



Cisco Wireless Controller コンフィギュレーションガイド、リリース 8.2

初版：2015年11月03日

最終更新：2016年01月06日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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: <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)

© 2015 Cisco Systems, Inc. All rights reserved.



目次

はじめに ii

対象読者 ii

表記法 ii

関連資料 iii

Obtaining Documentation and Submitting a Service Request iii

システム管理 1

概要 3

シスコ ワイヤレスの概要 3

 シングルコントローラ展開 4

 マルチコントローラ展開 5

オペレーティング システム ソフトウェア 6

オペレーティング システムのセキュリティ 6

レイヤ 2 およびレイヤ 3 の動作 7

 動作上の要件 8

 設定要件 8

Cisco ワイヤレス LAN コントローラ 8

 クライアント ロケーション 9

コントローラ プラットフォーム 9

 Cisco 2500 シリーズ コントローラ 9

 Cisco 5500 シリーズ コントローラ 9

 Cisco Flex 7500 シリーズ コントローラ 10

 Cisco 8500 シリーズ コントローラ 10

 Cisco Virtual Wireless LAN Controller 11

 Cisco ワイヤレス サービス モジュール 2 11

 Cisco Services Ready Engine (SRE) の Cisco Wireless Controller 12

Cisco UWN ソリューション無線 LAN 12

ファイル転送	13
イーサネット経由の電源供給	13
Cisco Wireless LAN Controller のメモリ	13
Cisco Wireless LAN Controller のフェールオーバーの保護	14
使用する前に	15
設定ウィザードを使用したコントローラの設定	15
コントローラのコンソール ポートの接続	16
コントローラの設定 (GUI)	17
コントローラの設定 : CLI 設定ウィザードの使用	28
コントローラ Web GUI の使用方法	32
注意事項および制約事項	32
Web GUI へのログイン	33
GUI からのログアウト	33
Web モードおよびセキュア Web モードの有効化	33
Web モードおよびセキュア Web モードの有効化 (GUI)	33
Web モードおよびセキュア Web モードの有効化 (CLI)	34
外部で生成した SSL 証明書のロード	35
外部で生成した SSL 証明書について	35
SSL 証明書のロード (GUI)	36
SSL 証明書のロード (CLI)	37
コントローラ CLI の使用方法	38
コントローラ CLI へのログイン	39
注意事項および制約事項	39
ローカル シリアル接続の使用方法	39
リモート イーサネット接続の使用方法	40
CLI からのログアウト	41
CLI のナビゲーション	41
設定のないコントローラでの AutoInstall 機能の使用	42
AutoInstall 機能について	42
注意事項および制約事項	43
DHCP による IP アドレスの入手、および TFTP サーバからの設定ファイルの ダウンロード	43

設定ファイルの選択	44
AutoInstall の操作例	45
コントローラのシステムの日時の管理	46
コントローラのシステムの日時について	46
注意事項および制約事項	46
日時を取得するための NTP サーバの設定	46
NTP 認証の設定 (GUI)	47
NTP 認証の設定 (CLI)	47
日時の設定 (GUI)	48
日時の設定 (CLI)	49
Telnet および Secure Shell セッションの設定	51
Telnet と SSH について	51
Telnet および SSH の制約事項	51
Telnet および SSH セッションの設定 (GUI)	52
Telnet および SSH セッションの設定 (CLI)	53
指定した管理ユーザの Telnet の権限の設定 (GUI)	55
指定した管理ユーザの Telnet の権限の設定 (CLI)	55
Telnet または SSH_old を使用したアクセス ポイントのトラブルシューティング	55
Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (GUI)	56
Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (CLI)	56
コントローラの無線管理	57
ワイヤレス接続の有効化 (GUI)	57
ワイヤレス接続の有効化 (CLI)	58
ライセンスの管理	59
ライセンスのインストールおよび設定	59
ライセンスのインストールおよび設定に関する情報	59
ライセンスの使用に関する制限	60
アップグレードライセンスまたはキャパシティ Adder ライセンスの取得	61

アップグレードライセンスまたはキャパシティ Adder ライセンスの取得に関する情報	61
PAK 証明書の取得と登録	62
ライセンスのインストール	63
ライセンスのインストール (GUI)	63
ライセンスのインストール (CLI)	63
ライセンスの表示	64
ライセンスの表示 (GUI)	64
ライセンスの表示 (CLI)	65
サポートされるアクセス ポイントの最大数の設定	68
サポートされるアクセス ポイントの最大数の設定 (GUI)	68
サポートされるアクセス ポイントの最大数の設定 (CLI)	68
ライセンスの問題のトラブルシューティング	68
ap-count 評価ライセンスのアクティブ化	69
ap-count 評価ライセンスのアクティブ化に関する情報	69
ap-count 評価ライセンスのアクティブ化 (GUI)	69
ap-count 評価ライセンスのアクティブ化 (CLI)	70
使用権ライセンスの設定	71
使用権ライセンスに関する情報	71
使用権ライセンスの設定 (GUI)	73
使用権ライセンスの設定 (CLI)	73
ライセンスの再ホスト	73
ライセンスの再ホストについて	74
ライセンスの再ホスト	74
ライセンスの再ホスト (GUI)	74
ライセンスの再ホスト (CLI)	76
RMA 後にライセンスを交換コントローラに転送する	77
RMA 後の交換コントローラへのライセンスの転送について	77
RMA 後の交換コントローラへのライセンスの転送	78
802.11 帯域の設定	79
802.11 帯域の設定	79
802.11 帯域の設定について	79

802.11 帯域の設定 (GUI)	80
802.11 帯域の設定 (CLI)	81
帯域選択の設定	84
帯域選択の設定について	84
帯域選択の制約事項	84
帯域選択の設定	85
帯域選択の設定 (GUI)	85
帯域選択の設定 (CLI)	86
802.11 パラメータの設定	87
802.11n パラメータの設定	87
802.11n パラメータの設定について	87
802.11n パラメータの設定 (GUI)	88
802.11n パラメータの設定 (CLI)	89
802.11h のパラメータの設定	91
802.11h パラメータの設定について	91
802.11h のパラメータの設定 (GUI)	91
802.11h のパラメータの設定 (CLI)	92
802.11ac パラメータの設定	93
802.11ac パラメータの設定に関する情報	93
802.11ac サポートの制約事項	94
802.11ac 高スループットパラメータの設定 (GUI)	94
802.11ac 高スループットパラメータの設定 (CLI)	95
DHCP プロキシの設定	97
DHCP プロキシの設定について	97
DHCP プロキシの使用に関する制限	98
DHCP プロキシの設定 (GUI)	98
DHCP プロキシの設定 (GUI)	98
DHCP プロキシの設定 (CLI)	99
DHCP プロキシの設定 (CLI)	99
DHCP タイムアウトの設定 (GUI)	100
DHCP タイムアウトの設定 (CLI)	100
[DHCP Link Select] および [VPN Select] の設定	101

[DHCP Link Select] および [VPN Select] の設定の前提条件	101
[DHCP Link Select] と [VPN Select] の設定について	101
DHCP Link Select	102
DHCP VPN Select	102
モビリティに関する考慮事項	102
[DHCP Link Select] および [VPN Select] の設定 (CLI)	103
[DHCP Link Select] および [VPN Select] の設定 (GUI)	104
SNMP の設定	107
SNMP の設定 (CLI)	107
SNMP コミュニティ ストリング	109
SNMP コミュニティ ストリングのデフォルト値の変更 (GUI)	110
SNMP コミュニティ ストリングのデフォルト値の変更 (CLI)	110
リアルタイム統計情報の設定 (CLI)	111
SNMP トラップの拡張	111
アグレッシブ ロード バランシングの設定	113
アグレッシブ ロード バランシングの設定について	113
アグレッシブなロード バランシングの設定 (GUI)	114
アグレッシブなロード バランシングの設定 (CLI)	115
高速 SSID 変更の設定	117
高速 SSID 変更の設定について	117
高速 SSID 変更の設定 (GUI)	117
高速 SSID 変更の設定 (CLI)	118
802.3 ブリッジの設定	119
802.3 ブリッジの設定	119
802.3 ブリッジの設定について	119
802.3 ブリッジの制限	119
802.3 ブリッジの設定	120
802.3 ブリッジの設定 (GUI)	120
802.3 ブリッジの設定 (CLI)	120
802.3X のフロー制御の有効化	120
マルチキャストの設定	121
マルチキャスト モードの設定	121
マルチキャスト モードについて	121

マルチキャスト モード設定の制限	123
マルチキャスト モードの有効化 (GUI)	125
マルチキャスト モードの有効化 (CLI)	125
マルチキャスト グループの表示 (GUI)	127
マルチキャスト グループの表示 (CLI)	127
アクセス ポイントのマルチキャスト クライアント テーブルの表示 (CLI)	128
マルチキャスト ドメイン ネーム システムの設定	128
マルチキャスト ドメイン ネーム システムについて	128
マルチキャスト DNS の設定の制限	131
マルチキャスト DNS の設定 (GUI)	131
マルチキャスト DNS の設定 (CLI)	133
クライアント ローミングの設定	137
クライアント ローミングについて	137
コントローラ間ローミング	137
コントローラ内ローミング	138
サブネット間ローミング	138
VoIP による通話ローミング	138
CCX レイヤ 2 クライアント ローミング	139
注意事項および制約事項	140
CCX クライアント ローミング パラメータの設定 (GUI)	140
CCX クライアント ローミング パラメータの設定 (CLI)	141
CCX クライアント ローミング情報の取得 (CLI)	141
CCX クライアント ローミング問題のデバッグ (CLI)	142
IP-MAC アドレス バインディングの設定	143
IP-MAC アドレス バインディングの設定について	143
IP-MAC アドレス バインディングの設定 (CLI)	144
Quality of Service の設定	145
Quality of Service の設定	145
QoS について	145
Quality of Service プロファイルの設定	146
QoS プロファイルの設定 (GUI)	146
QoS プロファイルの設定 (CLI)	148

Quality of Service ロールの設定	149
Quality of Service ロールについて	149
QoS ロールの設定	150
QoS の設定 (GUI)	150
QoS ロールの設定 (CLI)	151
Application Visibility and Control の設定	153
Application Visibility and Control について	153
Application Visibility and Control の制限	154
Application Visibility and Control の設定 (GUI)	154
Application Visibility and Control の設定 (CLI)	156
NetFlow の設定	157
NetFlow 情報	157
NetFlow の設定 (GUI)	157
NetFlow の設定 (CLI)	158
メディアおよび EDCA パラメータの設定	159
音声パラメータとビデオパラメータの設定	159
音声パラメータとビデオパラメータの設定について	159
コールアドミッション制御	160
帯域幅ベースの CAC	160
負荷ベース CAC	160
Expedited Bandwidth Requests	161
U-APSD	162
Traffic Stream Metrics	162
音声パラメータの設定	163
音声パラメータの設定 (GUI)	163
音声パラメータの設定 (CLI)	165
ビデオパラメータの設定	166
ビデオパラメータの設定 (GUI)	166
ビデオパラメータの設定 (CLI)	167
音声設定とビデオ設定の表示	168
音声設定とビデオ設定の表示 (GUI)	168
音声設定とビデオ設定の表示 (CLI)	169
SIP ベースの CAC の設定	173

SIP ベースの CAC の制限	173
SIP ベースの CAC の設定 (GUI)	173
SIP ベースの CAC の設定 (CLI)	174
メディア パラメータの設定	175
メディア パラメータの設定 (GUI)	175
優先コール番号を使用した音声優先制御の設定	176
優先コール番号を使用した音声優先制御の設定について	176
優先コール番号を使用した音声優先制御の設定の前提条件	176
優先コール番号の設定 (GUI)	176
優先コール番号の設定 (CLI)	177
EDCA パラメータの設定	177
EDCA パラメータについて	177
EDCA パラメータの設定 (GUI)	178
EDCA パラメータの設定 (CLI)	179
Cisco Discovery Protocol の設定	181
Cisco Discovery Protocol の設定について	181
Cisco Discovery Protocol の設定に関する制限	181
Cisco Discovery Protocol の設定	183
Cisco Discovery Protocol の設定 (GUI)	183
Cisco Discovery Protocol の設定 (CLI)	184
Cisco Discovery Protocol 情報の表示	186
Cisco Discovery Protocol 情報の表示 (GUI)	186
Cisco Discovery Protocol 情報の表示 (CLI)	188
CDP デバッグ情報の取得	189
コントローラと NTP サーバの認証の設定	191
コントローラと NTP サーバの認証の設定について	191
NTP サーバの認証の設定 (GUI)	191
NTP サーバの認証の設定 (CLI)	192
RFID タグ追跡の設定	193
RFID タグ追跡の設定について	193
RFID タグ追跡の設定 (CLI)	195
RFID タグ追跡情報の表示 (CLI)	195

RFID タグ追跡問題のデバッグ (CLI)	196
コントローラのデフォルト設定へのリセット	197
コントローラのデフォルト設定へのリセットについて	197
コントローラのデフォルト設定へのリセット (GUI)	198
コントローラのデフォルト設定へのリセット (CLI)	198
コントローラ ソフトウェアと設定の管理	199
コントローラ ソフトウェアのアップグレード	199
コントローラ ソフトウェアのアップグレードに関する制限	200
コントローラ ソフトウェアのアップグレード (GUI)	203
コントローラ ソフトウェアのアップグレード (CLI)	205
アクセス ポイントへのイメージのプレダウロード	207
アクセス ポイントのプレダウロードのプロセス	208
アクセス ポイントへのイメージのプレダウロードの制限	209
アクセス ポイントへのイメージのプレダウロード : グローバル コン フィギュレーション (GUI)	210
アクセス ポイントへのイメージのプレダウロードの設定 (GUI)	212
アクセス ポイントへのイメージのプレダウロード (CLI)	214
コントローラとのファイルのやり取り	217
ログイン バナー ファイルのダウンロード	217
ログイン バナー ファイルのダウンロード (GUI)	218
ログイン バナー ファイルのダウンロード (CLI)	219
ログイン バナーのクリア (GUI)	220
デバイスの証明書のダウンロード	220
デバイスの証明書のダウンロード (GUI)	221
デバイスの証明書のダウンロード (CLI)	222
CA 証明書のダウンロード	223
CA 証明書のダウンロード (GUI)	224
CA 証明書のダウンロード (CLI)	225
PAC のアップロード	226
PAC のアップロード (GUI)	226
PAC のアップロード (CLI)	227
設定ファイルのアップロードおよびダウンロード	228

設定ファイルのアップグレード	229
設定ファイルのアップロード (GUI)	229
設定ファイルのアップロード (CLI)	229
設定ファイルのダウンロード	230
設定ファイルのダウンロード (GUI)	231
設定ファイルのダウンロード (CLI)	232
設定の保存	233
設定ファイルの編集	234
コントローラの設定のクリア	235
コントローラ設定の消去	235
コントローラのリセット	236
ユーザアカウントの管理	237
ゲストユーザアカウントの設定	237
ゲストアカウントの作成について	237
ユーザアカウントの管理に関する制限	237
Lobby Ambassador アccountの作成	238
ロビーアンバサダーアカウントの作成 (GUI)	238
ロビーアンバサダーアカウントの作成 (CLI)	239
ロビーアンバサダーとしてのゲストユーザアカウントの作成 (GUI)	239
ゲストユーザアカウントの表示	240
ゲストアカウントの表示 (GUI)	240
ゲストアカウントの表示 (CLI)	240
管理者のユーザ名とパスワードの設定	241
管理者のユーザ名とパスワードの設定について	241
ユーザ名とパスワードの設定 (GUI)	241
ユーザ名とパスワードの設定 (CLI)	241
パスワードの回復	242
SNMP v3 ユーザのデフォルト値の変更	242
SNMP v3 ユーザのデフォルト値の変更について	242
SNMP v3 ユーザのデフォルト値の変更 (GUI)	243
SNMP v3 ユーザのデフォルト値の変更 (CLI)	243
証明書署名要求の生成	244

サードパーティ証明書のダウンロード (GUI)	246
サードパーティ証明書のダウンロード (CLI)	247
Web 認証の管理	249
Web 認証証明書の入手	249
Web 認証証明書について	249
チェーン証明書のサポート	249
Web 認証証明書の入手 (GUI)	250
Web 認証証明書の入手 (CLI)	250
Web 認証プロセス	251
Web 認証プロセスのセキュリティ アラートの無効化	252
デフォルトの Web 認証ログイン ページの選択	254
デフォルトの Web 認証ログイン ページについて	254
デフォルトの Web 認証ログイン ページの選択 (GUI)	255
デフォルトの Web 認証ログイン ページの選択 (CLI)	256
例：カスタマイズされた Web 認証ログイン ページの作成	258
例：変更されたデフォルトの Web 認証ログイン ページの例	261
外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの使用	262
カスタマイズされた Web 認証ログイン ページについて	262
外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 (GUI)	262
外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 (CLI)	262
カスタマイズされた Web 認証ログイン ページのダウンロード	263
カスタマイズされた Web 認証ログイン ページのダウンロードの前提条件	264
カスタマイズされた Web 認証ログイン ページのダウンロード (GUI)	264
カスタマイズされた Web 認証ログイン ページのダウンロード (CLI)	265
例：カスタマイズされた Web 認証ログイン ページ	266
Web 認証ログイン ページの設定の確認 (CLI)	266
WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て	267

WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページ の割り当てについて	267
WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページ の割り当て (GUI)	267
WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページ の割り当て (CLI)	268
スリープ状態にあるクライアントの認証の設定	270
スリープ状態にあるクライアントの認証について	270
スリープ状態にあるクライアントの制限	271
スリープ状態のクライアントの認証の設定 (GUI)	271
スリープ状態のクライアントの認証の設定 (CLI)	272
有線ゲスト アクセスの設定	273
有線ゲスト アクセスについて	273
有線ゲストのアクセスを設定するための前提条件	274
有線ゲストのアクセスの設定に関する制限	274
有線ゲスト アクセスの設定 (GUI)	275
有線ゲスト アクセスの設定 (CLI)	277
IPv6 クライアントのゲスト アクセスのサポート	279
Ethernet over GRE トンネル	281
Ethernet over GRE トンネルについて	281
EoGRE トンネリングに関する制約事項	285
Cisco WLC での EoGRE の設定 (GUI)	286
WLC での EoGRE の設定 (CLI)	288
FlexConnect AP の EoGRE の設定 (GUI)	289
FlexConnect AP の EoGRE の設定 (CLI)	289
トラブルシューティング	291
LED の解釈	291
LED の解釈について	291
コントローラの LED の解釈	292
Lightweight アクセス ポイント LED の解釈	292
システム メッセージ	292
システム メッセージについて	292

システム リソースの表示	296
システム リソースの表示について	296
システム リソースの表示 (GUI)	297
システム リソースの表示 (CLI)	297
CLI を使用したトラブルシューティング	297
システム ログとメッセージ ログの設定	299
システム ログとメッセージ ログについて	299
システム ログとメッセージ ログの設定 (GUI)	299
メッセージ ログの表示 (GUI)	302
システム ログとメッセージ ログの設定 (CLI)	302
システム ログとメッセージ ログの表示 (CLI)	306
アクセス ポイント イベント ログの表示	306
アクセス ポイント イベント ログについて	306
アクセス ポイント イベント ログの表示 (CLI)	306
ログとクラッシュ ファイルのアップロード	307
ログとクラッシュ ファイルをアップロードするための前提条件	307
ログとクラッシュ ファイルのアップロード (GUI)	307
ログとクラッシュ ファイルのアップロード (CLI)	308
コントローラからのコア ダンプのアップロード	309
コントローラからのコア ダンプのアップロードについて	309
コア ダンプを自動的に FTP サーバにアップロードするようにコントローラを 設定する (GUI)	310
コア ダンプを自動的に FTP サーバにアップロードするようにコントローラを 設定する (CLI)	311
コントローラからサーバへのコア ダンプのアップロード (CLI)	312
パケット キャプチャ ファイルのアップロード	313
パケット キャプチャ ファイルのアップロードについて	313
パケット キャプチャ ファイルのアップロードに関する制約事項	314
パケット キャプチャ ファイルのアップロード (GUI)	315
パケット キャプチャ ファイルのアップロード (CLI)	316
メモリ リークの監視	316
メモリ リークの監視 (CLI)	316

