM authentication failed.」

**説明** 表示されたステーションは、Cisco Centralized Key Management (CCKM) 認証に失敗しました。

**推奨処置** WDS アクセス ポイントを使用するように設定されているアクセス ポイントのトポロジが機能していることを確認します。

**エラーメッセージ** DOT11-4-CCMP\_REPLAY: 「AES-CCMP TSC replay was detected on packet (TSC 0x%11x received from &e).」

**説明** フレームは、AES-CCMP TSC 再送を示しています。受信パケットにおける AES-CCMP TSC の再送は、ほとんどの場合、アクティブな攻撃を示します。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-CKIP\_MIC\_FAILURE: 「CKIP MIC failure was detected on a packet (Digest 0x%x) received from %e).」

**説明** フレームで、CKIP MIC エラーが検出されました。受信パケットにおける CKIP MIC エラーは、ほとんどの場合、アクティブな攻撃を示します。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-CKIP\_REPLAY: 「CKIP SEQ replay was detected on a packet (SEQ 0x%x) received from %e.」

**説明** フレームで、CKIP SEQ 再送が検出されました。受信パケットにおける CKIP SEQ の再送は、ほとんどの場合、アクティブな攻撃を示します。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-TKIP\_MIC\_FAILURE: 「Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x%11x) encrypted and protected by %s key.」

**説明** 表示されたペア キーを使用してローカルに復号化されたユニキャスト フレーム上で、表示されたステーションから、TKIP Michael MIC の失敗が検出されました。

**推奨処置** 受信パケットにおける Michael MIC の失敗は、ネットワークがアクティブな攻撃を受けていることを示している可能性があります。無線 LAN から潜在的な不正デバイスを探して削除します。このエラーは、クライアントの設定に誤りがあること、またはクライアントに障害があることを示している可能性もあります。

**エラーメッセージ** DOT11-4-TKIP\_MIC\_FAILURE\_REPORT: 「Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x0) encrypted and protected by %s key」

**説明** アクセスポイントは、表示されたステーションから EAPOL キーを受信しました。このキーは、このアクセスポイントによって送信されたパケット上で TKIP Michael MIC が失敗したことを、アクセスポイントに通知しています。

**推奨処置** なし。

**エラーメッセージ** DOT11-3-TKIP\_MIC\_FAILURE\_REPEATED: 「Two TKIP Michael MIC failures were detected within %s seconds on %s interface.The interface will be put on MIC failure hold state for next %d seconds」

**説明** 表示されたインターフェイスで、表示された時間内に 2 つの TKIP Michael MIC 障害が検出されました。これは通常、ネットワークがアクティブな攻撃を受けていることを示しているため、表示された時間、インターフェイスはホールドされます。このホールド時

間中は TKIP 暗号を使用するステーションのアソシエーションが解除され、ホールド時間が終了するまで再アソシエートできません。ホールド時間が終了したら、インターフェイスは通常どおり動作します。

**推奨処置** MIC 障害は通常、ネットワークがアクティブな攻撃を受けていることを示しています。無線 LAN から潜在的な不正デバイスを探して削除します。これが偽のアラームで、インターフェイスのホールド時間が長すぎる場合は、**countermeasure tkip hold-time** コマンドを使用してホールド時間を調整します。

**エラーメッセージ** DOT11-4-TKIP\_REPLAY: 「TKIP TSC replay was detected on a packet (TSC 0x%ssx received from %e).」

**説明** フレームで、TKIP TSC 再送が検出されました。受信パケットにおける TKIP TSC の再送は、ほとんどの場合、アクティブな攻撃を示します。

**推奨処置** なし。

**エラーメッセージ** DOT11-4-WLAN\_RESOURCE\_LIMIT: 「WLAN limit exceeded on interface %s and network-id %d.」

**説明** このアクセスポイントの VLAN または WLAN の数が上限の 16 個に達しました。

**推奨処置** アクセスポイントが、割り当てられたネットワーク ID がオンの RADIUS とのアソシエートを試行している場合は、静的 VLAN の設定を解除するか、数を減らします。

**エラーメッセージ** SOAP-3-WGB\_CLIENT\_VLAN\_SOAP: 「Workgroup Bridge Ethernet client VLAN not configured.」

**説明** ワークグループブリッジに装着されているクライアントデバイス用に設定されている VLAN がありません。

**推奨処置** ワークグループブリッジにアタッチされているクライアントデバイスに対応するように VLAN を設定します。

**エラーメッセージ** DOT11-4-NO\_VLAN\_NAME: 「VLAN name %s from RADIUS server is not configured for station %e.」

**説明** RADIUS サーバにより返された VLAN 名は、アクセスポイントで設定する必要があります。

**推奨処置** アクセスポイントで VLAN 名を設定します。

**エラーメッセージ** DOT11-4-NO\_VLAN\_ID: 「VLAN id %d from Radius server is not configured for station %e.」

**説明** RADIUS サーバにより返された VLAN ID は、アクセスポイントで設定する必要があります。

**推奨処置** アクセスポイントで VLAN ID を設定します。

**エラーメッセージ** SOAP-3-ERROR: 「Reported on line %d in file %s.%s.」

**説明** コントローラ ASIC の表示されたファイル名にある表示された行番号で、内部エラーが発生しました。

**推奨処置** なし。

**エラーメッセージ** SOAP\_FIPS-2-INIT\_FAILURE: 「SOAP FIPS initialization failure: %s.」

**説明** SOAP FIPS 初期化エラー。

**推奨処置** なし。

**エラーメッセージ** SOAP\_FIPS-4-PROC\_FAILURE: 「SOAP FIPS test failure: %s.」

**説明** SOAP FIPS テストの重大なエラー。

**推奨処置** なし。

**エラーメッセージ** SOAP\_FIPS-4-PROC\_WARNING: 「SOAP FIPS test warning: %s.」

**説明** SOAP FIPS テストの重大ではないエラー。

**推奨処置** なし。

**エラーメッセージ** SOAP\_FIPS-2-SELF\_TEST\_IOS\_FAILURE: 「IOS crypto FIPS self test failed at %s.」

**説明** IOS 暗号化ルーチンでの SOAP FIPS セルフ テストが失敗しました。

**推奨処置** IOS イメージをチェックします。

**エラーメッセージ** SOAP\_FIPS-2-SELF\_TEST\_RAD\_FAILURE: 「RADIO crypto FIPS self test failed at %s on interface %s %d.」

**説明** 無線暗号化ルーチンでの SOAP FIPS セルフ テストが失敗しました。

**推奨処置** 無線イメージをチェックします。

**エラーメッセージ** SOAP\_FIPS-2-SELF\_TEST\_IOS\_SUCCESS: 「IOS crypto FIPS self test passed.」

**説明** SOAP FIPS セルフ テストに合格しました。

**推奨処置** なし。

## ■ アクセスポイント間プロトコルメッセージ

**エラーメッセージ** SOAP\_FIPS-2-SELF\_TEST\_RAD\_SUCCESS: 「RADIO crypto FIPS self test passed on interface %s %d.」

**説明** 無線インターフェイスでの、SOAP FIPS セルフテストに合格しました。

**推奨処置** なし。

**エラーメッセージ** DOT11-6-MCAST\_DISCARD: 「%s mode multicast packets are discarded in %s multicast mode.」

**説明** ワークグループブリッジとして設定されているアクセスポイントは、クライアントモードではインフラストラクチャモードのマルチキャストパケットをドロップし、インフラストラクチャモードではクライアントモードのマルチキャストパケットをドロップします。

**推奨処置** なし。

## アクセスポイント間プロトコルメッセージ

**エラーメッセージ** DOT11-6-STANDBY\_ACTIVE: 「Standby to Active, Reason = %s (%d).」

**説明** 表示された理由により、アクセスポイントはスタンバイモードからアクティブモードに移行しています。

**推奨処置** なし。

**エラーメッセージ** DOT11-6-STANDBY\_REQUEST: 「Hot Standby request to shutdown radios from %e.」

**説明** このアクセスポイントのいずれかの無線インターフェイスでエラーが検出されたため、表示されたスタンバイアクセスポイントは、このアクセスポイントに無線インターフェイスのシャットダウンを要求しました。

**推奨処置** なし。

**エラーメッセージ** DOT11-6-ROGUE\_AP: 「Rogue AP %e reported.Reason: %s.」

**説明** ステーションは表示された理由で潜在的な不正アクセスポイントを報告しました。

**推奨処置** なし。



# ローカル認証サーバメッセージ

**エラーメッセージ** RADSRV-4-NAS\_UNKNOWN: Unknown authenticator: [ip-address]

**説明** ローカル Remote Authentication Dial-In User Service (RADIUS) サーバが認証要求を受信しましたが、その要求を転送した Network Access Server (NAS; ネットワーク アクセスサーバ) の IP アドレスを認識していません。

**推奨処置** 無線 LAN 上のすべてのアクセスポイントが、ローカル RADIUS サーバで NAS として設定されていることを確認します。

**エラーメッセージ** RADSRV-4-NAS\_KEYMIS: NAS shared key mismatch.

**説明** ローカル RADIUS サーバが認証要求を受信しましたが、メッセージ署名で、共有キーテキストが一致していないことが示されています。

**推奨処置** NAS またはローカル RADIUS サーバ上のいずれかで、共有キーの設定を修正します。

**エラーメッセージ** RADSRV-4\_BLOCKED: Client blocked due to repeated failed authentications

**説明** ユーザが、ブロックをトリガーするように設定されている回数の認証に失敗し、アカウントが無効となりました。

**推奨処置** `clear radius local-server user username` 特権 EXEC コマンドを使用してユーザを解除するか、または、設定したロックアウト時間によってユーザに対するブロックが期限切れとなるようにします。