CCXv5 クライアント デバイスのトラブルシューティング	318
CCXv5 クライアント デバイスのトラブルシューティングについて	318
CCXv5 クライアント デバイスの制約事項	318
診断チャネルの設定	318
診断チャネルの設定 (GUI)	319
診断チャネルの設定 (CLI)	319
クライアント レポートの設定	324
クライアント レポートの設定 (GUI)	324
クライアント レポートの設定 (CLI)	325
ローミング診断とリアルタイム診断の設定	325
ローミング診断とリアルタイム診断の設定 (CLI)	326
デバッグ ファシリティの使用方法	329
デバッグ ファシリティの使用方法について	329
デバッグ ファシリティの設定 (CLI)	330
無線スニファの設定	334
無線スニファについて	334
無線スニファの必須条件	334
無線スニファの制約事項	335
アクセス ポイントのスニファの設定 (GUI)	335
アクセス ポイントのスニファの設定 (CLI)	336
Telnet または SSH_old を使用したアクセス ポイントのトラブルシューティング	337
Telnet または SSH を使用したアクセス ポイントのトラブルシューティングについて	337
Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (GUI)	338
Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (CLI)	338
アクセス ポイント監視サービスのデバッグ	339
アクセス ポイント監視サービスのデバッグについて	339
アクセス ポイント監視サービスの問題のデバッグ (CLI)	339
OfficeExtend アクセス ポイントのトラブルシューティング	340
OfficeExtend アクセス ポイントのトラブルシューティングについて	340

OfficeExtend の LED の解釈	340
RF カバレッジが最適になるように OfficeExtend アクセス ポイントを配置する	340
一般的な問題のトラブルシューティング	340
ポートとインターフェイスの設定	343
ポートとインターフェイスの概要	345
ポートについて	345
ディストリビューション システム ポートについて	346
ディストリビューション システム ポートの設定に関する制限	346
サービス ポートについて	348
インターフェイスに関する情報	348
インターフェイスの設定に関する注意事項	349
動的 AP 管理について	349
WLAN について	350
管理インターフェイスの設定	353
管理インターフェイスについて	353
管理インターフェイスの設定 (GUI)	354
管理インターフェイスの設定 (CLI)	355
AP マネージャ インターフェイスの設定	357
AP マネージャ インターフェイスについて	357
AP マネージャ インターフェイス設定の制約事項	358
AP マネージャ インターフェイスの設定 (GUI)	358
AP マネージャ インターフェイスの設定 (CLI)	359
設定例 : Cisco 5500 シリーズ コントローラでの AP マネージャの設定	360
仮想インターフェイスの設定	363
仮想インターフェイスについて	363
仮想インターフェイスの設定 (GUI)	364
仮想インターフェイスの設定 (CLI)	364
サービス ポート インターフェイスの設定	367
サービス ポート インターフェイスについて	367
サービス ポート インターフェイスの設定に関する制限	367
サービス ポート インターフェイスの設定 (GUI)	367

サービス ポート インターフェイスの設定 (CLI)	368
動的インターフェイスの設定	369
動的インターフェイスについて	369
動的インターフェイス設定の前提条件	370
動的インターフェイスの設定に関する制約事項	370
動的インターフェイスの設定 (GUI)	371
動的インターフェイスの設定 (CLI)	372
ポートの設定	375
ポートの設定 (GUI)	375
リンク集約の設定	377
リンク集約について	377
リンク集約の制約事項	378
リンク集約の有効化 (GUI)	380
リンク集約の有効化 (CLI)	380
リンク集約の設定の確認 (CLI)	380
リンク集約をサポートするための隣接デバイスの設定	381
リンク集約と複数の AP マネージャ インターフェイス間の選択	381
複数の AP マネージャ インターフェイスの設定	383
複数の AP マネージャ インターフェイスについて	383
複数の AP マネージャ インターフェイス設定の制約事項	384
複数の AP マネージャ インターフェイスの作成 (GUI)	384
複数の AP マネージャ インターフェイスの作成 (CLI)	385
VLAN Select の設定	387
VLAN Select について	387
VLAN 選択の設定に関する制限	388
インターフェイス グループの設定	388
インターフェイス グループについて	388
インターフェイス グループの設定に関する制限	389
インターフェイス グループの作成 (GUI)	389
インターフェイス グループの作成 (CLI)	389
インターフェイス グループへのインターフェイスの追加 (GUI)	390
インターフェイス グループへのインターフェイスの追加 (CLI)	390

インターフェイス グループ内の VLAN の表示 (CLI)	390
WLAN へのインターフェイス グループの追加 (GUI)	390
WLAN へのインターフェイス グループの追加 (CLI)	391
インターフェイス グループの設定	393
インターフェイス グループについて	393
インターフェイス グループの設定に関する制限	394
インターフェイス グループの作成 (GUI)	394
インターフェイス グループの作成 (CLI)	395
インターフェイス グループへのインターフェイスの追加 (GUI)	395
インターフェイス グループへのインターフェイスの追加 (CLI)	395
インターフェイス グループ内の VLAN の表示 (CLI)	395
WLAN へのインターフェイス グループの追加 (GUI)	396
WLAN へのインターフェイス グループの追加 (CLI)	396
マルチキャストの最適化の設定	397
マルチキャスト最適化について	397
マルチキャスト VLAN の設定 (GUI)	398
マルチキャスト VLAN の設定 (CLI)	398
ハイ アベイラビリティの設定	399
ハイ アベイラビリティに関する情報	399
ハイ アベイラビリティの制約事項	403
ハイ アベイラビリティ (GUI) の設定	407
ハイ アベイラビリティ (CLI) の設定	408
VideoStream の設定	411
VideoStream の設定	413
VideoStream について	413
VideoStream の前提条件	413
VideoStream の設定に関する制限	414
VideoStream の設定 (GUI)	414
VideoStream の設定 (CLI)	418
メディア ストリームの表示とデバッグ	419
セキュリティ ソリューションの設定	421
Cisco Unified Wireless Network Solution セキュリティ	423

セキュリティの概要	423
レイヤ1 ソリューション	423
レイヤ2 ソリューション	424
レイヤ2 ソリューションの制約事項	424
レイヤ3 ソリューション	424
統合されたセキュリティ ソリューション	424
RADIUS の設定	427
RADIUS について	427
ACS 上での RADIUS の設定	430
RADIUS の設定 (GUI)	431
RADIUS の設定 (CLI)	437
コントローラによって送信される RADIUS 認証属性	441
Access-Accept パケットで受け付けられる認証属性 (Airespace)	444
RADIUS アカウンティング属性	452
TACACS+ の設定	455
TACACS+ について	455
TACACS+ VSA	458
ACS 上での TACACS+ の設定	459
TACACS+ の設定 (GUI)	461
TACACS+ の設定 (CLI)	463
TACACS+ 管理サーバのログの表示	465
FIPS 設定、CC、UCAPL	467
FIPS の概要	467
FIPS のセルフテスト	468
CC について	469
UCAPL について	469
FIPS の設定 (CLI)	469
CC の設定 (CLI)	470
UCAPL の設定 (CLI)	470
最大ローカル データベース エントリの設定	471
最大ローカル データベース エントリの設定について	471
最大ローカル データベース エントリの設定 (GUI)	471

最大ローカル データベース エントリの設定 (CLI)	472
コントローラでのローカル ネットワーク ユーザの設定	473
コントローラ上のローカル ネットワーク ユーザについて	473
コントローラに対するローカル ネットワーク ユーザの設定 (GUI)	473
コントローラに対するローカル ネットワーク ユーザの設定 (CLI)	475
パスワード ポリシーの設定	477
パスワード ポリシーについて	477
パスワード ポリシーの設定 (GUI)	478
パスワード ポリシーの設定 (CLI)	478
LDAP の設定	481
LDAP について	481
LDAP の設定 (GUI)	482
LDAP の設定 (CLI)	484
ローカル EAP の設定	487
ローカル EAP について	487
ローカル EAP の制約事項	489
ローカル EAP の設定 (GUI)	490
ローカル EAP の設定 (CLI)	495
SpectraLink 社の NetLink 電話用システムの設定	501
SpectraLink NetLink 電話について	501
SpectraLink 社の NetLink 電話の設定	501
長いプリアンプルの有効化 (GUI)	501
長いプリアンプルの有効化 (CLI)	502
Enhanced Distributed Channel Access の設定 (CLI)	503
RADIUS NAC サポートの設定	505
RADIUS NAC サポートについて	505
デバイス登録	506
中央 Web 認証	506
ローカル Web 認証	506
RADIUS NAC サポートの制約事項	506
RADIUS NAC サポートの設定 (GUI)	508
RADIUS NAC サポートの設定 (CLI)	508

設定の RADIUS VSA およびレルム	509
RADIUS VSA の設定	509
RADIUS VSA に関する情報	509
RADIUS AVP リストの XML サンプル ファイル	510
RADIUS AVP リストのダウンロード (GUI)	510
RADIUS AVP リストのアップロード (GUI)	511
RADIUS AVP リストのアップロードおよびダウンロード (CLI)	512
RADIUS レルムの設定	512
RADIUS レルムについて	512
RADIUS レルムの設定の前提条件	514
RADIUS レルムの設定に関する制約事項	514
WLAN でのレルムの設定 (GUI)	514
WLAN でのレルムの設定 (CLI)	514
RADIUS 認証サーバでのレルムの設定 (GUI)	515
RADIUS 認証サーバでのレルムの設定 (CLI)	515
RADIUS アカウンティングサーバでのレルムの設定 (GUI)	515
RADIUS アカウンティングサーバでのレルムの設定 (CLI)	515
無線による管理機能の使用	517
無線による管理機能について	517
無線による管理機能の有効化 (GUI)	517
無線による管理機能の有効化 (CLI)	517
動的インターフェイスによる管理機能	519
動的インターフェイスによる管理機能について	519
動的インターフェイスによる管理機能の設定 (CLI)	520
DHCP オプション 82 の設定	521
DHCP オプション 82 について	521
DHCP オプション 82 の制約事項	522
DHCP オプション 82 の設定 (GUI)	522
DHCP オプション 82 の設定 (CLI)	522
アクセス コントロール リストの設定と適用	525
アクセス コントロール リストについて	525
アクセス コントロール リストの制約事項	526

アクセス コントロール リストの設定と適用 (GUI)	527
アクセス コントロール リストの設定	527
インターフェイスへのアクセス コントロール リストの適用	529
コントローラ CPU へのアクセス コントロール リストの適用	530
WLAN へのアクセス コントロール リストの適用	530
WLAN への事前認証アクセス コントロール リストの適用	531
アクセス コントロール リストの設定と適用 (CLI)	531
アクセス コントロール リストの設定	531
アクセス コントロール リストの適用	532
レイヤ2 アクセス コントロール リストの設定	533
レイヤ2 アクセス コントロール リストの設定について	533
レイヤ2 アクセス コントロール リストの制約事項	534
レイヤ2 アクセス コントロール リストの設定 (CLI)	534
WLAN とレイヤ2 ACL のマッピング (CLI)	535
FlexConnectアクセスポイントを使用したローカルにスイッチされる WLAN とレイヤ2 ACL のマッピング (CLI)	535
レイヤ2 アクセス コントロール リストの設定 (GUI)	535
WLAN へのレイヤ2 アクセス コントロール リストの適用 (GUI)	537
WLAN の AP へのレイヤ2 アクセス コントロール リストの適用 (GUI)	537
DNS ベースのアクセス コントロール リストの設定	538
DNS ベースのアクセス コントロール リストについて	538
DNS ベースのアクセス コントロール リストの制約事項	538
DNS ベースのアクセス コントロール リストの設定 (CLI)	538
DNS ベースのアクセス コントロール リストの設定 (GUI)	540
管理フレーム保護の設定	541
管理フレーム保護について	541
管理フレーム保護の制約事項	543
管理フレーム保護の設定 (GUI)	544
管理フレーム保護の設定の表示 (GUI)	544
管理フレーム保護の設定 (CLI)	545
管理フレーム保護の設定の表示 (CLI)	545
管理フレーム保護の問題のデバッグ (CLI)	545

クライアント除外ポリシーの設定	547
クライアント除外ポリシーの設定 (GUI)	547
クライアント除外ポリシーの設定 (CLI)	548
Identity ネットワーキングの設定	551
Identity ネットワーキングについて	551
Identity ネットワーキングで使用される RADIUS 属性	552
AAA Override の設定	557
AAA Override について	557
AAA Override の制約事項	558
正しい QoS 値を取得するための RADIUS サーバディクショナリ ファイルの更新	558
AAA Override の設定 (GUI)	560
AAA Override の設定 (CLI)	560
不正なデバイスの管理	561
不正なデバイスについて	561
不正検出の設定 (GUI)	565
不正検出の設定 (CLI)	567
不正なアクセス ポイントの分類	573
不正なアクセス ポイントの分類について	573
不正なアクセス ポイントの分類の制限	576
不正分類ルールの設定 (GUI)	577
不正なデバイスの表示および分類 (GUI)	580
不正分類ルールの設定 (CLI)	584
不正なデバイスの表示および分類 (CLI)	586
Cisco TrustSec SXP の設定	591
Cisco TrustSec SXP について	591
Cisco TrustSec SXP の制約事項	593
Cisco TrustSec SXP の設定 (GUI)	593
新規 SXP 接続の作成 (GUI)	594
Cisco TrustSec SXP の設定 (CLI)	594
ローカル ポリシーの設定	597
ローカル ポリシーについて	597
ローカル ポリシー分類の制約事項	598

ローカル ポリシーの設定 (GUI)	600
ローカル ポリシーの設定 (CLI)	601
Cisco Intrusion Detection System の設定	603
Cisco Intrusion Detection System について	603
回避クライアント	603
その他の情報	604
IDS センサーの設定 (GUI)	604
回避クライアントの表示 (GUI)	605
IDS センサーの設定 (CLI)	605
回避クライアントの表示 (CLI)	607
IDS シグニチャの設定	609
IDS シグニチャについて	609
IDS シグニチャの設定 (GUI)	612
IDS シグニチャのアップロードまたはダウンロード	612
IDS シグニチャの有効化または無効化	613
IDS シグニチャ イベントの表示 (GUI)	615
IDS シグニチャの設定 (CLI)	616
IDS シグニチャ イベントの表示 (CLI)	617
wIPS の設定	619
wIPS について	619
wIPS の制約事項	627
アクセス ポイントでの wIPS の設定 (GUI)	627
アクセス ポイントでの wIPS の設定 (CLI)	627
wIPS 情報の表示 (CLI)	629
Wi-Fi Direct クライアント ポリシーの設定	631
Wi-Fi Direct クライアント ポリシーについて	631
Wi-Fi Direct クライアント ポリシーの制限	631
Wi-Fi Direct クライアント ポリシーの設定 (GUI)	632
Wi-Fi Direct クライアント ポリシーの設定 (CLI)	632
Wi-Fi Direct クライアント ポリシーの監視とトラブルシューティング (CLI)	633
Web 認証プロキシの設定	635
Web 認証プロキシについて	635

Web 認証プロキシの設定 (GUI)	636
Web 認証プロキシの設定 (CLI)	637
意図的な悪用の検出	639
意図的な悪用の検出	639
WLAN の使用	641
WLAN の設定	643
WLAN の前提条件	643
WLAN の制約事項	644
WLAN について	645
WLAN の作成および削除 (GUI)	645
WLAN の有効化および無効化 (GUI)	647
WLAN の作成および削除 (CLI)	647
WLAN の有効化および無効化 (CLI)	648
WLAN の表示 (CLI)	648
WLAN の検索 (GUI)	648
インターフェイスへの WLAN の割り当て	649
Network Access Identifier の設定 (CLI)	649
WLAN ごとのクライアント カウントの設定	651
WLAN ごとのクライアント カウントの設定に関する制約事項	651
WLAN ごとのクライアント カウントの設定について	652
WLAN ごとのクライアント カウントの設定 (GUI)	652
WLAN ごとの最大クライアント数の設定 (CLI)	652
WLAN ごとの各 AP 無線に対する最大クライアント数の設定 (GUI)	653
WLAN ごとの各 AP 無線に対する最大クライアント数の設定 (CLI)	653
クライアントの認証解除 (CLI)	653
DHCP の設定	655
DHCP for WLANs の設定に関する制限	655
Dynamic Host Configuration Protocol について	655
内部 DHCP サーバ	655
外部 DHCP サーバ	656
DHCP 割り当て	656
DHCP の設定 (GUI)	657

DHCP の設定 (CLI)	659
DHCP のデバッグ (CLI)	659
DHCP スコープの設定	661
DHCP スコープの設定に関する制限	661
DHCP スコープについて	661
DHCP スコープの設定 (GUI)	661
DHCP スコープの設定 (CLI)	663
WLAN の MAC フィルタリングの設定	665
MAC フィルタリングの制限	665
WLAN の MAC フィルタリングについて	665
MAC フィルタリングの有効化	665
ローカル MAC フィルタの設定	667
ローカル MAC フィルタの設定に関する前提条件	667
ローカル MAC フィルタについて	667
ローカル MAC フィルタの設定 (CLI)	667
タイムアウトの設定	669
無効なクライアントのタイムアウトの設定	669
無効なクライアントのタイムアウトの設定について	669
無効なクライアントのタイムアウトの設定 (CLI)	669
セッションタイムアウトの設定	670
セッションタイムアウトについて	670
セッションタイムアウトの設定 (GUI)	670
セッションタイムアウトの設定 (CLI)	670
ユーザアイドルタイムアウトの設定	671
WLAN ごとのユーザアイドルタイムアウトについて	671
WLAN ごとのユーザアイドルタイムアウトの設定 (CLI)	671
DTIM period の設定	673
DTIM Period について	673
DTIM period の設定 (GUI)	674
DTIM period の設定 (CLI)	674
ピアツーピア ブロッキングの設定	677
ピア ツー ピア ブロッキングの制約事項	677

ピアツーピア ブロッキングについて	678
ピアツーピア ブロッキングの設定 (GUI)	678
ピアツーピア ブロッキングの設定 (CLI)	679
レイヤ 2 セキュリティの設定	681
レイヤ 2 セキュリティの前提条件	681
Static WEP キーの設定 (CLI)	682
802.1X 動的キーおよび許可の設定 (CLI)	682
802.11r BSS の高速移行の設定	683
802.11r 高速移行の制約事項	683
802.11r の高速移行について	685
802.11r の高速移行の設定 (GUI)	687
802.11r の高速移行の設定 (CLI)	688
802.11r BSS の高速移行のトラブルシューティング	689
802.1X 認証への MAC 認証フェールオーバーの設定	689
802.1X 認証への MAC 認証フェールオーバーの設定 (GUI)	690
802.1X 認証への MAC 認証フェールオーバーの設定 (CLI)	690
802.11w の設定	690
802.11w の制約事項	690
802.11w に関する情報	691
802.11w の設定 (GUI)	692
802.11w の設定 (CLI)	692
Static WEP と Dynamic WEP の両方をサポートする WLAN の設定	695
Static および Dynamic WEP の設定に関する制約事項	695
Static WEP と Dynamic WEP の両方をサポートする WLAN について	696
WPA1 と WPA2	696
WPA1 +WPA2 の設定	698
WPA1+WPA2 の設定 (GUI)	698
WPA1+WPA2 の設定 (CLI)	699
Sticky Key Caching の設定	701
Sticky Key Caching について	701
Sticky Key Caching の制約事項	701
Sticky Key Caching の設定 (CLI)	702