**エラーメッセージ** DOT1X-SHIM-6-AUTH\_OK: 「Interface %s authenticated [%s].」

**説明** 802.1x 認証が正常に終了しました。

**推奨処置** なし。

**エラーメッセージ** DOT1X-SHIM-3-AUTH\_FAIL: 「Interface %s authentication failed.」

**説明** 装着されたデバイスの 802.1x 認証に失敗しました。

**推奨処置** クライアントおよび RADIUS サーバで、802.1x 認定証の設定をチェックします。

**エラーメッセージ** DOT1X-SHIM-3-INIT\_FAIL: 「Unable to init - %s.」

**説明** シムレイヤの初期化中にエラーが発生しました。

**推奨処置**

**エラーメッセージ** DOT1X-SHIM-3-UNSUPPORTED\_KM: 「Unsupported key management: %X.」

**説明** シムレイヤの初期化中にエラーが発生しました。サポートされていないキー管理タイプが検出されました。

**推奨処置** なし。

**エラーメッセージ** DPT1X-SHIM-4-PLUMB\_KEY\_ERR: 「Unable to plumb keys - %s.」

**説明** シムレイヤがキーを調べようとしたときに、予測していなかったエラーが発生しました。

**推奨処置** なし。

**エラーメッセージ** DOT1X-SHIM-3-PKT\_TX\_ERR: 「Unable to tx packet -%s.」

**説明** シムレイヤが dot1x パケットを送信しようとしたときに、予測していなかったエラーが発生しました。

**推奨処置** なし。

**エラーメッセージ** DOT1X-SHIM-3-ENCAP\_ERR: 「Packet encap failed for %e.」

**説明** シムレイヤが dot1x パケットを送信しようとしたときに、予測していなかったエラーが発生しました。パケットのカプセル化に失敗しました。

**推奨処置** なし。

**エラーメッセージ** DOT1X-SHIM-3-SUPP\_START\_FAIL: 「Unable to start supplicant on %s.」

**説明** 表示されたインターフェイスでシムレイヤが dot1x サプリカントを開始しようとしたときに、予測していなかったエラーが発生しました。

**推奨処置** なし。

**エラーメッセージ** DOT1X-SHIM=3-NO\_UPLINK: 「No uplink found for %s.」

**説明** dot11 インターフェイスで dot1x イベントまたはメッセージを処理している間に、アップリンクが予測されているが見つからないという状況に陥りました。

**推奨処置** なし。

**エラーメッセージ** Information Group rad\_acct: Radius server <ip address> is responding again (previously dead). Error Group acct: No active radius servers found. Id 106

**説明** このメッセージは、アクセスポイントで **radius-server deadtime 10** コマンドが設定されている場合に表示されます。このコマンドは、アクセスポイントが、応答しないサーバの使用を試行しない期間を設定するためのものです。したがって、要求がタイムアウトす

るまでに必要な時間を避けて、次の設定済みサーバを試行することができます。dead とマークされている RADIUS サーバは、すべてのサーバが dead とマークされていない限り、指定した期間（分単位）、その他の要求にもスキップされます。デッド タイムを 10 分間に設定するということは、このサーバを 10 分間使用できないことを意味します。

**推奨処置** このログを消去する必要がある場合は、このコマンドを無効にします。実際、このメッセージは大きな問題ではありません。単なる情報ログです。

## WDS メッセージ

**エラーメッセージ** WLCCP-WDS-6-REPEATER\_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.

**説明** リピータ アクセス ポイントは、WDS をサポートしません。

**推奨処置** なし。

**エラーメッセージ** WLCCP-WDS-6-PREV\_VER\_AP: A previous version of AP is detected.

**説明** WDS デバイスが、古いバージョンのアクセス ポイントを検出しました。

**推奨処置** なし。

**エラーメッセージ** WLCCP-AP-6-INFRA: WLCCP Infrastructure Authenticated

**説明** アクセス ポイントが、WDS デバイスの認証に成功しました。

**推奨処置** なし。

**エラーメッセージ** WLCCP-AP-6-STAND\_ALONE: Connection lost to WLCCP server, changing to Stand-Alone Mode

**説明** アクセス ポイントが WDS デバイスへの接続を失い、スタンドアロン モードになっています。

**推奨処置** なし。

**エラーメッセージ** WLCCP-AP-6-PREV\_VER\_WDS: A previous version of WDS is detected

**説明** アクセス ポイントが、古いバージョンの WDS を検出しました。

**推奨処置** ネットワーク上で、サポートされていないバージョンの WDS がないかどうかを確認します。

**エラーメッセージ** WLCCP-AP-6-UNSUP\_VER\_WDS: An unsupported version of WDS is detected

**説明** アクセスポイントが、サポートされていないバージョンの WDS を検出しました。

**推奨処置** ネットワーク上で、サポートされていないバージョンの WDS がないかどうかを確認します。

**エラーメッセージ** WLCCP-NM-3-WNM\_LINK\_DOWN: Link to WNM is down

**説明** ネットワーク マネージャが、keep-active メッセージに応答していません。

**推奨処置** ネットワーク マネージャ、またはネットワーク マネージャへのネットワークパスに問題がないか確認します。

**エラーメッセージ** WLCCP-NM-6-WNM\_LINK\_UP: Link to WNM is up

**説明** ネットワーク マネージャが、keep-active メッセージに応答するようになりました。

**推奨処置** なし。

**エラーメッセージ** WLCCP-NM-6-RESET: Resetting WLCCP-NM

**説明** ネットワーク マネージャ IP アドレスの変更、または一時的なリソース不足状態により、WDS ネットワーク マネージャ サブシステムがリセットされた可能性があります、間もなく動作は通常の状態に戻ります。

**推奨処置** なし。

**エラーメッセージ** WLCCP-WDS-3-RECOVER: 「%s」

**説明** WDS 正常回復エラー。

**推奨処置** なし。

## ミニ IOS メッセージ

**エラーメッセージ** MTS-2-PROTECT\_PORT\_FAILURE: An attempt to protect port [number] failed

**説明** ポートを保護しようとしたときに、初期化に失敗しました。

**推奨処置** なし。

**エラーメッセージ** MTS-2-SET\_PW\_FAILURE: Error %d enabling secret password.

**説明** ユーザがシークレット パスワードを有効にしようとしたときに、初期化に失敗しました。

**推奨処置** なし。

**エラーメッセージ** この設定を NVRAM に保存すると、NVRAM の最後に保存されたネットワーク管理やセキュリティ ファイルが破損する可能性があります。Continue?[no]:

**説明** この警告メッセージは、アクセスポイントの CLI 経由で設定変更を保存しようとしたときに、この CLI インターフェイスに表示されます。原因はフラッシュメモリの容量不足です。無線が故障すると、.rcore ファイルが作成されます。このファイルは、無線にファームウェアまたはハードウェアの問題があることを示しますが、ハードウェアの問題はあまり起こりません。

**推奨処置** この警告メッセージが表示されないようにするには、フラッシュメモリで生成された rcore ファイルを削除します。rcore ファイルの拡張子は .rcore です。このファイルは、無線がある時点でダウンしたことを示しているだけであるため、削除してもかまいません。rcore ファイルを CLI セッションに次のように表示することができます。

```
r15_5705_AB50_A8341F30.rcore
```

## アクセスポイントまたはブリッジについてのメッセージ

**エラーメッセージ** APBR-4-SEND\_PKT\_FAILED: Failed to Send Packet on port ifDescr (error= errornum)errornum: status error number

HASH(0x2096974)

**説明** アクセスポイント、またはブリッジがパケットの送信に失敗しました。この状態は、外部ノイズまたは干渉がある場合に見られることがあります。

**推奨処置** ノイズまたは干渉の発生源をチェックしてください。

**エラーメッセージ** APBR-6-DDP\_CLNT\_RESET: Detected probable reset of hosthost: host MAC address HASH(0x2080f04)

**説明** アクセスポイントまたはブリッジが、別のインフラストラクチャデバイスの再起動を検出しました。

**推奨処置** このメッセージが継続的に表示される場合は、アクセスポイントをリブートしてください。

## Cisco Discovery Protocol メッセージ

**エラーメッセージ** CDP\_PD-2-POWER\_LOW: %s - %s %s (%e)

**説明** システムに十分な電力が供給されていません。

**推奨処置** インライン パワーの供給源を再設定するか、交換してください。

## 外部 RADIUS サーバエラーメッセージ

**エラーメッセージ** RADUYS:response-authenticator decrypt fail, paklen 32

**説明** このエラーメッセージは、RADIUS サーバとアクセス ポイントの間で、RADIUS 共有キーが一致していないことを示しています。

**推奨処置** RADIUS サーバとアクセス ポイントで同じ共有キーが使用されていることを確認してください。

## LWAPP エラーメッセージ

**エラーメッセージ** LWAPP-3-CDP: Failure sending CDP Update to Controller.Reason "s"

**説明** アクセス ポイントの CDP アップデートをコントローラに送信できませんでした。

**推奨処置** なし。

**エラーメッセージ** LWAPP-3-CLIENTERRORLOG: "s"

**説明** このログメッセージは、LWAPP クライアントエラー イベントを示しています。このメッセージは、LWAPP アクセス ポイントの加入問題をトラブルシューティングしやすくするためにログに記録されています。

**推奨処置** なし。

**エラーメッセージ** LWAPP-3-CLIENTEVENTLOG: "s"

**説明** このログメッセージは、LWAPP クライアント通知イベントを示しています。このメッセージは、LWAPP アクセス ポイントの加入問題をトラブルシューティングしやすくするためにログに記録されています。

**推奨処置** なし。

**エラーメッセージ** LWAPP-3-UNSUPPORTEDDRM: Got unsupported CCX RM Measurement "s" request "d" from Controller.

**説明** コントローラから、サポートされていない CCX 無線管理測定が要求されました。

**推奨処置** なし。

**エラーメッセージ** LWAPP-5-WRONG\_DFS\_SLOT: DFS action on non-DFS radio "d"

**説明** 無線 b/g での DFS 処理

**推奨処置** なし。

## センサーメッセージ

**エラーメッセージ** SENSOR-3-TEMP\_CRITICAL: System sensor "d" has exceeded CRITICAL temperature thresholds

**説明** 環境テストの測定値の 1 つが、最大しきい値を超えています。

**推奨処置** 指定された状況を解決してください。解決できなかった場合、予防措置として、システムが、システム自身をシャットダウンすることがあります。原因が温度または電圧にあるかどうかを確認するには、**show environment all** と入力します。これが温度に対する重大な警告である場合は、ルータのファンが動作していること、および部屋の冷却および空調が機能していることを確認してください。この状況により、システムが適切に動作できなくなることがあります。