CKIP の設定	705
CKIP について	705
CKIP の設定 (GUI)	706
CKIP の設定 (CLI)	707
レイヤ 3 セキュリティの設定	709
VPN パススルーを使用したレイヤ 3 セキュリティの設定	709
VPN パススルーを使用したレイヤ 3 セキュリティの制約事項	709
VPN パススルーについて	709
VPN パススルーの設定	710
VPN パススルーの設定 (GUI)	710
VPN パススルーの設定 (CLI)	710
Web 認証を使用したレイヤ 3 セキュリティの設定	710
WLAN の Web 認証を設定するための前提条件	710
WLAN の Web 認証の設定に関する制約事項	711
Web 認証について	711
Web 認証の設定	712
Web 認証の設定 (GUI)	712
Web 認証の設定 (CLI)	712
キャプティブバイパスの設定	713
キャプティブバイパスについて	713
キャプティブバイパスの設定 (CLI)	714
MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定	715
MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーについて	715
MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定 (GUI)	716
MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定 (CLI)	717
QoS プロファイルの割り当て	719
QoS プロファイルについて	719
WLAN への QoS プロファイルの割り当て (GUI)	720
WLAN への QoS プロファイルの割り当て (CLI)	722

QoS Enhanced BSS の設定 725

Cisco 7921 および 7920 Wireless IP Phone で QoS Enhanced BSS を使用するための前提
条件 725

QoS Enhanced BSS の制約事項 726

QoS Enhanced BSS について 726

QBSS の設定 (GUI) 727

QBSS の設定 (CLI) 728

メディア セッション スヌーピングおよびレポートの設定 729

メディア セッション スヌーピングおよびレポートの制約事項 729

メディア セッション スヌーピングおよびレポートについて 729

メディア セッション スヌーピングの設定 (GUI) 730

メディア セッション スヌーピングの設定 (CLI) 730

Key Telephone System-Based CAC の設定 735

Key Telephone System-Based CAC の制約事項 735

Key Telephone System-Based CAC について 735

KTS-based CAC の設定 (GUI) 736

KTS-based CAC の設定 (CLI) 736

関連コマンド 737

ローミングしている音声クライアントのリアンカーの設定 739

ローミングしている音声クライアントのリアンカーの設定に関する制約事項 739

ローミングしている音声クライアントのリアンカーについて 739

ローミングしている音声クライアントのリアンカーの設定 (GUI) 740

ローミングしている音声クライアントのリアンカーの設定 (CLI) 740

シームレスな IPv6 モビリティの設定 743

IPv6 モビリティを設定するための前提条件 743

IPv6 モビリティの設定に関する制約事項 744

IPv6 モビリティについて 744

IPv6 のグローバルな設定 745

IPv6 のグローバルな設定 (GUI) 745

IPv6 のグローバルな設定 (CLI) 745

IPv6 クライアントのための RA ガードの設定 745

RA ガードについて 745

RA ガードの設定 (GUI)	746
RA ガードの設定 (CLI)	746
IPv6 クライアントのための RA スロットリングの設定	746
RA スロットリングについて	746
RA スロットリングの設定 (GUI)	747
RA スロットル ポリシーの設定 (CLI)	747
IPv6 ネイバー ディスカバリ キャッシングの設定	748
IPv6 ネイバー ディスカバリについて	748
ネイバー バインディングの設定 (GUI)	748
ネイバー バインディングの設定 (CLI)	749
Cisco Client Extensions の設定	751
Cisco Client Extensions を設定するための前提条件	751
Cisco Client Extensions の設定に関する制約事項	751
Cisco Client Extensions について	752
CCX Aironet IE の設定 (GUI)	752
クライアントの CCX バージョンの表示 (GUI)	752
CCX Aironet IE の設定 (CLI)	753
クライアントの CCX バージョンの表示 (CLI)	753
リモート LAN の設定	755
リモート LAN を設定するための前提条件	755
リモート LAN の設定に関する制約事項	755
リモート LAN について	756
リモート LAN の設定 (GUI)	756
リモート LAN の設定 (CLI)	757
AP グループの設定	759
AP グループを設定するための前提条件	759
コントローラ プラットフォームでサポートされる AP グループ	759
アクセス ポイント グループの設定に関する制約事項	760
アクセス ポイント グループについて	761
アクセス ポイント グループの設定	762
アクセス ポイント グループの作成 (GUI)	763
アクセス ポイント グループの作成 (CLI)	765

アクセス ポイント グループの表示 (CLI)	766
RF プロファイルの設定	767
RF プロファイルを設定するための前提条件	767
RF プロファイルの設定に関する制約事項	767
RF プロファイルについて	768
RF プロファイルの設定 (GUI)	771
RF プロファイルの設定 (CLI)	773
AP グループへの RF プロファイルの適用 (GUI)	776
AP グループへの RF プロファイルの適用 (CLI)	776
802.1X 認証を使用した Web リダイレクトの設定	777
802.1X 認証を使用した Web リダイレクトについて	777
条件付き Web リダイレクト	777
スプラッシュ ページ Web リダイレクト	778
RADIUS サーバの設定 (GUI)	779
Web リダイレクトの設定	780
Web リダイレクトの設定 (GUI)	780
Web リダイレクトの設定 (CLI)	780
WLAN ごとのアカウントिंग サーバの無効化 (GUI)	781
WLAN ごとのカバレッジ ホールの検出の無効化	781
WLAN 上のカバレッジ ホールの検出の無効化 (GUI)	782
WLAN 上のカバレッジ ホールの検出の無効化 (CLI)	782
NAC アウトオブバンド統合の設定	785
NAC アウトオブバンドの前提条件	785
NAC アウトオブバンドの制限	786
NAC アウトオブバンド統合について	787
NAC アウトオブバンド統合の設定 (GUI)	788
NAC アウトオブバンド統合の設定 (CLI)	789
パッシブクライアントの設定	791
パッシブクライアントの制約事項	791
パッシブクライアントについて	791
パッシブクライアントの設定 (GUI)	792
マルチキャスト-マルチキャスト モードの有効化 (GUI)	793

コントローラでのグローバルマルチキャストモードの有効化 (GUI)	793
コントローラでのパッシブクライアント機能の有効化 (GUI)	794
パッシブクライアントの設定 (CLI)	794
クライアントプロファイルの設定	797
クライアントプロファイルを設定するための前提条件	797
クライアントプロファイルの設定に関する制約事項	798
クライアントプロファイルについて	798
クライアントプロファイルの設定 (GUI)	798
クライアントプロファイルの設定 (CLI)	799
WLAN ごとの RADIUS 送信元サポートの設定	801
WLAN ごとの RADIUS 送信元サポートの前提条件	801
WLAN ごとの RADIUS 送信元サポートの制約事項	801
WLAN ごとの RADIUS 送信元サポートについて	801
WLAN ごとの RADIUS 送信元サポートの設定 (CLI)	802
WLAN ごとの RADIUS 送信元サポートのステータスのモニタリング (CLI)	802
モバイル コンシエルジュの設定	805
モバイル コンシエルジュについて	805
モバイル コンシエルジュの設定 (802.11u)	806
モバイル コンシエルジュの設定 (802.11u) (GUI)	806
モバイル コンシエルジュの設定 (802.11u) (CLI)	807
802.11u Mobility Services Advertisement Protocol の設定	808
802.11u MSAP について	808
802.11u MSAP の設定 (GUI)	809
MSAP の設定 (CLI)	809
802.11u HotSpot の設定	809
802.11u HotSpot について	809
802.11u Hotspot の設定 (GUI)	810
Hotspot 2.0 の設定 (CLI)	810
アクセスポイントでの HotSpot2 の設定 (GUI)	812
アクセスポイントでの HotSpot2 の設定 (CLI)	813
802.1Q-in-Q VLAN タギングの情報	816
802.1Q-in-Q VLAN タギングの制約事項	817

802.1Q-in-Q VLAN タギングの設定 (GUI)	818
802.1Q-in-Q VLAN タギングの設定 (CLI)	819
経路ローミングの設定 821	
経路ローミングの制約事項	821
経路ローミングについて	821
経路ローミングの設定 (CLI)	823
VLAN タギング 802.1Q-in-Q の設定 825	
802.1Q-in-Q VLAN タギングの情報	825
802.1Q-in-Q VLAN タギングの制約事項	826
802.1Q-in-Q VLAN タギングの設定 (GUI)	827
802.1Q-in-Q VLAN タギングの設定 (CLI)	828
Lightweight アクセス ポイントの制御 829	
アクセス ポイント通信プロトコルの使用 831	
アクセス ポイント通信プロトコルについて	831
アクセス ポイント通信プロトコルの制約事項	832
データ暗号化の設定	832
データ暗号化のためのガイドライン	833
Cisco 5500 シリーズ コントローラ用 DTLS イメージのアップグレードまたはダウ ングレード	834
DTLS イメージへまたは DTLS イメージからのアップグレード時のガイドラ イン	834
データ暗号化の設定 (GUI)	835
データ暗号化の設定 (CLI)	835
CAPWAP の最大伝送単位情報の表示	836
CAPWAP のデバッグ	836
コントローラ ディスカバリ プロセス	837
コントローラ ディスカバリ プロセスの制約事項	838
アクセス ポイントのコントローラへの join の確認	838
アクセス ポイントのコントローラへの join の確認 (GUI)	838
アクセス ポイントのコントローラへの join の確認 (CLI)	839
CAPWAP の望ましいモード設定 841	
優先モードについて	841

優先モードの設定のガイドライン	841
CAPWAP 設定の望ましいモード (GUI)	842
CAPWAP 設定の望ましいモード (CLI)	843
アクセス ポイントの検索	845
アクセス ポイントの検索について	845
AP フィルタの検索 (GUI)	845
インターフェイスの詳細の監視	848
アクセス ポイント無線の検索	850
アクセス ポイント無線の検索について	850
アクセス ポイント無線の検索 (GUI)	850
アクセス ポイントのグローバル クレデンシャルの設定	853
アクセス ポイントのグローバル クレデンシャルの設定について	853
アクセス ポイントのグローバル クレデンシャルに関する制約事項	854
アクセス ポイントのグローバル資格情報の設定 (GUI)	855
アクセス ポイントのグローバル資格情報の設定 (CLI)	856
アクセス ポイントの認証の設定	857
アクセス ポイントに対する認証の設定について	857
アクセス ポイントの認証を設定するための前提条件	857
アクセス ポイントの認証に関する制約事項	858
アクセス ポイントの認証の設定 (GUI)	858
アクセス ポイントの認証の設定 (CLI)	859
スイッチの認証の設定	860
組み込みアクセス ポイントの設定	863
組み込みアクセス ポイントについて	863
自律アクセス ポイントの Lightweight モードへの変換	867
自律アクセス ポイントの Lightweight モードへの変換について	868
自律アクセス ポイントの Lightweight モードへの変換に関する制約事項	868
Lightweight モードから Autonomous モードへの復帰	868
以前のリリース (CLI) への復帰	869
MODE ボタンと TFTP サーバを使用して前のリリースへの復帰	869
アクセス ポイントの許可	870
SSC を使用したアクセス ポイントの許可	870

SSC を使用する仮想コントローラのアクセス ポイントの許可	870
SSC (GUI) の設定	870
SSC の設定 (CLI)	871
MIC を使用したアクセス ポイントの許可	871
LSC を使用したアクセス ポイントの許可	871
ローカルで有効な証明書 (GUI) の設定	872
ローカルで有効な証明書 (CLI) の設定	873
アクセス ポイントの許可 (GUI)	875
アクセス ポイントの許可 (CLI)	875
アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定	876
アクセス ポイントからの CAPWAP フレームの VLAN タギングについて	876
アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定 (GUI)	876
アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定 (CLI)	877
DHCP オプション 43 および DHCP オプション 60 の使用	877
アクセス ポイント join プロセスのトラブルシューティング	879
アクセス ポイントの Syslog サーバの設定 (CLI)	880
アクセス ポイントの join 情報の表示	881
アクセス ポイントの join 情報の表示 (GUI)	881
アクセス ポイントの join 情報の表示 (CLI)	882
Lightweight モードに変換されるアクセス ポイントへのデバッグ コマンドの送信	883
変換したアクセス ポイントがクラッシュ情報をコントローラに送信する方法について	884
変換したアクセス ポイントが無線コア ダンプをコントローラに送信する方法について	884
無線コア ダンプの取得 (CLI)	884
無線コア ダンプのアップロード (GUI)	885
無線コア ダンプのアップロード (CLI)	885
変換したアクセス ポイントからのメモリ コア ダンプのアップロード	886
アクセス ポイントのコア ダンプのアップロード (GUI)	887
アクセス ポイントのコア ダンプのアップロード (CLI)	887
AP クラッシュ ログ情報の表示	888

APクラッシュ ログ情報の表示 (GUI)	888
APクラッシュ ログ情報の表示 (CLI)	888
変換されたアクセス ポイントの MAC アドレスの表示	888
Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化	889
Lightweight アクセス ポイントでの固定 IP アドレスの設定	889
固定 IP アドレスの設定 (GUI)	890
固定 IP アドレスの設定 (CLI)	890
サイズの大きなアクセス ポイントのイメージのサポート	891
アクセス ポイントの回復 : TFTP リカバリ手順の使用	892
パケットキャプチャの設定	893
パケットキャプチャについて	893
パケットキャプチャの制約事項	894
パケットキャプチャの設定 (CLI)	894
OfficeExtend アクセス ポイントの設定	897
OfficeExtend アクセス ポイントについて	897
OEAP 600 シリーズ アクセス ポイント	898
ローカル モードの OEAP	899
600 シリーズ OfficeExtend アクセス ポイントに対してサポートされる WLAN の設定	899
600 シリーズ OfficeExtend アクセス ポイントに対する WLAN のセキュリティ 設定	900
認証の設定	904
600 シリーズ OfficeExtend アクセス ポイントでサポートされるユーザ カウン ト	905
リモート LAN の設定	905
チャンネルの管理と設定	906
その他の注意事項	907
セキュリティの実装	908
OfficeExtend アクセス ポイントのライセンスング	908
OfficeExtend アクセス ポイントの設定	909
OfficeExtend アクセス ポイントの設定 (GUI)	909
OfficeExtend アクセス ポイントの設定 (CLI)	911

WLAN またはリモート LAN のスプリット トンネリングの設定	914
WLAN またはリモート LAN のスプリット トンネリングの設定 (GUI)	914
WLAN またはリモート LAN のスプリット トンネリングの設定 (CLI)	914
OfficeExtend アクセス ポイントでの個人 SSID の設定	915
OfficeExtend アクセス ポイント統計情報の表示	917
設定の Cisco 700 シリーズ アクセス ポイント	919
Cisco 700 シリーズ アクセス ポイントに関する情報	919
設定の Cisco 700 シリーズ アクセス ポイント	919
LAN ポートの有効化 (CLI)	920
702W LAN ポートの有効化	920
Cisco ワークグループブリッジの使用	921
Cisco ワークグループブリッジについて	921
Cisco ワークグループブリッジの制約事項	923
WGB の設定例	925
ワークグループブリッジのステータスの表示 (GUI)	925
ワークグループブリッジのステータスの表示 (CLI)	926
WGB の問題のデバッグ (CLI)	926
Cisco 以外のワークグループブリッジの使用	929
Cisco 以外のワークグループブリッジについて	929
他社のワークグループブリッジの制約事項	930
バックアップコントローラの設定	931
バックアップコントローラの設定について	931
バックアップコントローラの設定に関する制約事項	932
バックアップコントローラの設定 (GUI)	932
バックアップコントローラの設定 (CLI)	934
アクセスポイントのフェールオーバープライオリティの設定	937
アクセスポイントに対するフェールオーバープライオリティの設定について	937
アクセスポイントのフェールオーバープライオリティの設定 (GUI)	938
アクセスポイントのフェールオーバープライオリティの設定 (CLI)	938
フェールオーバープライオリティの設定の表示 (CLI)	939
AP の再送信間隔および再試行回数の設定	941
AP 再送信間隔および再試行回数の設定について	941

アクセス ポイントの再送信間隔と再試行回数の制約事項	941
AP の再送信間隔と再試行回数の設定 (GUI)	942
アクセス ポイントの再送信間隔と再試行回数の設定 (CLI)	942
Country Code の設定	945
国番号の設定について	945
国コードの設定に関する制約事項	946
Country Code の設定 (GUI)	947
Country Code の設定 (CLI)	948
アクセス ポイントでの RFID トラッキングの最適化	951
アクセス ポイントでの RFID トラッキングの最適化について	951
アクセス ポイントでの RFID トラッキングの最適化 (GUI)	952
アクセス ポイントでの RFID トラッキングの最適化 (CLI)	952
プローブ要求フォワーディングの設定	955
プローブ要求フォワーディングの設定について	955
プローブ要求フォワーディングの設定 (CLI)	955
コントローラとアクセス ポイント上の一意的デバイス ID の取得	957
コントローラとアクセス ポイント上の Unique Device Identifier の取得について	957
コントローラとアクセス ポイント上の Unique Device Identifier の取得 (GUI)	958
コントローラとアクセス ポイント上の Unique Device Identifier の取得 (CLI)	958
リンク テストの実行	959
リンク テストの実行について	959
リンク テストの実行 (GUI)	960
リンク テストの実行 (CLI)	961
リンク遅延の設定	963
リンク遅延の設定について	963
リンク遅延の制約事項	964
リンク遅延の設定 (GUI)	964
リンク遅延の設定 (CLI)	965
TCP MSS の設定	967
TCP MSS の設定について	967
TCP MSS の設定 (GUI)	967
TCP MSS の設定 (CLI)	968

Power over Ethernet の設定	969
Power over Ethernet の設定について	969
Power over Ethernet の設定 (GUI)	971
Power over Ethernet の設定 (CLI)	973
クライアントの表示	975
クライアントの表示 (GUI)	975
クライアントの表示 (CLI)	977
アクセス ポイントの LED 状態の設定	979
LED 状態の設定	979
アクセス ポイントに対する LED 状態の設定について	979
ネットワーク内のアクセス ポイントの LED 状態のグローバル設定 (GUI)	979
ネットワーク内のアクセス ポイントの LED 状態のグローバル設定 (CLI)	980
特定のアクセス ポイントで LED 状態の設定 (GUI)	980
特定のアクセス ポイントで LED 状態の設定 (CLI)	980
点滅する LED の設定	980
点滅する LED の設定について	980
点滅する LED の設定 (CLI)	980
デュアルバンド無線によるアクセス ポイントの設定	983
デュアルバンド無線によるアクセス ポイントの設定 (GUI)	983
デュアルバンド無線によるアクセス ポイントの設定 (CLI)	984
UDP Lite の設定	985
UDP Lite について	985
UDP Lite のグローバル設定 (GUI)	986
AP 上での UDP Lite の設定 (GUI)	986
UDP Lite の設定 (CLI)	987
Cisco Hyperlocation	989
Cisco Hyperlocation について	989
Cisco Hyperlocation の設定	990
Cisco Hyperlocation の設定 (GUI)	990
Cisco Hyperlocation の設定 (CLI)	991
Cisco Air Time Fairness	993
Cisco Air Time Fairness について	993