**エラーメッセージ** SENSOR-3-TEMP\_NORMAL: "s" temperature sensor is now normal

**説明** 環境テストの測定値の 1 つが、通常の動作温度を下回っています。

**推奨処置** なし。

**エラーメッセージ** SENSOR-3-TEMP\_SHUTDOWN: Shutting down the system because of dangerously HIGH temperature at sensor "d".

**説明** 環境テストの測定値の 1 つが、ルータの動作温度環境を超えています。

**推奨処置** 高温の原因を調べます。

**エラーメッセージ** SENSOR-3-TEMP\_WARNING: "s" temperature sensor "d" has exceeded WARNING temperature thresholds

**説明** 環境テストの測定値の 1 つが、警告のしきい値を超えています。

**推奨処置** 状況を注意深くモニタし、可能であれば、環境を冷却して改善します。

**エラーメッセージ** SENSOR-3-VOLT\_CRITICAL: System sensor "d" has exceeded CRITICAL voltage thresholds

**説明** 環境テストの測定値の 1 つが、電圧の最大しきい値を超えています。

**推奨処置** 指定された状況を解決してください。解決できなかった場合、予防措置として、システムが、システム自身をシャットダウンすることがあります。原因が電圧にあるかどうかを確認するには、**show environment all** と入力します。この状況により、システムが適切に動作できなくなることがあります。

**エラーメッセージ** SENSOR-3-VOLT\_NORMAL: System sensor "d" ("d") is now operating under NORMAL voltage

**説明** 測定された環境テスト ポイントの 1 つが、正常な動作温度を下回っています。

**推奨処置** なし。

**エラーメッセージ** SENSOR-3-VOLT\_WARNING: Voltage monitor "d" ("d") has exceeded voltage thresholds

**説明** 電圧テストの測定値の 1 つが、電圧が標準範囲外にあることを示しています。

**説明** 電源をチェックするか、または TAC にお問い合わせください。

## SNMP エラーメッセージ

**エラーメッセージ** SNMP-3-AUTHFAILIPV6: Authentication failure for SNMP request from hostUnrecognized format '%P'

**説明** このホストにより、適切に認証されていない SNMP 要求が送信されました。

**推奨処置** SNMP 要求で使用されているコミュニティまたはユーザ名がルータで設定されていること確認してください。

**エラーメッセージ** SNMP-3-INPUT\_QFULL\_ERR: Packet dropped due to input queue full

**説明** 入力キューがいっぱいであるため、SNMP パケットがドロップされました。

**推奨処置** コマンド **show snmp** を使用して、ドロップされたパケットの数を確認します。エラー状態が解消されるまで、このデバイスに対する SNMP アクセスをすべて停止します。



**エラーメッセージ** SNMP-3-INTERRUPT\_CALL\_ERR: "s" function, cannot be called from interrupt handler

**説明** このメッセージは、この関数に対して、割り込みハンドラからコールが行われたことを示しています。コールが失敗し、デバイスが、malloc コールのスタックの下方でリポートされるため、このようなコールは許可されません。

**推奨処置** このメッセージが繰り返し現れる場合は、表示されるとおりに書き写し、テクニカル サポート 担当者に報告してください。

**エラーメッセージ** SNMP-4-NOENGINEIDV6: Remote snmpEngineID for Unrecognized format '%P' not found when creating user: "s"

**説明** ユーザを作成しようとしたのですが、失敗しました。リモート エージェント（または、SNMP マネージャ）のエンジン ID が設定されていなかった可能性があります。

**推奨処置** リモート snmpEngineID を設定し、ユーザを再設定します。同じ問題が続く場合は、出力されたエラーメッセージをそのままコピーし、シスコのテクニカル サポートに提出してください。

**エラーメッセージ** SNMP\_MGR-3-MISSINGHOSTIPV6: Cannot locate information on SNMP informs host:Unrecognized format '%P'

**説明** この SNMP の応答要求の宛先となるテーブル エントリが見つかりません。したがって、応答要求型通知はこの宛先に送信されません。

**推奨処置** show snmp host コマンド、および show snmp コマンドを実行します。エラーメッセージ、および show コマンドからの出力を表示されているとおりに書き写し、テクニカル サポート 担当者に報告してください。snmp-server host コンフィギュレーション コマンドを使用して、応答要求の宛先を削除し、再度追加することにより、この状態が解消されることがあります。解消されない場合は、システムの再ロードが必要になる可能性があります。

## SSH エラーメッセージ

**エラーメッセージ** SSH-5-SSH2\_CLOSE: SSH2 Session from "%s" (tty = "%d") for user "%s" using crypto cipher "%s", hmac "%s" closed

**説明** SSH セッションの終了情報

**推奨処置** なし - 情報のみのメッセージです。

**エラーメッセージ** SSH-5-SSH2\_SESSION: SSH2 Session request from "%s" (tty = "%d") using crypto cipher "%s", hmac "%s" "%s"

**説明** SSH セッションの要求情報

**推奨処置** なし - 情報のみのメッセージです。

**エラーメッセージ** SSH-5-SSH2\_USERAUTH: User `''%s''` authentication for SSH2 Session from `%s` (tty = `%d`) using crypto cipher `''%s''`, hmac `''%s''` `%s`

**説明** SSH ユーザ認証ステータス情報

**推奨処置** なし - 情報のみのメッセージです。

**エラーメッセージ** SSH-5-SSH\_CLOSE: SSH Session from `%s` (tty = `%d`) for user `''%s''` using crypto cipher `''%s''` closed

**説明** SSH セッションの終了情報

**推奨処置** なし - 情報のみのメッセージです。

**エラーメッセージ** SSH-5-SSH\_SESSION: SSH Session request from `%s` (tty = `%d`) using crypto cipher `''%s''` `%s`

**説明** SSH セッションの要求情報

**推奨処置** なし - 情報のみのメッセージです。

**エラーメッセージ** SSH-5-SSH\_USERAUTH: User `''%s''` authentication for SSH Session from `%s` (tty = `%d`) using crypto cipher `''%s''` `%s`

**説明** SSH ユーザ認証ステータス情報

**推奨処置** なし - 情報のみのメッセージです。



## 用語集

- 4 位相偏移変調** IEEE 802.11b 準拠の無線 LAN で、2Mbps の伝送に使用される変調技術。
- 802.11** 2.4GHz 周波数帯で稼働する 1Mbps および 2Mbps 無線 LAN に対するキャリア検知メディア アクセス コントロールと物理層の規格を定めている IEEE 規格。
- 802.11a** 5GHz 周波数帯で稼働する無線 LAN に対するキャリア検知メディア アクセス コントロールと物理層の規格を定めている IEEE 規格。
- 802.11b** 2.4GHz 周波数帯で稼働する 5.5Mbps および 11Mbps 無線 LAN に対するキャリア検知メディア アクセス コントロールと物理層の規格を定めている IEEE 規格。
- 802.11g** 2.4GHz 周波数帯で稼働する 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、および 54Mbps LAN に対するキャリア検知メディア アクセス コントロールと物理層の規格を定めている IEEE 規格。
- 802.3af** Power over Ethernet (PoE) のメカニズムを定めている IEEE 規格。この規格は、標準のイーサネット ケーブル配線を介して電力およびデータの両方を提供する機能を規定します。

## B

- beacon** 無線デバイスのアベイラビリティと存在を信号で通知する無線 LAN パケット。ビーコン パケットはアクセス ポイントおよびベース ステーションから送信されますが、コンピュータ対コンピュータ (アドホック) モードで実行されている場合は、クライアントの無線カードから送信されます。
- BOOTP** ブート プロトコル。ネットワーク上のデバイスに静的に IP アドレスを割り当てる際に使用されるプロトコルです。
- BPSK** IEEE 802.11b 準拠の無線 LAN で、1Mbps の伝送に使用される変調技術です。

## C

- CCK** Complementary Code Keying (相補コードキー入力)。IEEE 802.11b 準拠の無線 LAN で、5.5Mbps および 11Mbps の伝送に使用される変調技術。

<b>CCKM</b>	Cisco Centralized Key Management。CCKM を使用すると、認証されているクライアント デバイスは、あるアクセス ポイントから別のアクセス ポイントへ、再アソシエーションの際にほとんど遅延を感じることなくローミングできます。ネットワーク上のアクセス ポイントは、Wireless Domain Service (WDS; 無線ドメイン サービス) を提供し、サブネット上の CCKM 対応クライアント デバイスに対してセキュリティ クレデンシャルのキャッシュを生成します。WDS アクセス ポイントのクレデンシャルのキャッシュにより、CCKM 対応クライアント デバイスが新しいアクセス ポイントにローミングする際に発生する再アソシエーションに必要な時間が大幅に短縮されます。
<b>CSMA</b>	Carrier Sense Multiple Access (キャリア検知多重アクセス)。IEEE 802.11 規格で定められた無線 LAN のメディア アクセス手段です。
<b>D</b>	
<b>dBi</b>	アンテナ ゲインの測定に一般的に使用されるデシベルと等方性アンテナの比率。dBi の値が大きいほどゲインが高く、対応角度が鋭角になります。
<b>DHCP</b>	Dynamic Host Configuration Protocol。多数のオペレーティング システムで使用でき、ネットワーク上のデバイスに指定範囲内の IP アドレスを自動発行するプロトコル。割り当てられたアドレスは、管理者が指定した一定の期間、デバイスに保持されます。
<b>DNS</b>	Domain Name System (ドメイン ネーム システム) サーバ。テキスト名を IP アドレスに変換するサーバ。英数字のホスト名とそれらに対応する IP アドレスが登録されたデータベースを保持します。
<b>DSSS</b>	Direct Sequence Spread Spectrum (ダイレクト シーケンス スペクトラム 拡散方式)。スペクトラム 拡散方式の無線送信の一種。その信号を、広範な周波数帯に連続して送信します。
<b>E</b>	
<b>EAP</b>	Extensible Authentication Protocol。オプションの IEEE 802.1x セキュリティ機能。大規模なユーザ ベースを持ち、EAP 対応の Remote Authentication Dial-In User Service (RADIUS) サーバにアクセスする組織に最適なプロトコルです。
<b>G</b>	
<b>gateway</b>	2 つの互換性のないネットワークを接続するデバイス。
<b>GHz</b>	ギガヘルツ。10 億サイクル / 秒。周波数の測定単位です。