Cisco Air Time Fairness の設定 (GUI)	997
Cisco ATF モニタ モードの設定 (GUI)	997
Cisco ATF ポリシーの設定 (GUI)	997
Cisco ATF Enforcement SSID の設定 (GUI)	998
ATF 統計情報のモニタリング (GUI)	998
Cisco Air Time Fairness の設定 (CLI)	998
Cisco Universal Small Cell 8x18 デュアルモード モジュール	1001
Cisco Universal Small Cell 8x18 デュアルモード モジュールについて	1001
Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定	1002
Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定 (GUI)	1002
Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定 (CLI)	1003
さまざまなシナリオでの USC8x18 デュアルモード モジュールの設定	1003
FlexConnect ローカルスイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (GUI)	1003
FlexConnect ローカルスイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (CLI)	1003
FlexConnect グループ ローカルスイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (GUI)	1004
FlexConnect グループ ローカルスイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (CLI)	1004
ローカルモード中央スイッチングでの USC8x18 デュアルモード モジュールの設定 (GUI)	1005
ローカルモード中央スイッチングでの USC8x18 デュアルモード モジュールの設定 (CLI)	1005
無線リソース管理の設定	1007
RRM の設定	1009
無線リソース管理について	1009
無線リソースの監視	1010
送信電力の制御	1010
最小/最大送信電力の設定による TPC アルゴリズムの無効化	1011
動的チャネル割り当て	1012
カバレッジ ホールの検出と修正	1014

RRM の利点	1014
RRM の設定について	1014
RRM の設定に関する制限	1015
RF グループ モードの設定 (GUI)	1015
RF グループ モードの設定 (CLI)	1016
送信電力制御の設定 (GUI)	1017
Off-Channel Scanning Defer の設定	1018
オフチャネル スキャンの延期について	1018
WLAN に対する Off-Channel Scanning Defer の設定	1019
WLAN に対する Off-Channel Scanning Defer の設定 (GUI)	1019
WLAN に対する Off-Channel Scanning Defer の設定 (CLI)	1019
動的チャネル割り当ての設定 (GUI)	1020
カバレッジ ホールの検出の設定 (GUI)	1024
RRM プロファイルしきい値、監視チャネル、および監視間隔の設定 (GUI)	1025
RRM の設定 (CLI)	1027
RRM 設定の表示 (CLI)	1031
RRM 問題のデバッグ (CLI)	1032
RF グループの設定	1033
RF グループについて	1033
RF グループ リーダー	1034
RF グループ名	1035
RF グループの設定	1036
RF グループ名の設定 (GUI)	1036
RF グループ名の設定 (CLI)	1036
RF グループ ステータスの表示	1037
RF グループ ステータスの表示 (GUI)	1037
RF グループ ステータスの表示 (CLI)	1038
RF グループ内の不正アクセス ポイント検出の設定	1038
RF グループ内の不正アクセス ポイント検出について	1038
RF グループ内の不正アクセス ポイント検出の設定	1039
RF グループ内の不正アクセス ポイント検出の有効化 (GUI)	1039

RF グループ内の不正アクセス ポイント検出の設定 (CLI)	1039
RRM の無効化	1041
RRM の無効化について	1041
RRM を上書きするための前提条件	1042
アクセス ポイント無線へのチャンネルおよび送信電力設定の静的割り当て	1042
チャンネルおよび送信電力設定の静的割り当て (GUI)	1042
チャンネルおよび送信電力設定の静的割り当て (CLI)	1044
Cisco ワイヤレス LAN コントローラに対するチャンネルおよび電力の動的割り当てのグローバルな無効化	1048
チャンネルおよび電力の動的割り当ての無効化 (GUI)	1048
チャンネルおよび電力の動的割り当ての無効化 (CLI)	1048
CCX 無線管理機能の設定	1049
CCX 無線管理機能について	1049
無線測定要求	1049
ロケーション調整	1050
CCX 無線管理の設定	1050
CCX 無線管理の設定 (GUI)	1050
CCX 無線管理の設定 (CLI)	1051
CCX 無線管理情報の表示 (CLI)	1052
CCX 無線管理問題のデバッグ (CLI)	1053
設定の最適化されたローミング	1055
ローミングの最適化に関する情報	1055
ローミングの最適化の制約事項	1056
ローミングの最適化の設定 (GUI)	1056
ローミングの最適化の設定 (CLI)	1057
パケットの検出しきい値設定のレシーバ起動	1059
レシーバのパケット検出開始しきい値について	1059
Rx SOP の制約事項	1060
Rx SOP の設定 (GUI)	1060
RxSOP の設定 (CLI)	1061
Cisco CleanAir の設定	1063
CleanAir について	1065

CleanAir について	1065
Cisco CleanAir システムの Cisco ワイヤレス LAN コントローラの役割	1066
Cisco CleanAir で検出できる干渉の種類	1066
永続的デバイス	1067
永続的デバイスの検出	1068
永続的デバイスの伝搬	1068
アクセス ポイントによる干渉源の検出	1068
CleanAir の前提条件と制約事項	1069
CleanAir の前提条件	1069
CleanAir の制約事項	1070
Cisco CleanAir の設定	1073
コントローラでの Cisco CleanAir の設定	1073
Cisco ワイヤレス LAN コントローラでの Cisco CleanAir の設定 (GUI)	1073
Cisco ワイヤレス LAN コントローラでの Cisco CleanAir の設定 (CLI)	1076
アクセス ポイントに対する Cisco CleanAir の設定	1080
アクセス ポイントに対する Cisco CleanAir の設定 (GUI)	1080
アクセス ポイントに対する Cisco CleanAir の設定 (CLI)	1081
干渉デバイスのモニタリング	1083
干渉デバイスをモニタリングするための前提条件	1083
干渉デバイスのモニタリング (GUI)	1083
干渉デバイスのモニタリング (CLI)	1085
アクセス ポイントによる干渉源の検出	1085
デバイスのタイプによる干渉源の検出	1086
永続的干渉源の検出	1086
永続的デバイスのモニタリング (GUI)	1086
永続的デバイスのモニタリング (CLI)	1086
無線帯域の電波品質のモニタリング	1087
無線帯域の電波品質のモニタリング (GUI)	1087
無線帯域の電波品質のモニタリング (CLI)	1088
電波品質のサマリーの表示	1088
ある無線帯域のすべてのアクセス ポイントの電波品質の表示	1088
ある無線帯域のアクセス ポイントの電波品質の表示	1088

無線帯域の電波品質（ワースト ケース）のモニタリング（GUI）	1088
無線帯域の電波品質（ワースト ケース）のモニタリング（CLI）	1089
電波品質のサマリーの表示（CLI）	1089
ある無線帯域におけるすべてのアクセス ポイントの中で最も悪い電波品質に関する情報の表示（CLI）	1089
ある無線帯域のアクセス ポイントの電波品質の表示（CLI）	1089
デバイス タイプごとのアクセス ポイントの電波品質の表示（CLI）	1089
永続的干渉源の検出（CLI）	1090
Spectrum Expert の接続の設定	1091
Spectrum Expert 接続について	1091
Spectrum Expert の設定（GUI）	1091
FlexConnect の設定	1095
FlexConnect の設定	1097
FlexConnect について	1097
FlexConnect 認証プロセス	1099
FlexConnect の制約事項	1104
FlexConnect の設定	1106
リモート サイトでのスイッチの設定	1106
FlexConnect に対するコントローラの設定	1107
FlexConnect に対するコントローラの設定（ゲストアクセスに使用される中央でスイッチされた WLAN の場合）	1108
FlexConnect に対するコントローラの設定（GUI）	1109
FlexConnect に対するコントローラの設定（CLI）	1112
FlexConnect のアクセス ポイントの設定	1114
FlexConnect のアクセス ポイントの設定（GUI）	1114
FlexConnect のアクセス ポイントの設定（CLI）	1116
WLAN 上のローカル認証用のアクセス ポイントの設定（GUI）	1119
WLAN 上のローカル認証用のアクセス ポイントの設定（CLI）	1119
クライアント デバイスの WLAN への接続	1120
FlexConnect イーサネット フォールバックの設定	1120
FlexConnect イーサネット フォールバックについて	1120
FlexConnect イーサネット フォールバックの制約事項	1121

FlexConnect イーサネット フォールバックの設定 (GUI)	1121
FlexConnect イーサネット フォールバックの設定 (CLI)	1121
FlexConnect ACL の設定	1123
アクセス コントロール リストについて	1123
FlexConnect ACL の制限	1124
FlexConnect ACL の設定 (GUI)	1125
FlexConnect ACL の設定 (CLI)	1127
FlexConnect ACL の表示およびデバッグ (CLI)	1128
FlexConnect グループの設定	1129
FlexConnect グループについて	1129
FlexConnect グループおよびバックアップ RADIUS サーバ	1130
FlexConnect グループおよび CCKM	1130
FlexConnect グループおよび Opportunistic Key Caching	1131
FlexConnect グループおよびローカル認証	1131
FlexConnect グループの設定	1133
FlexConnect グループの設定 (GUI)	1133
FlexConnect グループの設定 (CLI)	1136
FlexConnect グループの VLAN-ACL マッピングの設定	1138
FlexConnect グループの VLAN-ACL マッピングの設定 (GUI)	1138
FlexConnect グループの VLAN-ACL マッピングの設定 (CLI)	1139
VLAN-ACL マッピングの表示 (CLI)	1139
FlexConnect グループの WLAN-VLAN マッピングの設定	1139
FlexConnect グループの WLAN-VLAN マッピングの設定 (GUI)	1139
FlexConnect グループの WLAN-VLAN マッピングの設定 (CLI)	1140
FlexConnect の AAA Override の設定	1143
認証、許可、アカウントिंग オーバーライドについて	1143
FlexConnect の AAA Override に関する制約事項	1145
アクセス ポイント上の FlexConnect に対する AAA Override の設定 (GUI)	1146
アクセス ポイント上の FlexConnect に対する VLAN Override の設定 (CLI)	1147
FlexConnect アクセス ポイントに対する FlexConnect AP のアップグレードの設定	1149
FlexConnect AP のアップグレードについて	1149

FlexConnect アクセス ポイントに対する FlexConnect AP アップグレードに関する 制約事項	1150
FlexConnect AP のアップグレードの設定 (GUI)	1150
FlexConnect AP のアップグレードの設定 (CLI)	1151
モビリティ グループの設定	1153
モビリティ グループの設定	1155
モビリティについて	1155
モビリティ グループについて	1159
モビリティ グループ内でのメッセージング	1162
NAT デバイスでのモビリティ グループの使用	1162
モビリティ グループを設定するための前提条件	1163
モビリティ グループの設定 (GUI)	1165
モビリティ グループの設定 (CLI)	1167
モビリティ グループの統計の表示	1171
モビリティ グループの統計の表示 (GUI)	1171
モビリティ グループの統計の表示 (CLI)	1173
自動アンカー モビリティの設定	1175
Auto-Anchor モビリティについて	1175
注意事項および制約事項	1176
自動アンカー モビリティの設定 (GUI)	1177
自動アンカー モビリティの設定 (CLI)	1178
WLAN モビリティ セキュリティの値の検証	1181
WLAN モビリティ セキュリティの値について	1181
シンメトリック モビリティ トンネリングの使用	1183
シンメトリック モビリティ トンネリングについて	1183
注意事項および制約事項	1184
シンメトリック モビリティ トンネリングの確認 (GUI)	1184
シンメトリック モビリティ トンネリングが有効な場合の確認 (CLI)	1184
モビリティ ping テストの実行	1185
モビリティ ping テストについて	1185
注意事項および制約事項	1185
モビリティ ping テストの実行 (CLI)	1186

固定 IP アドレスを持つクライアントのダイナミック アンカーの設定 1187

固定 IP を持つクライアントのダイナミック アンカーについて 1187

固定 IP クライアントのダイナミック アンカーの機能 1187

注意事項および制約事項 1188

固定 IP クライアントのダイナミック アンカーの設定 (GUI) 1189

固定 IP クライアントのダイナミック アンカーの設定 (CLI) 1189

外部マッピングの設定 1191

外部マッピングについて 1191

外部コントローラの MAC マッピングの設定 (GUI) 1191

外部コントローラの MAC マッピングの設定 (CLI) 1191

プロキシ モバイル IPv6 の設定 1193

プロキシ モバイル IPv6 について 1193

プロキシ モバイル IPv6 の制約事項 1194

プロキシ モバイル IPv6 の設定 (GUI) 1194

プロキシ モバイル IPv6 の設定 (CLI) 1197

新しいモビリティの設定 1201

新しいモビリティについて 1201

新しいモビリティの制約事項 1202

新しいモビリティの設定 (GUI) 1202

新しいモビリティの設定 (CLI) 1204



はじめに

ここでは、このマニュアルの対象読者、構成、および表記法について説明します。また、他のマニュアルの入手方法についても説明します。この章は、次の項で構成されています。

- [対象読者](#), [li](#) ページ
- [表記法](#), [li](#) ページ
- [関連資料](#), [lii](#) ページ
- [Obtaining Documentation and Submitting a Service Request](#), [liii](#) ページ

対象読者

このマニュアルは、Cisco ワイヤレス LAN コントローラおよび Cisco Lightweight アクセス ポイントを設定および管理する経験豊富なネットワーク管理者を対象としています。

表記法

このマニュアルでは、次の表記法を使用しています。

表 1: 表記法

表記法	用途
bold フォント	コマンド、キーワード、およびユーザが入力したテキストは、 bold フォントで示しています。
<i>italic</i> フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、 <i>italic</i> フォントで示しています。
[]	角カッコの中の要素は、省略可能です。

表記法	用途
{ x y z }	いずれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示するターミナルセッションおよび情報は、courier フォントで示しています。
<>	パスワード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。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



(注) 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。



ヒント 「問題解決に役立つ情報」です。



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。

関連資料

これらのマニュアルでは、シスコ ワイヤレスに関する詳細情報を提供しています。

- Cisco ワイヤレス LAN コントローラ設定ガイド
http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html
- Cisco ワイヤレス LAN コントローラ コマンド リファレンス
http://www.cisco.com/en/US/products/ps10315/prod_command_reference_list.html
- *Cisco Wireless LAN Controller System Message Guide*
- http://www.cisco.com/en/US/products/ps10315/products_system_message_guides_list.html

- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*
http://www.cisco.com/en/US/products/ps10315/prod_release_notes_list.html
- *Cisco Wireless Mesh Access Points、 Design and Deployment Guide*
http://www.cisco.com/en/US/products/ps11451/products_implementation_design_guides_list.html
- Cisco Prime Infrastructure マニュアル
http://www.cisco.com/en/US/products/ps12239/products_documentation_roadmaps_list.html
- シスコ モビリティ サービス エンジン マニュアル
http://www.cisco.com/en/US/products/ps9806/tsd_products_support_series_home.html

シスコ ワイヤレス ソリューションに関するユーザ マニュアルにアクセスするには、このリンクをクリックしてください。

<http://www.cisco.com/cisco/web/psa/default.html?mode=prod>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: <http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.



第 部

システム管理

- [概要, 3 ページ](#)
- [使用する前に, 15 ページ](#)
- [ライセンスの管理, 59 ページ](#)
- [802.11 帯域の設定, 79 ページ](#)
- [802.11 パラメータの設定, 87 ページ](#)
- [DHCP プロキシの設定, 97 ページ](#)
- [\[DHCP Link Select\] および \[VPN Select\] の設定, 101 ページ](#)
- [SNMP の設定, 107 ページ](#)
- [アグレッシブ ロード バランシングの設定, 113 ページ](#)
- [高速 SSID 変更の設定, 117 ページ](#)
- [802.3 ブリッジの設定, 119 ページ](#)
- [マルチキャストの設定, 121 ページ](#)
- [クライアント ローミングの設定, 137 ページ](#)
- [IP-MAC アドレス バインディングの設定, 143 ページ](#)
- [Quality of Service の設定, 145 ページ](#)
- [Application Visibility and Control の設定, 153 ページ](#)

- [メディアおよび EDCA パラメータの設定, 159 ページ](#)
- [Cisco Discovery Protocol の設定, 181 ページ](#)
- [コントローラと NTP サーバの認証の設定, 191 ページ](#)
- [RFID タグ追跡の設定, 193 ページ](#)
- [コントローラのデフォルト設定へのリセット, 197 ページ](#)
- [コントローラ ソフトウェアと設定の管理, 199 ページ](#)
- [ユーザアカウントの管理, 237 ページ](#)
- [Web 認証の管理, 249 ページ](#)
- [有線ゲスト アクセスの設定, 273 ページ](#)
- [Ethernet over GRE トンネル, 281 ページ](#)
- [トラブルシューティング, 291 ページ](#)



第 1 章

概要

- [シスコワイヤレスの概要, 3 ページ](#)
- [オペレーティング システム ソフトウェア, 6 ページ](#)
- [オペレーティング システムのセキュリティ, 6 ページ](#)
- [レイヤ 2 およびレイヤ 3 の動作, 7 ページ](#)
- [Cisco ワイヤレス LAN コントローラ, 8 ページ](#)
- [コントローラ プラットフォーム, 9 ページ](#)
- [Cisco UWN ソリューション無線 LAN, 12 ページ](#)
- [ファイル転送, 13 ページ](#)
- [イーサネット経由の電源供給, 13 ページ](#)
- [Cisco Wireless LAN Controller のメモリ, 13 ページ](#)
- [Cisco Wireless LAN Controller のフェールオーバーの保護, 14 ページ](#)

シスコ ワイヤレスの概要

シスコ ワイヤレスは、企業およびサービス プロバイダーに 802.11 ワイヤレス ネットワーキング ソリューションを提供するように設計されています。シスコ ワイヤレスによって、大規模無線 LAN の展開および管理が簡素化され、他に類のないクラス最高のセキュリティインフラストラクチャを実現できます。オペレーティング システムによって、すべてのデータ クライアント、通信、およびシステム管理機能の管理、無線リソース管理 (RRM) 機能の実行、オペレーティング システムのセキュリティソリューションを使用したシステム全体のモビリティポリシーの管理、およびオペレーティング システムのセキュリティ フレームワークを使用したすべてのセキュリティ機能の調整が行われます。

シスコワイヤレス ソリューションは、Cisco ワイヤレス LAN コントローラとそれにアソシエートされている Lightweight アクセス ポイントで構成されます。これらはすべてオペレーティング シ

システムによって制御され、次のいずれか、またはすべてのオペレーティングシステムのユーザインターフェイスによって同時に管理されます。

- HTTP、HTTPS、またはこれら両方の機能をすべて備えた Cisco ワイヤレス LAN コントローラの Web ユーザ インターフェイス。個々のコントローラを設定および監視できます。
- 全機能を備えたコマンドライン インターフェイス (CLI)。個々の Cisco ワイヤレス LAN コントローラの設定と監視に使用できます。
- Cisco Prime Infrastructure。1 つ以上の Cisco ワイヤレス LAN コントローラとアソシエート先 アクセス ポイントを設定し監視するために使用できます。Prime Infrastructure には、大規模なシステムのモニタリングと制御を容易に行えるツールが備わっています。Cisco Prime Infrastructure の詳細については、http://www.cisco.com/en/US/products/ps12239/tsd_products_support_series_home.html を参照してください。
- 業界標準の SNMP V1、V2c、および V3 インターフェイスであれば、SNMP 準拠のサードパーティ製ネットワーク管理システムと併用できます。

シスコ ワイヤレス ソリューションは、クライアント データ サービス、クライアントの監視と制御、すべての不正なアクセス ポイントの検出、監視、および阻止機能をサポートします。これは、Lightweight アクセス ポイント、Cisco ワイヤレス LAN コントローラ、およびオプションの Cisco Prime Infrastructure を使用して、企業やサービスプロバイダーに無線サービスを提供します。



(注) このマニュアル内では、特に記載されていない限り、すべての Cisco ワイヤレス LAN コントローラをコントローラと呼び、すべての Cisco Lightweight アクセス ポイントをアクセス ポイントと呼びます。

シングルコントローラ展開

スタンドアロンのコントローラでは、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートすることができます。サポートされている機能は、次のとおりです。