## I

- IEEE** Institute of Electrical and Electronic Engineers (米国電気電子技術者協会)。出版物、会議、規格策定などの活動を通じて、電気技術者を支援する専門家団体です。イーサネットの 802.3 規格および無線 LAN の 802.11 規格を策定します。
- IP アドレス** ステーションのインターネット プロトコル (IP) アドレス。
- IP サブネット マスク** IP サブネットワークの識別に使用される番号。IP アドレスが LAN で認識可能かどうか、あるいは、ゲートウェイ経由で到達させる必要があるかどうかを示します。この番号は、255.255.255.0 のように IP アドレスと同様の形式で表されます。

## M

- MAC** Media Access Control (メディア アクセス コントロール) アドレス。イーサネット データ パケットで、アクセス ポイントやクライアント アダプタなどのイーサネット デバイスを識別するために使用される 48 ビットの一意な番号です。

## O

- Orthogonal Frequency Division Multiplex (OFDM; 直交周波数分割多重方式)** IEEE 802.11a 準拠の無線 LAN で、6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、および 54Mbps の伝送に使用される変調技術。

## R

- range** トランスミッタが信号を送信できる直線距離。
- RF** Radio Frequency (無線周波数)。無線を使用したテクノロジーに使用される一般用語です。
- RP-TNC** Cisco Aironet の無線機器とアンテナに特有のコネクタ タイプ。スペクトラム拡散デバイスに関する FCC 規則の Part 15.203 では、送信機器で使用できるアンテナのタイプが制限されています。この規則に適合するため、Cisco Aironet では、他のすべての無線 LAN プロバイダーの製品と同様に、無許可のアンテナを無線機器に取り付けることができないよう、無線装置とアンテナに固有のコネクタを使用しています。

**S**

**SSID** Service Set Identifier (サービスセット ID)。「無線ネットワーク名」とも呼ばれます。無線ネットワークの識別に使用され、ステーションで相互通信やアクセスポイントとの通信に必要とされる一意の識別子。SSIDには、最大 32 文字の英数字を使用できます。

**U**

**UNII** Unlicensed National Information Infrastructure。5.15 ~ 5.35GHz および 5.725 ~ 5.825GHz 周波数帯で稼働する UNII デバイスに関する規制です。

**UNII-1** 5.15 ~ 5.25GHz 周波数帯で稼働する UNII デバイスに関する規制。

**UNII-2** 5.25 ~ 5.35GHz 周波数帯で稼働する UNII デバイスに関する規制。

**UNII-3** 5.725 ~ 5.825GHz 周波数帯で稼働する UNII デバイスに関する規制。

**W**

**WDS** Wireless Domain Service (WDS; 無線ドメイン サービス)。無線 LAN で WDS を提供するアクセスポイントは、無線 LAN の CCKM 対応クライアント デバイスに対するクレデンシャルのキャッシュを維持します。CCKM 対応クライアントが、1 つのアクセスポイントから別のアクセスポイントにローミングする場合、WDS アクセスポイントは、マルチキャスト キーを持つ新しいアクセスポイントに、クライアントのクレデンシャルを転送します。クライアントと新しいアクセスポイントとの間で渡されるパケットは 2 つだけであるため、再アソシエーションの時間が大幅に短縮されます。

**WEP** Wired Equivalent Privacy (有線と同等のプライバシー)。IEEE 802.11 規格で定められているオプションのセキュリティ メカニズムです。ケーブルと同等のリンク完全性を無線デバイスで実現します。

**WLSE** Wireless LAN Solutions Engine。WLSE は Cisco Aironet 無線 LAN インフラストラクチャを管理するための専用のアプライアンスです。顧客が定義したグループ内のアクセスポイントを中央から識別および設定し、スループットとクライアントのアソシエーションに関してレポートします。WLSE の集中管理機能は、統合テンプレートベースの設定ツールでさらに拡張され、設定の簡易化と生産性の向上を実現します。