- ネットワークに追加された Lightweight アクセス ポイントの自動検出と自動設定。
- Lightweight アクセス ポイントの完全制御。
- ネットワークを介したコントローラへの Lightweight アクセス ポイントの接続。ネットワーク機器は、アクセス ポイントに Power over Ethernet (PoE) を提供してもしなくてもかまいません。

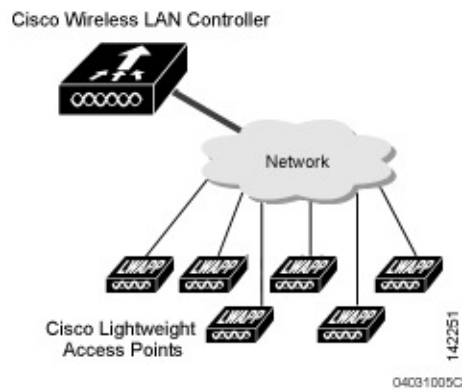
一部のコントローラでは、1 つのネットワークに障害が発生した場合、冗長ギガビットイーサネット接続を使用してこれを迂回します。



(注) 一部のコントローラは、複数の物理ポートを使用して、ネットワークの複数のサブネットに接続できます。この機能は、複数の VLAN を別々のサブネットに限定する場合などに役立ちます。

次の図は、一般的なシングルコントローラ展開を示しています。

図 1: シングルコントローラ展開



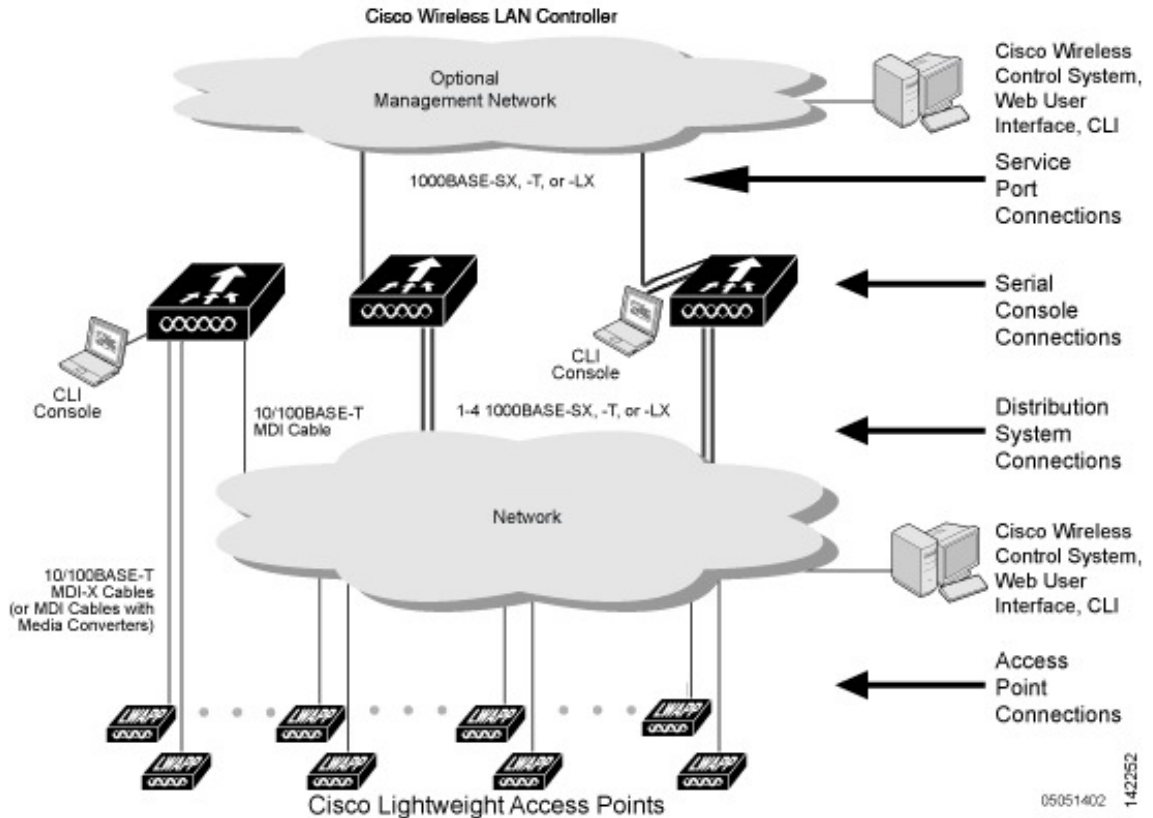
マルチコントローラ展開

すべてのコントローラは、複数のフロアとビルディングに配置されている Lightweight アクセス ポイントを同時にサポートできます。ただし、Cisco ワイヤレス LAN ソリューションの全機能が発揮されるのは、複数のコントローラが使用されている場合です。マルチコントローラシステムには、次の追加の機能があります。

- ネットワークに追加されたコントローラの RF パラメータの自動検出と自動設定。
- 同一サブネット（レイヤ 2）でのローミングとサブネット間（レイヤ 3）でのローミング。
- アクセス ポイントの負荷を減らす、任意の冗長コントローラへのアクセス ポイントの自動フェールオーバー。

次の図は、一般的なマルチコントローラ展開を示しています。また、この図では、オプションの専用管理ネットワークと、ネットワークとコントローラ間の 3 つの物理接続タイプも示しています。

図 2：一般的なマルチコントローラ展開



オペレーティング システム ソフトウェア

オペレーティング システム ソフトウェアは、コントローラと Lightweight アクセス ポイントを制御します。このソフトウェアには、オペレーティング システムのセキュリティ機能と無線リソース管理 (RRM) 機能がすべて組み込まれています。

オペレーティング システムのセキュリティ

オペレーティング システムのセキュリティ機能は、レイヤ 1、レイヤ 2、およびレイヤ 3 のセキュリティ コンポーネントを、Cisco WLAN ソリューション全体を対象とするシンプルなポリシー マネージャに統合したものです。ポリシー マネージャは、最大 16 の無線 LAN それぞれに対して、独立したセキュリティ ポリシーを作成する管理ツールです。

802.11 Static WEP の脆弱性は、次のような強固な業界標準のセキュリティ ソリューションを使用することで克服できます。

- Extensible Authentication Protocol (EAP; 拡張認証プロトコル) を使用した 802.1X ダイナミック キー。

- Wi-Fi Protected Access (WPA) ダイナミック キー。Cisco WLAN ソリューションの WPA 実装は次のとおりです。
 - Temporal Key Integrity Protocol (TKIP) と Message Integrity Code Checksum ダイナミック キー
 - WEP キー (事前共有キーのパスフレーズの有無を問わない)
- RSN (事前共有キーの有無を問わない)
- オプションの MAC フィルタリング

WEPの問題は、次のような業界標準のレイヤ3セキュリティソリューションを使用すると、さらに進んだ解決が可能です。

- パススルー VPN
- ローカルおよび RADIUS による MAC アドレス フィルタリング
- ローカルおよび RADIUS ユーザ/パスワード認証
- 手動および自動での無効化によるネットワーク サービスへのアクセスをブロック 手動で無効化するときは、クライアントの MAC アドレスを使用してアクセスをブロックします。自動による無効化は常にアクティブであり、クライアントが一定の回数の認証を繰り返し試みて失敗すると、オペレーティング システム ソフトウェアにより、設定した時間だけネットワーク サービスへのアクセスが自動的にブロックされます。この機能を使用すると、Brute-Force ログイン アタックを阻止できます。

これらとその他のセキュリティ機能は、業界標準の許可および認証方式を使用して、ビジネスクリティカルな無線 LAN トラフィックに対する最高のセキュリティを実現します。

レイヤ2およびレイヤ3の動作

コントローラと Lightweight アクセス ポイント間の Lightweight アクセス ポイント プロトコル (LWAPP) 通信は、レイヤ2またはレイヤ3で実行できます。コントローラと Lightweight アクセス ポイント間の Control and Provisioning of Wireless Access Points プロトコル (CAPWAP) 通信は、レイヤ3で実行されます。レイヤ2モードでは CAPWAP はサポートしていません。



- (注) IPv4 ネットワーク層プロトコルは、CAPWAP または LWAPP コントローラ システムでの転送でサポートされています。IPv6 (クライアント用のみ) と AppleTalk もサポートされていますが、Cisco 5500 シリーズ コントローラおよび Cisco WiSM2 のみでのサポートとなります。他のレイヤ3プロトコル (IPX、DECnet Phase IV、OSI CLNP など) およびレイヤ2 (ブリッジ) プロトコル (LAT および NetBeui など) はサポートしていません。

動作上の要件

レイヤ 3 LWAPP 通信を行う場合、コントローラと Lightweight アクセス ポイントが同一サブネットにあるときには、それらをレイヤ 2 デバイスを使用して接続します。異なるサブネットにある場合は、レイヤ 3 デバイスを使用して接続します。また、アクセス ポイントの IP アドレスが外部 DHCP サーバを介して静的または動的に割り当てられていることも必要です。

レイヤ 3 CAPWAP 通信を行う場合、コントローラと Lightweight アクセス ポイントが同一サブネットにあるときには、それらをレイヤ 2 デバイスを使用して接続します。異なるサブネットにある場合は、レイヤ 3 デバイスを使用して接続します。

設定要件

レイヤ 2 モードで Cisco ワイヤレス LAN ソリューションを稼働させている場合は、レイヤ 2 通信を制御するよう管理インターフェイスを設定する必要があります。

レイヤ 3 モードで Cisco ワイヤレス LAN ソリューションを稼働させている場合は、Lightweight アクセス ポイントおよびレイヤ 2 モード用に設定された管理インターフェイスを制御するよう AP 管理インターフェイスを設定する必要があります。

Cisco ワイヤレス LAN コントローラ

コントローラが複数展開されたネットワークに Lightweight アクセス ポイントを追加する場合、すべての Lightweight アクセス ポイントを、同一サブネット上の 1 つのマスター コントローラにアソシエートさせると便利です。そうすれば、複数のコントローラにログインして、新たに追加された Lightweight アクセス ポイントがアソシエートされているコントローラを検索する必要はなくなります。

Lightweight アクセス ポイントを追加するとき、各サブネット内の 1 つのコントローラをマスター コントローラとして割り当てることができます。同一サブネット上のマスター コントローラがアクティブである限り、プライマリ、セカンダリ、およびターシャリ コントローラが割り当てられていない新しいアクセス ポイントはすべて、マスター コントローラとのアソシエートを自動的に試みます。このプロセスについては、[Cisco Wireless LAN Controller のフェールオーバーの保護](#)、(14 ページ) で説明します。

Cisco Prime Infrastructure Web ユーザ インターフェイスを使用して、マスター コントローラを監視し、アクセス ポイントがマスター コントローラにアソシエートするのを確認できます。その後、アクセス ポイント設定を確認して、プライマリ、セカンダリ、ターシャリ コントローラをアクセス ポイントに割り当てて、プライマリ、セカンダリ、またはターシャリ コントローラに再アソシエートするように、アクセス ポイントをリポートできます。



- (注) Lightweight アクセス ポイントでは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられていない場合、レポート時には必ずマスター コントローラが最初に検索されます。マスター コントローラによって Lightweight アクセス ポイントを追加した後、プライマリ、セカンダリ、およびターシャリ コントローラを各アクセス ポイントに割り当てる必要があります。初期設定後は、すべてのコントローラのマスター設定を無効にすることを推奨します。

クライアント ロケーション

Cisco ワイヤレス LAN ソリューションで Cisco Prime Infrastructure を使用する場合、コントローラは、クライアント、不正なアクセス ポイント、不正なアクセス ポイントクライアント、無線周波数 ID (RFID) タグ ロケーションを定期的にチェックし、そのロケーションを Cisco Prime Infrastructure のデータベースに保存します。

コントローラ プラットフォーム

コントローラは、802.11a/n/ac プロトコルおよび 802.11b/g/n プロトコルをサポートする、企業向けの高性能無線スイッチング プラットフォームです。無線リソース管理 (RRM) 機能が搭載されているオペレーティング システムの制御下でコントローラを稼働することにより、802.11 RF 環境でのリアルタイムの変化に自動対応する Cisco UWN ソリューションが実現されます。コントローラは、高性能なネットワークおよびセキュリティハードウェアを中心に設計されており、他に例のないセキュリティを備えた信頼性の高い 802.11 企業ネットワークを実現します。

次のコントローラがサポートされています。

Cisco 2500 シリーズ コントローラ

Cisco 2500 シリーズ Wireless Controller は、Cisco Lightweight アクセス ポイントおよび Cisco Prime Infrastructure と組み合わせて使用することで、システム全体を対象とする無線 LAN 機能を提供します。Cisco 2500 シリーズのコントローラは、ワイヤレス アクセス ポイントと他のデバイスとの間でリアルタイムの通信を行い、中央集中型セキュリティポリシー、ゲストアクセス、ワイヤレス侵入防御システム (wIPS)、コンテキスト認識型 (ロケーション)、RF 管理、音声やビデオなどのモビリティサービスの QoS、およびテレワーカー ソリューションに対する OEAP のサポートなどの機能を備えています。

Cisco 2500 シリーズ コントローラの詳細については、<http://www.cisco.com/en/US/products/ps11630/index.html>を参照してください。

Cisco 5500 シリーズ コントローラ

現在、Cisco 5500 シリーズ Wireless LAN Controller には 1 つのモデル (5508) があります。Cisco 5500 シリーズ ワイヤレス コントローラは、中規模から大規模の企業およびキャンパス環境にお

いてミッションクリティカルなワイヤレスネットワークのサービスをシステム全体で実現する、拡張性と柔軟性に優れたプラットフォームです。

Cisco 5500 シリーズ コントローラには、電源装置を 1 つまたは 2 つ装着できます。コントローラに電源装置を 2 つ装着しておけば、電源装置が冗長構成になり、一方の電源装置に障害が発生しても、もう一方の電源装置から引き続きコントローラに電力を供給できます。

Cisco 5500 シリーズ コントローラの詳細については、http://www.cisco.com/en/US/products/ps10315/tsd_products_support_series_home.htmlを参照してください。

Cisco Flex 7500 シリーズ コントローラ

Cisco FLEX 7500 シリーズ コントローラを使用すると、地理的に分散したサイトを対象として、スケーラブルで安全なフル機能を持った FlexConnect ネットワーク サービスを展開できます。Cisco Flex 7500 シリーズ コントローラは、データセンター内の複雑なセキュリティ、管理、設定、およびトラブルシューティング処理を仮想化し、これらのサービスを各ストアに透過的に拡張します。展開に Cisco FLEX 7500 シリーズ コントローラを使用すれば、設定、管理、拡張が容易になります。

Cisco Flex 7500 シリーズ コントローラは、ブランチ ネットワーク内に FlexConnect ソリューションを導入する際のスケール要件を満たすように設計されています。Cisco ワイヤレスでは、FlexConnect と モニタ モード という 2 種類の導入モデルをサポートしています。FlexConnect は、アクセス ポイントが中央のコントローラによって制御および管理されながら、データはローカルにスイッチングできるようにすることで、ワイヤレスブランチネットワークをサポートするように設計されています。これは、規模が大きいときにコスト効率の良い FlexConnect ソリューションを実現することを目指しています。

制約事項

FlexConnect のみを導入する場合、次の制限が適用されます。

- マルチキャスト - ユニキャストは使用可能な唯一のデフォルト モードです。
- グローバル マルチキャストおよび IGMP スヌーピングはサポートされていません。
- IPv6 および Generic Attribute Registration Protocol (GARP) はサポートされていますが、マルチキャスト データはサポートされていません。

Cisco Flex 7500 シリーズ コントローラの詳細については、http://www.cisco.com/en/US/products/ps11635/tsd_products_support_series_home.htmlを参照してください。

Cisco 8500 シリーズ コントローラ

Cisco 8500 シリーズ コントローラは、ローカルモード、FlexConnect モード、およびメッシュモードをサポートして 7.3 リリースで導入されました。Cisco 8500 シリーズ コントローラは、拡張性と柔軟性に優れたプラットフォームであり、大規模なサービスプロバイダーや大規模なキャンパスへの導入においてミッションクリティカルなワイヤレス ネットワークを実現します。



- (注) 8510 コントローラは DC 電源を使用するため、各国固有の電源コードでは使用できません。そのため、12 ゲージ線を使用して、DC 電源に接続することを推奨します。

制約事項

- ローカル モードのみの導入：マルチキャスト-マルチキャストがデフォルトのモードです。
- ローカルおよび FlexConnect モードの導入
 - FlexConnect モード AP で IPv6 が必要な場合は、グローバル マルチキャストを無効にし、マルチキャスト-ユニキャスト モードに変更します。IPv6 および Generic Attribute Registration Protocol (GARP) は動作しますが、マルチキャストデータとビデオストリーミングはコントローラ間ではサポートされていません。
 - FlexConnect AP で IPv6 および GARP が不要でない場合は、マルチキャスト-マルチキャストにモードを変更し、グローバル マルチキャストおよび IGMP/MLD スヌーピングを有効にしてください。FlexConnect AP では、IPv6、GARP、マルチキャスト データ、VideoStream をサポートしています。

Cisco 8500 シリーズ コントローラの詳細については、http://www.cisco.com/en/US/products/ps12722/tsd_products_support_series_home.htmlを参照してください。

Cisco Virtual Wireless LAN Controller

Virtual Wireless LAN Controller は、業界標準の仮想化インフラストラクチャに準拠したハードウェアで実行できるソフトウェアです。仮想ワイヤレス LAN コントローラには、ユーザが要件に基づいてハードウェアを選択できる柔軟性があります。



- (注) Virtual Wireless LAN Controller のスナップショットを取得すると、VMware によってアクティビティが約 15 秒間一時停止されます。この間、AP は Virtual Wireless LAN Controller から切断されます。

Cisco 仮想ワイヤレス LAN コントローラの詳細については、http://www.cisco.com/en/US/products/ps12723/tsd_products_support_series_home.html参照してください。

Cisco ワイヤレス サービス モジュール 2

Cisco ワイヤレス サービス モジュール 2 (WiSM2) は、非常に優れたパフォーマンス、セキュリティ、および拡張性を実現する中規模から大規模の単一サイト WLAN 展開を提供して、ミッションクリティカルなワイヤレス ビジネス コミュニケーションをサポートします。これはハードウェアのコストの削減に役立ち、また無線ネットワークの運用と所有に関する総コストを減らすことができる柔軟な設定オプションが用意されています。

Cisco WiSM2 の詳細については、<http://www.cisco.com/en/US/products/ps11634/index.html>を参照してください。

Cisco Services Ready Engine (SRE) の Cisco Wireless Controller

Cisco Services Ready Engine (SRE) の Cisco ワイヤレス コントローラ アプリケーションを利用すると、中小企業やブランチ オフィスのシステム全体の規模でワイヤレス機能を活用できます。SRE の Cisco ワイヤレス コントローラはエン트리 レベルのコントローラであり、802.11n および 802.11ac のパフォーマンスとスケーラビリティを兼ね備えています。既存のネットワークとシームレスに統合できるため、総所有コストを抑え、投資を保護することができます。Cisco SRE モジュールは、第 2 世代シスコ サービス統合型ルータ (ISR G2) 用のルータ ブレードであり、モジュールの Cisco ワイヤレス コントローラ アプリケーションをリモートからいつでもプロビジョニングすることができます。この機能は、ワイヤレスをオンデマンドで迅速に導入し、運用コストを抑制し、ブランチ オフィスのインフラストラクチャを統合するのに役立ちます。

このコントローラは、Cisco Aironet アクセス ポイント、Cisco Prime Infrastructure、および Cisco Mobility Services Engine (MSE) 間のリアルタイム通信を提供し、一元化されたセキュリティ ポリシー、ワイヤレス侵入防御システム (wIPS) 機能、受賞歴のある RF 管理機能、ロケーショントラッキングのためのコンテキスト認識型機能、音声とビデオのための Quality of Service (QoS) を備えています。

Cisco Services Ready Engine (SRE) の Cisco ワイヤレス コントローラ アプリケーションの詳細については、<http://www.cisco.com/en/US/products/ps11716/index.html>を参照してください。

Cisco UWN ソリューション無線 LAN

Cisco UWN ソリューションでは、Lightweight アクセス ポイント全体に対して、最大 512 の WLAN を制御できます。各 WLAN には、それぞれ異なる WLAN ID (1 ~ 512)、それぞれ異なるプロファイル名、および WLAN SSID が割り当てられます。また、一意のセキュリティ ポリシーを割り当てることもできます。Lightweight アクセス ポイントでは、すべてのアクティブな Cisco UWN ソリューション WLAN SSID をブロードキャストし、各 WLAN に定義されているポリシーを適用します。



(注) コントローラが最適な性能と容易な管理で動作できるよう、無線 LAN と管理インターフェイスにはそれぞれ別の VLAN セットを割り当てることをお勧めします。

Cisco UWN ソリューションで無線による管理を有効にすると、CLI と Telnet、HTTP/HTTPS、および SNMP を使用して、有効になった無線 LAN 全体のシステムを管理できるようになります。

ファイル転送

オペレーティングシステムのコード、設定、および証明書ファイルは、GUI、CLI、またはCisco Prime Infrastructure を使用して、コントローラにアップロードしたり、コントローラからダウンロードしたりできます。

イーサネット経由の電源供給

Lightweight アクセス ポイントは、イーサネット ケーブルを介して、802.3af 準拠の Power over Ethernet (PoE) デバイスから電力供給を受けることができます。これにより、個々のデバイスへの電力供給や、余分な配線、コンジット、コンセントにかかるコストが低減され、設置時間を短縮できます。3600 シリーズ アクセス ポイントの 802.11ac 無線は、803.af の電源が十分でないため 803.at 互換の PoE デバイスに依存しなければなりません。PoE 機能を使用すると、AC コンセントの近くに Lightweight アクセス ポイントやその他の電力供給を要する装置を取り付ける必要がなくなるため、アクセス ポイントをより柔軟に配置して、最大限のカバレッジを得ることができます。

PoE を使用している場合は、1 本の CAT-5 ケーブルで各 Lightweight アクセス ポイントから PoE 機能が搭載されているネットワーク要素 (PoE 電源ハブや、Cisco WLAN ソリューションのシングルライン PoE インジェクタなど) に接続します。PoE 機器で Lightweight アクセス ポイントが PoE 対応であると判断された場合は、使用されていないイーサネットケーブルペアを使って、48 VDC の電力が Lightweight アクセス ポイントに供給されます。

PoE ケーブルの長さは、100BASE-T 仕様では 100 m、10BASE-T 仕様では 200 m に制限されています。

Cisco Wireless LAN Controller のメモリ

コントローラには 2 種類のメモリが搭載されています。揮発性 RAM には、現在のアクティブなコントローラ設定が保持され、NVRAM (非揮発性 RAM) にはリブート設定が保持されます。コントローラのオペレーティング システムを設定すると、揮発性 RAM の内容が変更されます。したがって、揮発性 RAM の設定を NVRAM に保存し、コントローラが現在の設定でリブートされるようにする必要があります。

次の処理を行うときは、どちらのメモリを編集しているか理解していることが重要になります。

- 設定ウィザードの使用方法
- コントローラの設定のクリア
- 設定の保存
- コントローラのリセット
- CLI からのログアウト

Cisco Wireless LAN Controller のフェールオーバーの保護

インストール時に、すべての Lightweight アクセス ポイントを専用のコントローラに接続して、正式な運用のために各 Lightweight アクセス ポイントを設定することをお勧めします。この手順では、プライマリ、セカンダリ、ターシャリ コントローラについてそれぞれの Lightweight アクセス ポイントを設定し、設定したモビリティ グループ情報を格納できるようにします。

フェールオーバーの回復時には、次の処理が実行されます。

- 設定されているアクセス ポイントでは、プライマリ、セカンダリ、ターシャリのコントローラへの接続を試み、さらにモビリティ グループ内の他のコントローラの IP アドレスへの接続を試みます。
- DNS は、コントローラの IP アドレスで解決されます。
- DHCP サーバは、コントローラの IP アドレス (DHCP オファァーのベンダー固有のオプション 43) を取得します。

マルチコントローラの導入では、1 台のコントローラに障害が発生した場合、アクセス ポイントは次のことを行います。

- Lightweight アクセス ポイントは、プライマリ、セカンダリ、またはターシャリ コントローラが割り当てられている場合、そのコントローラにアソシエートを試みます。
- アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられていない場合、またはプライマリ、セカンダリ、ターシャリ コントローラが使用できない場合には、マスター コントローラにアソシエートを試みます。
- アクセス ポイントがマスター コントローラを検出できなかった場合は、格納されているモビリティ グループ メンバに IP アドレスで接続を試みます。
- モビリティ グループ メンバが使用可能な場合、および Lightweight アクセス ポイントにプライマリ、セカンダリ、ターシャリ コントローラが割り当てられておらず、アクティブなマスター コントローラがない場合は、最も負荷の少ないコントローラにアソシエートを試み、そのディスカバリ メッセージに応答します。

コントローラが展開されている場合には、1 台のコントローラに障害が発生しても、アクティブなアクセス ポイントのクライアントセッションがただちにドロップする一方で、ドロップしたアクセス ポイントが別のコントローラにアソシエートするため、クライアントデバイスはすぐに再アソシエートと再認証を行うことができます。

ハイアベイラビリティの詳細については、http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a00809a3f5d.shtml を参照してください。



第 2 章

使用する前に

- [設定ウィザードを使用したコントローラの設定, 15 ページ](#)
- [コントローラのコンソールポートの接続, 16 ページ](#)
- [コントローラの設定 \(GUI\) , 17 ページ](#)
- [コントローラの設定 : CLI 設定ウィザードの使用, 28 ページ](#)
- [コントローラ Web GUI の使用方法, 32 ページ](#)
- [外部で生成した SSL 証明書のロード, 35 ページ](#)
- [外部で生成した SSL 証明書について, 35 ページ](#)
- [SSL 証明書のロード \(GUI\) , 36 ページ](#)
- [SSL 証明書のロード \(CLI\) , 37 ページ](#)
- [コントローラ CLI の使用方法, 38 ページ](#)
- [コントローラ CLI へのログイン, 39 ページ](#)
- [設定のないコントローラでの AutoInstall 機能の使用, 42 ページ](#)
- [AutoInstall 機能について, 42 ページ](#)
- [注意事項および制約事項, 43 ページ](#)
- [コントローラのシステムの日時の管理, 46 ページ](#)
- [Telnet および Secure Shell セッションの設定, 51 ページ](#)
- [コントローラの無線管理, 57 ページ](#)

設定ウィザードを使用したコントローラの設定

設定ウィザードでは、コントローラ上での基本的な設定を行うことができます。このウィザードは、コントローラを購入した直後やコントローラを工場出荷時のデフォルトにリセットした後に実行します。設定ウィザードは、GUI と CLI の両方の形式で使用できます。

コントローラのコンソールポートの接続

基本的な動作ができるようにコントローラを設定するには、VT-100ターミナルエミュレーションプログラム（HyperTerminal、ProComm、Minicom、Tip など）を実行する PC にコントローラを接続する必要があります。



- (注) Cisco 5500 シリーズ コントローラでは、RJ-45 コンソールポートと USB コンソールポートのどちらでも使用できます。USB コンソールポートを使用する場合は、5 ピン ミニタイプ B コネクタをコントローラの USB コンソールポートに接続し、もう一端を PC の USB タイプ A ポートに接続します。Windows PC を USB ポートに接続するのが初めての場合は、USB コンソール ドライバをインストールするための画面が表示されます。インストール画面の指示に従って、ドライバをインストールしてください。USB コンソール ドライバは PC 上の COM ポートにマッピングされるので、この COM ポートにターミナルエミュレータアプリケーションをマッピングする必要があります。

- ステップ 1** ヌルモデム シリアル ケーブルの一端をコントローラのコンソールポートに接続し、もう一端を PC のシリアルポートに接続します。
- ステップ 2** PC の VT-100 ターミナルエミュレーションプログラムを起動します。
- ステップ 3** ターミナルエミュレーションプログラムのパラメータを次のとおりに設定します。
- 9600 ボー
 - 8 データ ビット
 - 1 ストップ ビット
 - パリティなし
 - ハードウェア フロー制御なし
- ステップ 4** AC 電源コードをコントローラに接続し、アース付き 100 ~ 240 VAC、50/60 Hz の電源コンセントに差し込み、電源を入れます。起動スクリプトによって、オペレーティング システム ソフトウェアの初期化（コードのダウンロードおよび電源投入時自己診断テスト）および基本設定が表示されます。コントローラの電源投入時自己診断テストに合格した場合は、起動スクリプトによって設定ウィザードが実行されます。画面の指示に従って、基本設定を入力してください。

コントローラの設定 (GUI)

ステップ 1 PC をサービス ポートに接続し、コントローラと同じサブネットを使用するように設定します。

ステップ 2 PC 上で Internet Explorer 6.0 SP1 以上または Firefox 2.0.0.11 以上を起動して、アドレス行に「http://192.168.1.1」と入力します。すると、設定ウィザードが表示されます。

(注) サービスポートインターフェイスを使用する場合は、HTTP と HTTPS の両方を使用できます。HTTPS はデフォルトで有効になっており、HTTP も有効にすることができます。サービスポートインターフェイスに関連付けるデフォルト IP アドレスは 192.168.1.1 です。

図 3: 設定ウィザード : [System Information] 画面

The screenshot shows the 'System Information' step of the Configuration Wizard. The interface includes a 'System Name' text box, an 'Administrative User' section with 'User Name (e.g. admin)' (containing 'admin'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots) text boxes. A 'Next' button is located in the top right corner. The Cisco logo is in the top left, and the ID number 252063 is on the right side.

ステップ 3 [System Name] テキスト ボックスに、このコントローラに割り当てる名前を入力します。ASCII 文字を最大 31 文字入力できます。

ステップ 4 [User Name] テキスト ボックスに、このコントローラに割り当てる管理者ユーザ名を入力します。ASCII 文字を最大 24 文字入力できます。デフォルトのユーザ名は *admin* です。

ステップ 5 [Password] テキスト ボックスおよび [Confirm Password] テキスト ボックスに、このコントローラに割り当てる管理者パスワードを入力します。ASCII 文字を最大 24 文字入力できます。デフォルトのパスワードは *admin* です。

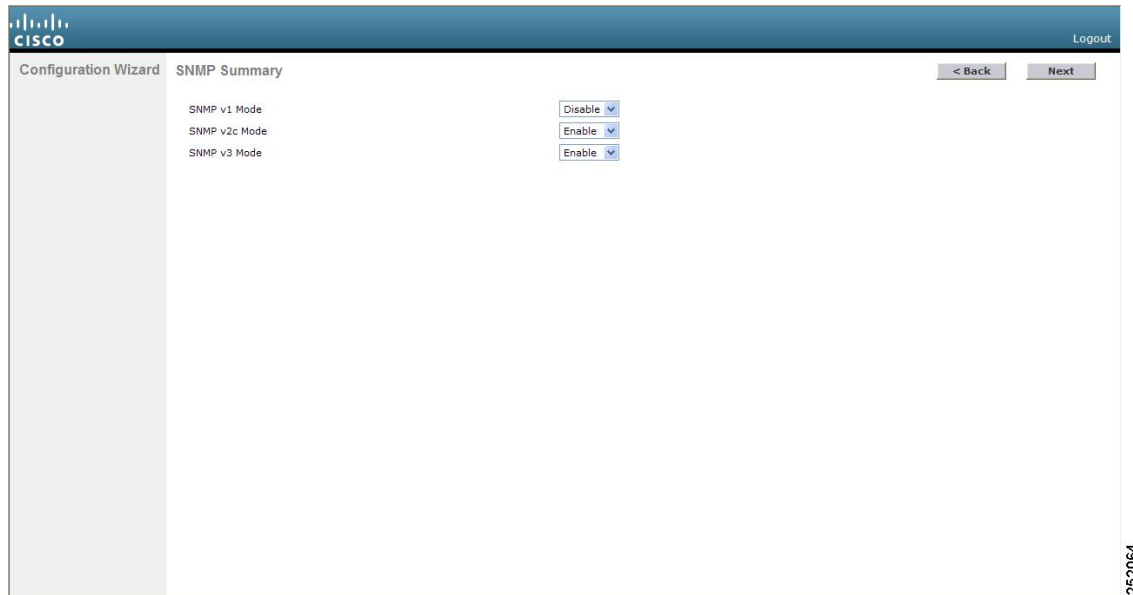
リリース 7.0.116.0 以降、次のパスワード ポリシーが実装されています。

- パスワードには、次の中から少なくとも 3 つのクラスの文字を含める必要があります。
 - 小文字の英字
 - 大文字の英字

- 数字
 - 特殊文字
- パスワードには同じ文字を連続して 4 回以上繰り返すことはできません。
 - 新規のパスワードとして、関連するユーザ名と同じものやユーザ名を逆にしたものは使用できません。
 - パスワードには、Cisco という語の大文字を小文字に変更したものや文字の順序を入れ替えたもの (cisco、ocsic など) を使用できません。さらに、i の代わりに 1、I または !、o の代わりに 0、または s の代わりに \$ を使用することはできません。

ステップ 6 [Next] をクリックします。[SNMP Summary] 画面が表示されます。

図 4: 設定ウィザード: [SNMP Summary] 画面



ステップ 7 このコントローラに対して簡易ネットワーク管理プロトコル (SNMP) v1 モードを有効にする場合は、[SNMP v1 Mode] ドロップダウンリストから [Enable] を選択します。有効にしない場合は、このパラメータを [Disable] のままにします。

(注) SNMP とは、IP ネットワーク上のノード (サーバ、ワークステーション、ルータ、スイッチなど) を管理するプロトコルです。現時点では、SNMP のバージョンには SNMPv1、SNMPv2c、SNMPv3 の 3 つがあります。

- ステップ 8** このコントローラに対して SNMPv2c モードを有効にするには、このパラメータを [Enable] のままにします。有効にしない場合は、[SNMP v2c Mode] ドロップダウン リストから [Disable] を選択します。
- ステップ 9** このコントローラに対して SNMPv3 モードを有効にするには、このパラメータを [Enable] のままにします。有効にしない場合は、[SNMP v3 Mode] ドロップダウン リストから [Disable] を選択します。
- ステップ 10** [Next] をクリックします。
- ステップ 11** 次のメッセージが表示されたら、[OK] をクリックします。

Default values are present for v1/v2c community strings.
Please make sure to create new v1/v2c community strings once the system comes up.
Please make sure to create new v3 users once the system comes up.
[Service Interface Configuration] 画面が表示されます。

図 5 : 設定ウィザード : [Service Interface Configuration] 画面

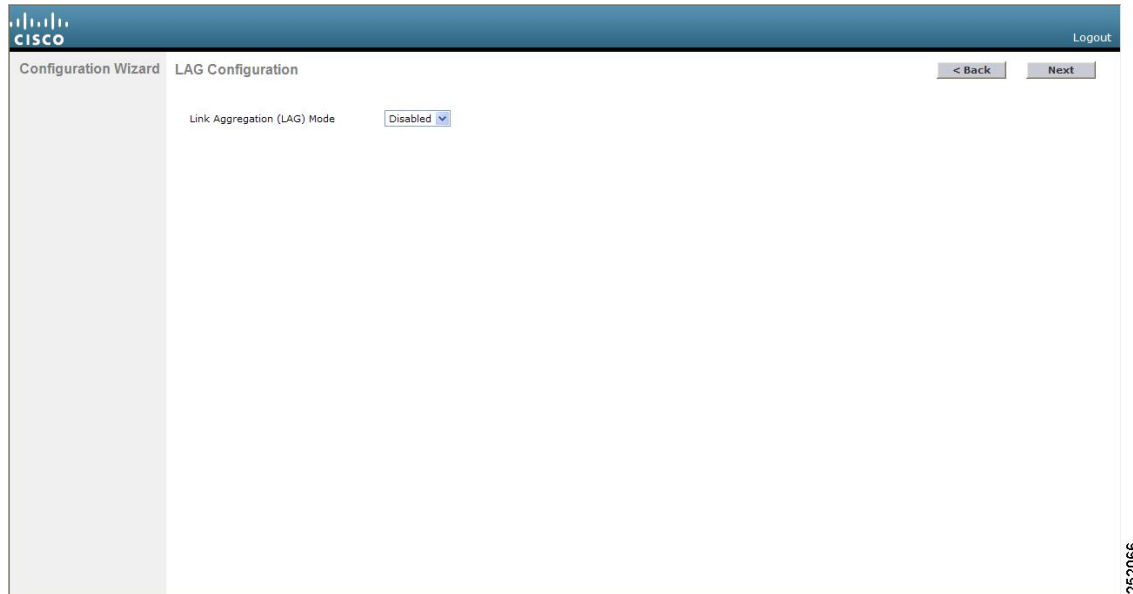
The screenshot shows the 'Service Interface Configuration' screen in the Cisco Configuration Wizard. The interface name is 'service-port' and the MAC address is '00:24:97:ccc:71:e1'. Under 'Interface Address', the 'DHCP Protocol' checkbox is checked, indicating it is enabled. The IP address is set to '192.168.1.1' and the netmask is '255.255.255.0'. There are 'Back' and 'Next' buttons at the top right of the configuration area.

- ステップ 12** コントローラのサービスポートインターフェイスの IP アドレスを DHCP サーバから取得するように設定するには、[DHCP Protocol Enabled] チェックボックスを選択します。サービスポートを使用しない場合、またはサービスポートに固定 IP アドレスを割り当てる場合は、このチェックボックスをオフにします。
- (注) サービスポートインターフェイスは、サービスポートを介した通信を制御します。このインターフェイスの IP アドレスは、管理インターフェイスとは異なるサブネット上のものであることが必要です。このように設定されていれば、コントローラを直接、または専用の管理ネットワーク経由で管理できるので、ネットワークがダウンしているときもサービスアクセスが可能になります。
- ステップ 13** 次のいずれかの操作を行います。
- DHCP を有効にした場合は、[IP Address] テキストボックスと [Netmask] テキストボックスの入力内容をクリアして空白にします。

- DHCP を無効にした場合は、[IP Address] テキスト ボックスと [Netmask] テキスト ボックスにサービスポートの固定 IP アドレスとネットマスクを入力します。

ステップ 14 [Next] をクリックします。
[LAG Configuration] 画面が表示されます。

図 6 : 設定ウィザード : [LAG Configuration] 画面



ステップ 15 リンク集約 (LAG) を有効にするには、[Link Aggregation (LAG) Mode] ドロップダウンリストから [Enabled] を選択します。LAG を無効にするには、このテキスト ボックスを [Disabled] のままにします。

ステップ 16 [Next] をクリックします。

[Management Interface Configuration] 画面が表示されます。

図 7: 設定ウィザード : [Management Interface Configuration] 画面

The screenshot shows the 'Management Interface Configuration' screen in the Cisco Configuration Wizard. The interface is divided into several sections with input fields:

- General Information:** Interface Name (management), MAC Address (00:24:97:cc:71:e0).
- Interface Address:** VLAN Identifier (0), IP Address (209.165.200.225), Netmask (255.255.255.224), Gateway (209.165.200.225).
- Physical Information:** Port Number (1), Backup Port (0), Active Port (1).
- DHCP Information:** Primary DHCP Server (1.1.1.1), Secondary DHCP Server (0.0.0.0).