**WNM** Wireless Network Manager (無線ネットワーク マネージャ)。

**WPA** Wi-Fi Protected Access (WPA) は、既存および将来の無線 LAN システムのデータ保護とアクセスコントロールの水準を大幅に向上させる、標準規格に基づく相互運用性の優れたセキュリティ拡張機能です。WPA は、現在策定中の IEEE 802.11i 規格のサブセットで、この規格と互換性があります。WPA では、データ保護に Temporal Key Integrity Protocol (TKIP) を使用し、認証済みキー管理に 802.1X を使用しています。

## あ

<b>アクセス ポイント</b>	電波を使用して、有線ネットワークと無線ステーションを接続する無線 LAN データ トランシーバ。
<b>アソシエート</b>	ステーションがアクセス ポイントと無線通信できるように適切に設定されること。
<b>アドホック ネットワーク</b>	アクセス ポイントを使用せずに、ステーションだけで構成された無線ネットワーク。
<b>アンテナ ゲイン</b>	一定圏内で無線エネルギーをある方向へ収束させるアンテナの能力を示す測定値。アンテナ ゲインが高いほど、特定の方向により収束された放射パターンとなります。

## い

<b>イーサネット</b>	最も広く使用されている有線のローカル エリア ネットワーク。キャリア 検知多重アクセス (CSMA) を使って複数のコンピュータによるネットワークの共有を可能にし、使用されている物理層に応じて 10Mbps、100Mbps、または 1000Mbps での動作を実現します。
<b>インフラストラクチャ</b>	有線イーサネット ネットワーク。

## く

<b>クライアント</b>	アクセス ポイントのサービスを使用して、ローカル エリア ネットワーク上で他のデバイスと無線通信を行う無線デバイス。
---------------	--

## し

<b>受信機感度</b>	受信機が受信し、正しくデータに変換することができる最も弱い信号の測定値。
--------------	--------------------------------------

## す

<b>スペクトラム拡散方式</b>	他の方式よりも広帯域幅にユーザ情報を拡散する無線送信テクノロジー。耐干渉性が向上し、無資格での運用が可能になるという利点を得るために必要なテクノロジーです。
<b>スロット時間</b>	コリジョンの後、パケットの再送信の前に、デバイスが待機する時間。スロット時間が短いと、バックオフ時間も短くなり、スループットが向上します。

## せ

**セル** 無線デバイスがベースステーションと通信できる無線範囲（カバレッジ）。セルのサイズは、転送速度、使用されるアンテナの種類、物理的な環境、およびその他の要因によって決まります。

**全方向性** 通常は、基本的に円状のアンテナ放射パターンを指します。

**送信電力** 無線送信の電力レベル。

## た

**ダイポール** 2つの素子（内部の場合もあり）で構成される低ゲイン（2.2dBi）アンテナの一種。

## て

**データレート** デバイスによってサポートされているデータ転送レートの範囲。データレートはメガビット/秒（Mbps）で測定されます。

## と

**等方性** 球形に信号を放射するアンテナ。

**ドメイン名** ネットワークまたはネットワークリソースのグループを示すテキストの名前。name.com（企業）、name.edu（教育関連組織）、name.gov（政府関連組織）、ISPname.net（ISPなどのネットワークプロバイダー）、name.ar（アルゼンチン）、name.au（オーストラリア）など、組織のタイプや地域ごとに付けられます。

## は

**パケット** ネットワーク上の通信に使用される基本的なメッセージ単位。パケットには通常、ルーティング情報とデータが含まれ、場合に応じてエラー検出情報が含まれます。

**バックオフ時間** LANにパケットを送信する前に、ステーションが待機するランダムな長さの時間。バックオフ時間はスロット時間の倍数であるため、スロット時間を短縮すると、結果として、バックオフ時間も短縮され、スループットが向上します。

## ふ

**ファームウェア** メモリチップにプログラミングされているソフトウェア。



<b>ファイルサーバ</b>	ファイル、メール、プログラムなどをローカルエリア ネットワークで共有するためのファイル用リポジトリ。
<b>ブロードキャスト パケット</b>	同一サブネット上のすべてのアドレスに送信される単一のデータ メッセージ (パケット)。
<b>へ</b>	
<b>変調</b>	ユーザ情報とトランスミッタのキャリア信号を組み合わせる数種類の技法。
<b>ま</b>	
<b>マルチキャスト パケット</b>	複数のアドレスに送信される単一のデータ メッセージ (パケット)。
<b>マルチパス</b>	無線信号が物体に当たって跳ね返ることで発生するエコー。
<b>ゆ</b>	
<b>ユニキャスト パケット</b>	特定の IP アドレスに送信される単一のデータ メッセージ (パケット)。
<b>ろ</b>	
<b>ローミング</b>	複数のアクセス ポイントを使用して、ユーザが LAN への連続した接続を維持したまま構内を移動できるようにする機能。
<b>わ</b>	
<b>ワークステーション</b>	クライアント アダプタが搭載されたコンピューティング デバイス。