Navigation buttons for '< Back' and 'Next >' are located at the top right. The Cisco logo and 'Configuration Wizard' are in the top left. A 'Logout' link is in the top right corner. A vertical ID '252067' is on the right edge.

(注) 管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。

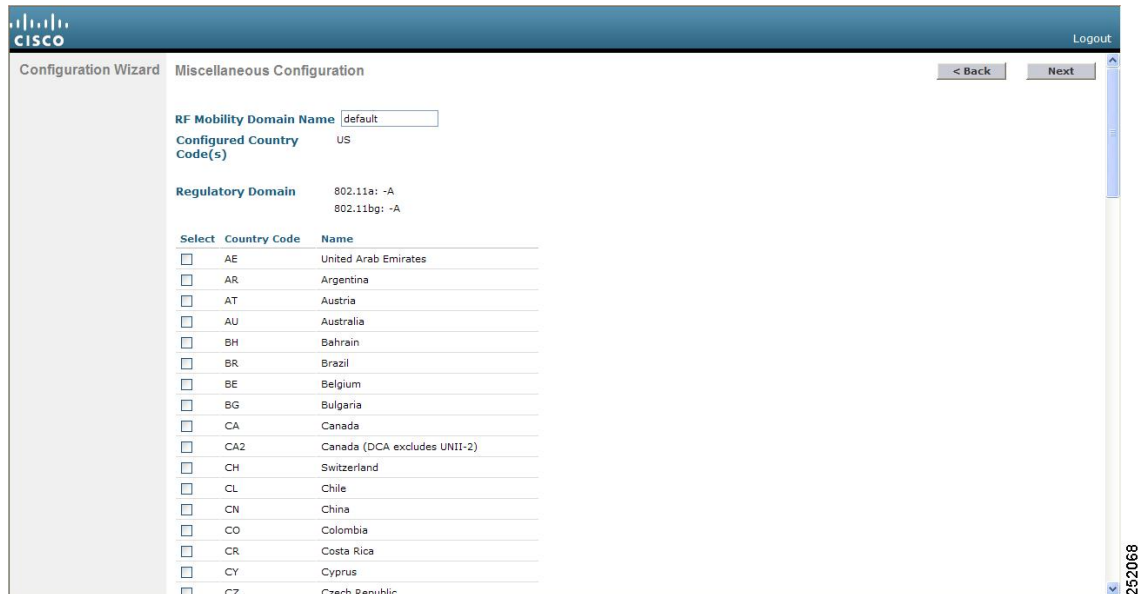
- ステップ 17** [VLAN Identifier] テキスト ボックスに、管理インターフェイスの VLAN 識別子 (有効な VLAN 識別子) を入力します。タグなし VLAN の場合は、0 を入力します。VLAN 識別子は、スイッチ インターフェイス設定と一致するように設定する必要があります。
- ステップ 18** [IP Address] テキスト ボックスに、管理インターフェイスの IP アドレスを入力します。
- ステップ 19** [Netmask] テキスト ボックスに、管理インターフェイス ネットマスクの IP アドレスを入力します。
- ステップ 20** [Gateway] テキスト ボックスに、デフォルト ゲートウェイの IP アドレスを入力します。
- ステップ 21** [Port Number] テキスト ボックスに、管理インターフェイスに割り当てられたポート番号を入力します。各インターフェイスは、少なくとも 1 つのプライマリ ポートにマップされます。
- ステップ 22** [Backup Port] テキスト ボックスに、管理インターフェイスに割り当てられたバックアップ ポートの番号を入力します。管理インターフェイスのプライマリ ポートに障害が発生した場合は、管理インターフェイスは自動的にバックアップ ポートに移動します。
- ステップ 23** [Primary DHCP Server] テキスト ボックスに、クライアント、コントローラの管理インターフェイス、およびサービス ポート インターフェイス (使用する場合) の IP アドレスを取得するためのデフォルト DHCP サーバの IP アドレスを入力します。
- ステップ 24** [Secondary DHCP Server] テキスト ボックスに、クライアント、コントローラの管理インターフェイス、およびサービス ポート インターフェイス (使用する場合) の IP アドレスを取得するためのセカンダリ DHCP サーバの IP アドレスをオプションで入力します。
- ステップ 25** [Next] をクリックします。[AP-Manager Interface Configuration] 画面が表示されます。

(注) Cisco 5500 シリーズ コントローラの場合は、この画面は表示されません。このシリーズは AP マネージャ インターフェイスの設定が必要ないからです。管理インターフェイスは、デフォルトで AP マネージャ インターフェイスとして動作します。

ステップ 26 [IP Address] テキスト ボックスに、AP マネージャ インターフェイスの IP アドレスを入力します。

ステップ 27 [Next] をクリックします。[Miscellaneous Configuration] 画面が表示されます。

図 8 : 設定ウィザード : [Miscellaneous Configuration] 画面



ステップ 28 [RF Mobility Domain Name] テキスト ボックスに、コントローラが所属するモビリティ グループ/RF グループの名前を入力します。

(注) ここで入力する名前は、モビリティ グループと RF グループの両方に割り当てられますが、これらのグループは同じではありません。どちらのグループもコントローラの集合を定義するものですが、目的が異なります。RF グループ内のすべてのコントローラは通常同じモビリティ グループに属し、モビリティ グループ内のすべてのコントローラは同じ RF グループに属します。ただし、モビリティ グループはスケラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現するのに対して、RF グループはスケラブルでシステム全体にわたる動的な RF 管理を実現します。

ステップ 29 [Configured Country Code(s)] テキストボックスに、コントローラが使用される国のコードが表示されます。別の国で使用する場合は、その国のチェックボックスを選択します。

(注) 複数の国のアクセス ポイントを 1 つのコントローラで管理する場合は、複数の Country Code を選択できます。設定ウィザードの実行後、コントローラに join している各アクセス ポイントに特定の国を割り当てる必要があります。

ステップ 30 [Next] をクリックします。

ステップ 31 次のメッセージが表示されたら、[OK] をクリックします。

Warning! To maintain regulatory compliance functionality, the country code setting may only be modified by a network administrator or qualified IT professional.

Ensure that proper country codes are selected before proceeding.?

[Virtual Interface Configuration] 画面が表示されます。

図 9 : 設定ウィザード : [Virtual Interface Configuration] 画面

ステップ 32 [IP Address] テキスト ボックスに、コントローラの仮想インターフェイスの IP アドレスを入力します。 IP アドレスは、未割り当ての架空のアドレスを入力します。

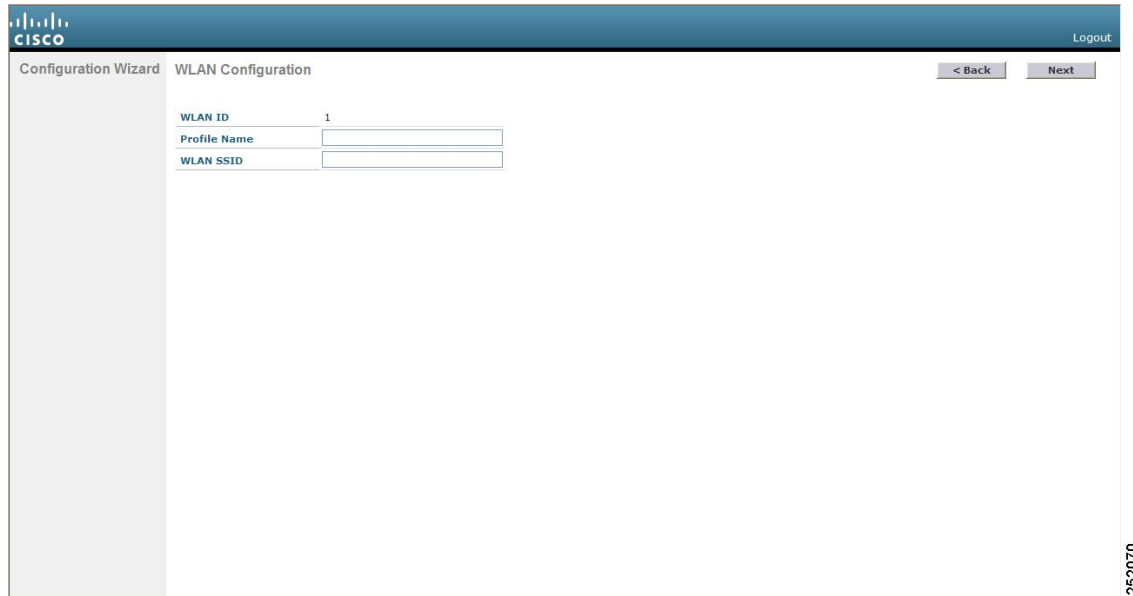
(注) 仮想インターフェイスは、モビリティ管理、DHCP リレー、およびゲスト Web 認証や VPN 終端などレイヤ 3 の組み込みセキュリティをサポートするために使用されます。同一のモビリティグループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。

ステップ 33 [DNS Host Name] テキスト ボックスに、レイヤ 3 Web 認証が有効化されているときの証明書のソース確認に使用されるドメイン ネーム システム (DNS) ゲートウェイの名前を入力します。

(注) 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスの DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

ステップ 34 [Next] をクリックします。[WLAN Configuration] 画面が表示されます。

図 10 : 設定ウィザード : [WLAN Configuration] 画面



ステップ 35 [Profile Name] テキスト ボックスに、この WLAN に割り当てるプロファイル名を英数字 32 文字以内で入力します。

ステップ 36 [WLAN SSID] テキスト ボックスに、ネットワーク名つまりサービスセット ID (SSID) を英数字 32 文字以内で入力します。SSID が設定されると、コントローラの基本機能が使用可能になり、そのコントローラに join されたアクセス ポイントの無線を有効化できるようになります。

ステップ 37 [Next] をクリックします。

ステップ 38 次のメッセージが表示されたら、[OK] をクリックします。

Default Security applied to WLAN is: [WPA2 (AES)] [Auth(802.1x)]. You can change this after the wizard is complete and the system is rebooted.?

[RADIUS Server Configuration] 画面が表示されます。

図 11 : 設定ウィザード : [RADIUS Server Configuration] 画面

The screenshot displays the 'RADIUS Server Configuration' page within a 'Configuration Wizard'. The page includes the following fields and controls:

- Server IP Address**: A text input field.
- Shared Secret Format**: A dropdown menu currently set to 'ASCII'.
- Shared Secret**: A text input field.
- Confirm Shared Secret**: A text input field.
- Port Number**: A text input field containing the value '1812'.
- Server Status**: A dropdown menu currently set to 'Disabled'.

Navigation buttons at the top right include '< Back', 'Apply', and 'Skip'. A 'Logout' link is also present in the top right corner. The Cisco logo is visible in the top left corner. A vertical ID number '262071' is located on the right side of the page.

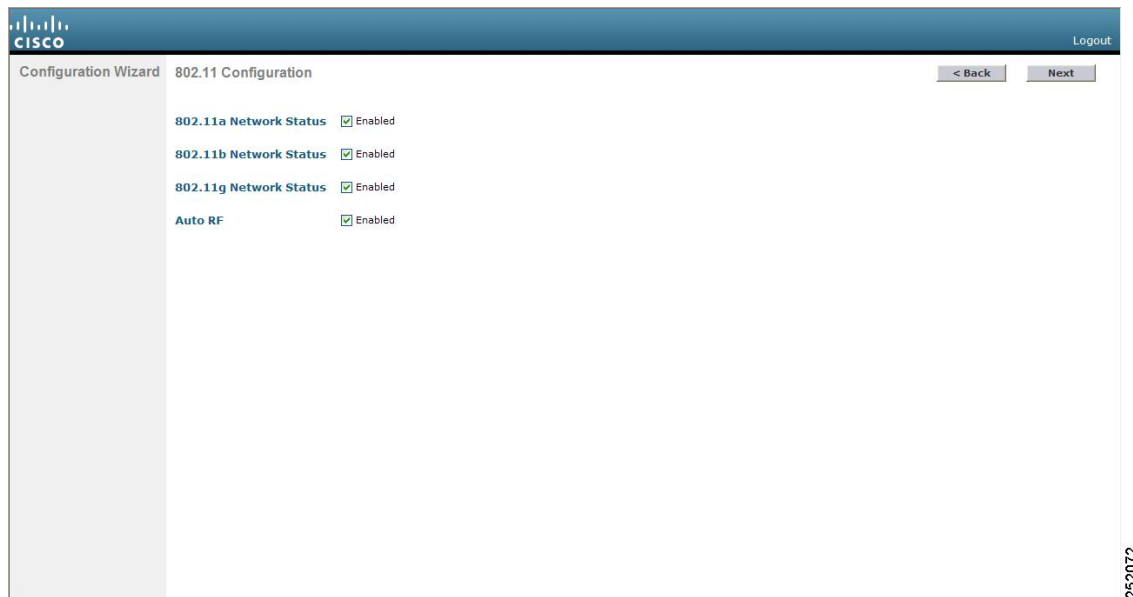
ステップ 39 [Server IP Address] テキスト ボックスに、RADIUS サーバの IP アドレスを入力します。

ステップ 40 [Shared Secret Format] ドロップダウン リストから、共有秘密の形式として [ASCII] または [Hex] を選択します。

(注) セキュリティ上の問題があった場合、[Shared Secret Format] ドロップダウン リストから共有秘密の形式として [HEX] を選択しても、RADIUS 共有秘密キーは [ASCII] モードに戻ります。

- ステップ 41 [Shared Secret] テキストボックスと [Confirm Shared Secret] テキストボックスに、RADIUS サーバによって使用される秘密キーを入力します。
- ステップ 42 [Port Number] テキストボックスに、RADIUS サーバの通信ポートを入力します。デフォルト値は 1812 です。
- ステップ 43 RADIUS サーバを有効にするには、[Server Status] ドロップダウンリストから [Enabled] を選択します。RADIUS サーバを無効にするには、このテキストボックスを [Disabled] のままにします。
- ステップ 44 [Apply] をクリックします。[802.11 Configuration] 画面が表示されます。

図 12 : 設定ウィザード : [802.11 Configuration] 画面



- ステップ 45 802.11a、802.11b、および 802.11g の Lightweight アクセス ポイント ネットワークを有効にするには、[802.11a Network Status]、[802.11b Network Status]、および [802.11g Network Status] の各チェックボックスを選択したままにします。これらのネットワークのサポートを無効にするには、このチェックボックスをオフにします。
- ステップ 46 コントローラの無線リソース管理 (RRM) 自動 RF 機能を有効にするには、[Auto RF] チェックボックスを選択したままにします。自動 RF 機能のサポートを無効にするには、このチェックボックスをオフにします。
- (注) 自動 RF 機能を有効にすると、コントローラが自動的に他のコントローラと RF グループを形成できるようになります。グループでは、チャンネルや送信電力の割り当てなど、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。

ステップ 47 [Next] をクリックします。[Set Time] 画面が表示されます。

図 13 : 設定ウィザード : [Set Time] 画面

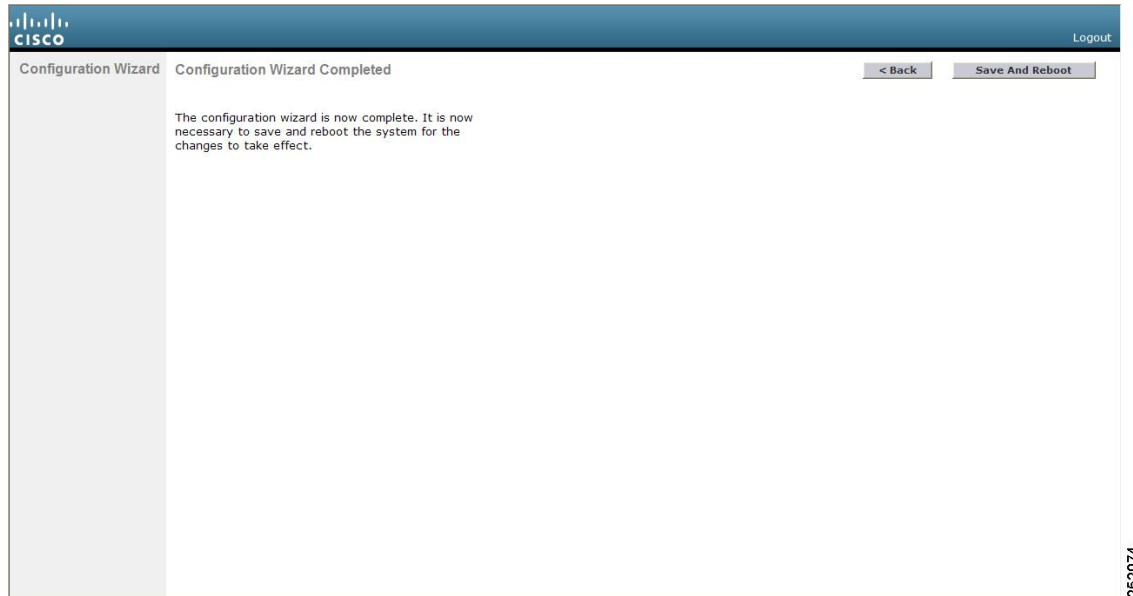
ステップ 48 コントローラのシステム時間を手動で設定するには、現在の日付を Month/DD/YYYY の形式で、現在の時刻を HH:MM:SS の形式で入力します。

ステップ 49 夏時間 (DST) が自動的に設定されないように時間帯を手動で設定するには、現地時間とグリニッジ標準時 (GMT) との差の時間の部分を [Delta Hours] テキストボックスに入力し、分の部分を [Delta Mins] テキストボックスに入力します。

(注) 時間帯を手動で設定するときは、GMT を基準とした現在の時間帯の時差を +/- を付けて入力します。たとえば、米国の太平洋標準時は、GMT の時刻より 8 時間遅れています。したがって、-8 と入力します。

ステップ 50 [Next] をクリックします。 [Configuration Wizard Completed] 画面が表示されます。

図 14 : 設定ウィザード : [Configuration Wizard Completed] 画面



ステップ 51 設定を保存してコントローラをリブートするには、[Save and Reboot] をクリックします。

ステップ 52 次のメッセージが表示されたら、[OK] をクリックします。

```
Configuration will be saved and the controller will be
rebooted. Click ok to confirm.?
```

コントローラの設定が保存されてリブートし、ログイン画面が表示されます。

コントローラの設定 : CLI 設定ウィザードの使用

はじめる前に

- 利用可能なオプションは、各設定パラメータの後の括弧内に示されます。デフォルト値は、すべて大文字で示されます。
- 入力した応答が正しくない場合は、「invalid response」などのエラーメッセージが表示され、ウィザードのプロンプトが再び表示されます。

- 前のコマンドラインに戻る必要があるときは、**ハイフン** キーを押してください。

- ステップ 1** AutoInstall プロセスを終了するかどうかをたずねるメッセージが表示されたら、「yes」と入力します。「yes」と入力しなかった場合は、30 秒後に AutoInstall プロセスが開始します。
(注) AutoInstall とは、設定ファイルを TFTP サーバからダウンロードしてから、設定を自動的にコントローラにロードする機能です。
- ステップ 2** システム名を入力します。これは、コントローラに割り当てる名前です。ASCII 文字を最大 31 文字入力できます。
- ステップ 3** このコントローラに割り当てる管理者のユーザ名およびパスワードを入力します。それぞれ、24 文字までの ASCII 文字を入力できます。
リリース 7.0.116.0 以降、次のパスワード ポリシーが実装されています。
- パスワードには、次の中から少なくとも 3 つのクラスの文字を含める必要があります。
 - 小文字の英字
 - 大文字の英字
 - 数字
 - 特殊文字
 - パスワードには同じ文字を連続して 4 回以上繰り返すことはできません。
 - 新規のパスワードとして、関連するユーザ名と同じものやユーザ名を逆にしたものは使用できません。
 - パスワードには、Cisco という語の大文字を小文字に変更したものや文字の順序を入れ替えたもの (cisco、ocsic など) を使用できません。さらに、i の代わりに 1、I または !、o の代わりに 0、または s の代わりに \$ を使用することはできません。
- ステップ 4** コントローラのサービス ポート インターフェイスの IP アドレスが DHCP サーバから取得されるように設定する場合は、**DHCP** と入力します。サービス ポートを使用しない場合、またはサービス ポートに固定 IP アドレスを割り当てる場合は、「none」と入力します。
(注) サービス ポート インターフェイスは、サービス ポートを介した通信を制御します。このインターフェイスの IP アドレスは、管理インターフェイスとは異なるサブネット上のものであることが必要です。このように設定されていれば、コントローラを直接、または専用の管理ネットワーク経由で管理できるので、ネットワークがダウンしているときもサービス アクセスが可能になります。
- ステップ 5** ステップ 4 で「none」と入力した場合は、サービス ポート インターフェイスの IP アドレスとネットマスクを次の 2 行で入力します。
- ステップ 6** リンク集約 (LAG) を有効にする場合は [yes] を選択し、無効にする場合は [NO] を選択します。
- ステップ 7** 管理インターフェイスの IP アドレスを入力します。
(注) 管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。

- ステップ 8** 管理インターフェイス ネットマスクの IP アドレスを入力します。
- ステップ 9** デフォルト ルータの IP アドレスを入力します。
- ステップ 10** 管理インターフェイスの VLAN 識別子 (有効な VLAN 識別子) を入力します。タグなし VLAN の場合は 0 を入力します。VLAN 識別子は、スイッチ インターフェイス設定と一致するように設定する必要があります。
- ステップ 11** クライアント、コントローラの管理インターフェイス、およびサービス ポート インターフェイス (使用する場合) が IP アドレスを取得するためのデフォルト DHCP サーバの IP アドレスを入力します。AP マネージャ インターフェイスの IP アドレスを入力します。
- (注) Cisco 5500 シリーズ コントローラの場合は、このプロンプトは表示されません。このシリーズは AP マネージャ インターフェイスの設定が必要ないからです。管理インターフェイスは、デフォルトで AP マネージャ インターフェイスとして動作します。
- ステップ 12** コントローラの仮想インターフェイスの IP アドレスを入力します。IP アドレスは、未割り当ての架空のアドレスを入力します。
- (注) 仮想インターフェイスは、モビリティ管理、DHCP リレー、およびゲスト Web 認証や VPN 終端などレイヤ 3 の組み込みセキュリティをサポートするために使用されます。同一のモビリティグループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。
- ステップ 13** 必要に応じて、コントローラを追加するモビリティグループ/RF グループの名前を入力します。
- (注) ここで入力する名前は、モビリティグループと RF グループの両方に割り当てられますが、これらのグループは同じではありません。どちらのグループもコントローラの集合を定義するものですが、目的が異なります。RF グループ内のすべてのコントローラは通常同じモビリティグループに属し、モビリティグループ内のすべてのコントローラは同じ RF グループに属します。ただし、モビリティグループはスケラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現するのに対して、RF グループはスケラブルでシステム全体にわたる動的な RF 管理を実現します。
- ステップ 14** ネットワーク名またはサービスセット ID (SSID) を入力します。SSID が設定されると、コントローラの基本機能が使用可能になり、そのコントローラに join されたアクセスポイントの無線を有効化できるようになります。
- ステップ 15** クライアントに独自の IP アドレス割り当てを許可する場合は YES と入力し、クライアントの IP アドレスが DHCP サーバから取得されるようにするには no と入力します。
- ステップ 16** RADIUS サーバをここで設定するには、YES と入力してから、RADIUS サーバの IP アドレス、通信ポート、および秘密キーを入力します。それ以外の場合は、no と入力します。no と入力すると、次のメッセージが表示されます。「Warning! The default WLAN security policy requires a RADIUS server. Please see the documentation for more details.」
- ステップ 17** コントローラが使用される国のコードを入力します。
- (注) 使用可能な Country Code の一覧を表示するには、help と入力します。
- (注) 複数の国のアクセスポイントを 1 つのコントローラで管理する場合は、複数の Country Code を入力できます。複数の Country Code を入力するには、Country Code をカンマで区切ります (「US,CA,MX」など)。設定ウィザードの実行後、コントローラに join している各アクセスポイントに特定の国を割り当てる必要があります。

- ステップ 18** 802.11b、802.11a、および 802.11g の Lightweight アクセス ポイント ネットワークを有効にするには **YES** と入力し、無効にするには **no** と入力します。
- ステップ 19** コントローラの無線リソース管理 (RRM) 自動 RF 機能を有効にするには **YES** と入力し、無効にするには **no** と入力します。
- (注) 自動 RF 機能を有効にすると、コントローラが自動的に他のコントローラと RF グループを形成できるようになります。グループでは、チャンネルや送信電力の割り当てなど、グループの RRM パラメータ設定を最適化するリーダーが動的に選出されます。
- ステップ 20** 電源投入時にコントローラの時間設定が外部ネットワーク タイム プロトコル (NTP) サーバから受信されるようにするには、「**YES**」と入力して NTP サーバを設定します。それ以外の場合は、**no** と入力します。
- (注) Cisco サービス統合型ルータにインストールされるコントローラ ネットワーク モジュールにはバッテリーがないため、時間設定を保存することはできません。したがって、電源投入時に外部 NTP サーバから時間設定を受信する必要があります。
- ステップ 21** ステップ 20 で **no** と入力した場合に、コントローラのシステム時間をここで手動設定するには、**YES** と入力します。システム時間を後で設定する場合は、**no** と入力します。
- ステップ 22** ステップ 21 で **YES** と入力した場合は、現在の日付を MM/DD/YY の形式で、現在の時刻を HH:MM:SS の形式で入力します。
- ステップ 22 を完了すると、ウィザードに、IPv6 パラメータを設定するかどうかを確認するプロンプトが表示されます。 **yes** と入力して続行します。
- ステップ 23** サービスポートインターフェイスの IPv6 アドレスの設定を入力します。 **static** または **SLAAC** のいずれかを入力できます。
- **SLAAC** と入力すると、IPv6 アドレスが自動設定されます。
 - **static** と入力する場合は、サービスインターフェイスの IPv6 アドレスとそのプレフィックス長を入力する必要があります。
- ステップ 24** 管理インターフェイスの IPv6 アドレスを入力します。
- ステップ 25** 管理インターフェイスの IPv6 アドレスのプレフィックス長を入力します。
- ステップ 26** 管理インターフェイスのゲートウェイ IPv6 アドレスを入力します。
- 管理インターフェイス設定が完了すると、ウィザードに、RADIUS サーバの IPv6 パラメータを設定するように指示するプロンプトが表示されます。 **yes** と入力します。
- ステップ 27** RADIUS サーバの IPv6 アドレスを入力します。
- ステップ 28** RADIUS サーバの通信ポート番号を入力します。デフォルト値は 1812 です。
- ステップ 29** RADIUS サーバの IPv6 アドレス用の秘密キーを入力します。
- RADIUS サーバ設定が完了すると、ウィザードに、IPv6 NTP サーバを設定するように指示するプロンプトが表示されます。 **yes** と入力します。
- ステップ 30** NTP サーバの IPv6 アドレスを入力します。
- ステップ 31** 設定が正しいかどうかをたずねるプロンプトが表示されたら、**yes** または **NO** と入力します。
- yes** と入力すると、コントローラは設定を保存してリポートし、ログオンプロンプトが表示されます。

コントローラ Web GUI の使用方法

Web ブラウザ、つまり、グラフィカルユーザインターフェイス (GUI) は、各コントローラに組み込まれています。

最大 5 名のユーザが、コントローラ http または https (http+SSL) 管理ページを同時に閲覧して、パラメータを設定し、コントローラとそのアソシエートされているアクセス ポイントの動作ステータスを監視することができます。



(注) Cisco UWN ソリューションのセキュリティを強化するために、HTTPS インターフェイスを有効にし、HTTP インターフェイスを無効にすることをお勧めします。

注意事項および制約事項

コントローラ GUI を使用する場合、次のガイドラインに従います。

- GUI を使用する PC では、Windows 7、Windows XP SP1 以降のリリース、または Windows 2000 SP4 以降のリリースが稼働している必要があります。
- コントローラ GUI は、Microsoft Internet Explorer バージョン 6.0 SP1 以降、または Mozilla Firefox 2.0.0.11 以降に対応しています。



(注) Opera および Netscape はサポートされていません。

- サービス ポート インターフェイスまたは管理インターフェイスを使用して GUI にアクセスできますが、サービス ポート インターフェイスの使用をお勧めします。
- サービス ポート インターフェイスを使用する場合は、HTTP と HTTPS の両方を使用できます。HTTPS はデフォルトで有効になっており、HTTP も有効にすることができます。サービス ポート インターフェイスに関連付けるデフォルト IP アドレスは 192.168.1.1 です。
- GUI のページ上部にある [Help] をクリックすると、オンラインヘルプが表示されます。オンラインヘルプを表示するには、ブラウザのポップアップブロックを無効にする必要があります。

Web GUI へのログイン

-
- ステップ 1** ブラウザのアドレスバーに IP アドレス コントローラを入力します。接続をセキュリティで保護するには、**https://ip-address** と入力します。接続をセキュリティで保護しない場合は、**http://ip-address** と入力します。
- ステップ 2** ユーザ名とパスワードを入力する画面が表示されたら、有効な値を入力して [OK] をクリックします。[Summary] ページが表示されます。
- (注) 設定ウィザードで作成されたユーザ名およびパスワードでは、大文字と小文字が区別されます。デフォルトのユーザ名は **admin**、デフォルトのパスワードは **admin** です。
-

GUI からのログアウト

-
- ステップ 1** ページの右上の [Logout] をクリックします。
- ステップ 2** [Close] をクリックするとログアウトプロセスが完了し、それ以降は、権限のないユーザはコントローラ コントローラ GUI にはアクセスできなくなります。
- ステップ 3** 決定を確認する画面が表示されたら、[Yes] をクリックします。
-

Web モードおよびセキュア Web モードの有効化

この項では、ディストリビューション システム ポートを Web ポート (HTTP を使用) またはセキュア Web ポート (HTTPS を使用) として有効にする手順について説明します。HTTPS を有効化すると、GUI 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。HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。また、外部で生成された証明書をダウンロードすることもできます。

Web モードおよびセキュア Web モードの設定は、コントローラ GUI と CLI のどちらでも実行できます。

Web モードおよびセキュア Web モードの有効化 (GUI)

-
- ステップ 1** [Management] > [HTTP-HTTPS] を選択します。

[HTTP-HTTPS Configuration] ページが表示されます。

- ステップ 2** Web モード（ユーザが「`http://ip-address`」を使用してコントローラ GUI にアクセスできます）を有効にするには、[HTTP Access] ドロップダウンリストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。デフォルト値は [Disabled] です。Web モードの接続は、セキュリティで保護されません。
- ステップ 3** セキュア Web モード（ユーザが「`https://ip-address`」を使用してコントローラ GUI にアクセスできます）を有効にするには、[HTTPS Access] ドロップダウンリストから [Enabled] を選択します。有効にしない場合は、[Disabled] を選択します。デフォルト値は [Enabled] です。セキュア Web モードの接続は、セキュリティで保護されています。
- ステップ 4** [Web Session Timeout] テキストボックスに、Web セッションが非アクティブのためにタイムアウトするまでの時間を分単位で入力します。10 ～ 160 分（両端の値を含む）の値を入力できます。デフォルト値は 30 分です。
- ステップ 5** [Apply] をクリックします。
- ステップ 6** ステップ 3 でセキュア Web モードを有効にした場合は、ローカル Web アドミニストレーション SSL 証明書が生成されて自動的に GUI に適用されます。現在の証明書の詳細は、[HTTP-HTTPS Configuration] ページの中央に表示されます。
- （注） 必要に応じて、現在の証明書を削除することもできます。削除するには、[Delete Certificate] をクリックします。[Regenerate Certificate] をクリックすると、新しい証明書が生成されます。
- ステップ 7** [Save Configuration] をクリックします。

Web モードおよびセキュア Web モードの有効化（CLI）

- ステップ 1** 次のコマンドを入力して、Web モードを有効または無効にします。
- ```
config network webmode {enable | disable}
```
- このコマンドを実行すると、ユーザが「`http://ip-address`」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値では無効になっています。Web モードの接続は、セキュリティで保護されません。
- ステップ 2** 次のコマンドを入力して、セキュア Web モードを有効または無効にします。
- ```
config network secureweb {enable | disable}
```
- このコマンドを実行すると、ユーザが「`https://ip-address`」を使用してコントローラの GUI にアクセスできるようになります。デフォルト値は有効（enable）です。セキュア Web モードの接続は、セキュリティで保護されています。
- ステップ 3** 次のコマンドを入力して、セキュア Web モードのセキュリティの強化を有効または無効にします。
- ```
config network secureweb cipher-option high {enable | disable}
```
- このコマンドを実行すると、ユーザが「`https://ip-address`」を使用してコントローラの GUI にアクセスできるようになりますが、ブラウザが 128 ビット（またはそれ以上）の暗号をサポートしている必要があります。デフォルト値はディセーブルです。



**ステップ 4** 次のコマンドを入力して、Web 管理に対して SSLv2 を有効または無効にします。

```
config network secureweb cipher-option sslv2 {enable | disable}
```

SSLv2 を無効にすると、SSLv2 だけを使用するように設定されたブラウザからは接続できなくなります。SSLv3 以降などセキュリティの強化されたプロトコルを使用するように設定されたブラウザを使用する必要があります。デフォルト値はディセーブルです。

**ステップ 5** 次のコマンドを入力して、Web 認証および Web 管理 に対して RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) 暗号スイート (CBC 暗号スイートに優先) の環境設定を有効または無効にします。

```
config network secureweb cipher-option rc4-preference {enable | disable}
```

**ステップ 6** 次のコマンドを入力して、コントローラが証明書を生成したことを確認します。

```
show certificate summary
```

以下に類似した情報が表示されます。

```
Web Administration Certificate..... Locally Generated
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
```

**ステップ 7** (任意) このコマンドを入力して新しい証明書を生成します。

```
config certificate generate webadmin
```

数秒後、証明書が生成されたことをコントローラが確認します。

**ステップ 8** 次のコマンドを入力して、リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを不揮発性 RAM (NVRAM) に保存します。

```
save config
```

**ステップ 9** 次のコマンドを入力して、コントローラをリブートします。

```
reset system
```

## 外部で生成した SSL 証明書のロード

ここでは、外部で生成した SSL 証明書をロードする方法について説明します。

## 外部で生成した SSL 証明書について

TFTP サーバを使用して、外部で生成された SSL 証明書をコントローラにダウンロードできます。TFTP を使用する際の注意事項は次のとおりです。

- サービス ポート経由で証明書をロードする場合、サービス ポートはルーティングできないため、TFTP サーバはコントローラと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。また、証明書をディストリビューションシステム ネットワーク ポート経由でロードする場合は、TFTP サーバはどのサブネットに存在していてもかまいません。

- サードパーティの TFTP サーバを Cisco Prime Infrastructure と同じ PC 上で実行することはできません。Prime Infrastructure 内蔵 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。



(注) チェーン証明書は Web 認証でのみサポートされています。管理証明書ではサポートされていません。

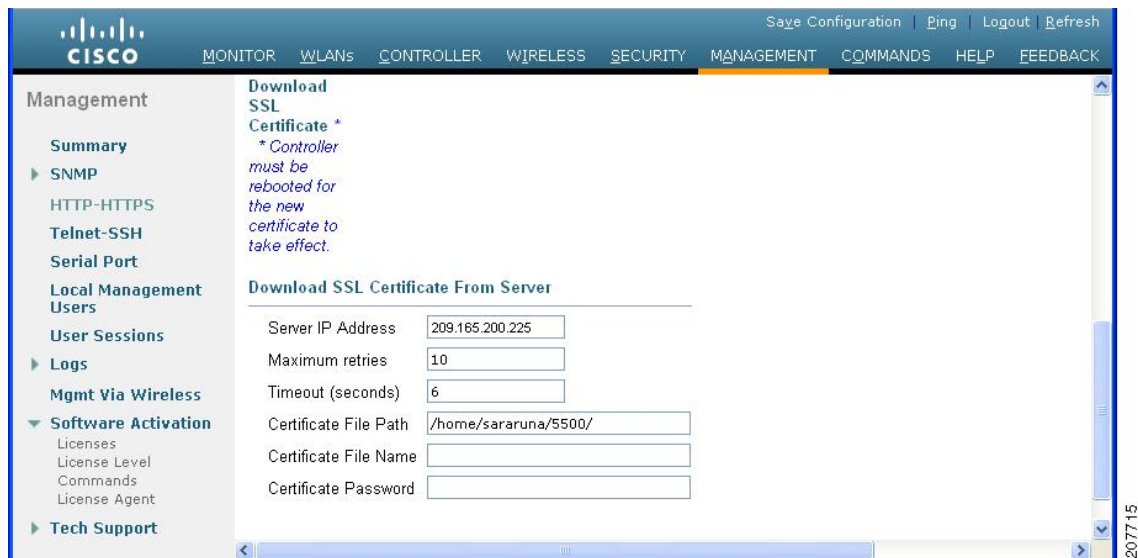


(注) 各 HTTPS 証明書には RSA キーが組み込まれています。キーの長さは、比較的安全性の低い 512 ビットから、非常に安全性の高い数千ビットまでさまざまです。認証局から新しい証明書を取得する際、証明書に組み込まれた RSA キーの長さが 768 ビット以上であることを確認してください。

## SSL 証明書のロード (GUI)

ステップ 1 [HTTP Configuration] ページの [Download SSL Certificate] チェックボックスを選択します。

図 15 : [HTTP Configuration] ページ



- ステップ 2 [Server IP Address] テキスト ボックスに、TFTP サーバの IP アドレスを入力します。
- ステップ 3 [Maximum Retries] テキスト ボックスに、TFTP サーバによる証明書のダウンロードの最大試行回数を入力します。
- ステップ 4 [Timeout] テキスト ボックスに、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を入力します。
- ステップ 5 [Certificate File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。
- ステップ 6 [Certificate File Name] テキスト ボックスに、証明書の名前を入力します（webadmindcert\_name.pem）。
- ステップ 7 （任意） [Certificate Password] テキスト ボックスに、証明書を暗号化するためのパスワードを入力します。
- ステップ 8 [Apply] をクリックします。
- ステップ 9 [Save Configuration] をクリックします。
- ステップ 10 [Commands] > [Reboot] > [Reboot] > [Save and Reboot] を選択し、コントローラをリブートして変更内容を反映します。

## SSL 証明書のロード (CLI)

- ステップ 1 パスワードを使用して、.PEM エンコード ファイル形式の HTTPS 証明書を暗号化します。PEM エンコード ファイルは、Web アドミニストレーション証明書ファイル（webadmindcert\_name.pem）と呼ばれます。

- ステップ 2 webadmindcert\_name.pem ファイルを TFTP サーバ上のデフォルト ディレクトリに移動します。

- ステップ 3 現在のダウンロードの設定を表示するには、次のコマンドを入力してプロンプトに **n** と応答します。

```
transfer download start
```

以下に類似した情報が表示されます。

```
Mode..... TFTP
Data Type..... Admin Cert
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... <directory path>
TFTP Filename.....
Are you sure you want to start? (y/n) n
Transfer Canceled
```

- ステップ 4 次のコマンドを使用して、ダウンロード設定を変更します。

```
transfer download mode tftp
```

```
transfer download datatype webauthcert
```

```
transfer download serverip TFTP_server_IP_address
```

```
transfer download path absolute_TFTP_server_path_to_the_update_file
```

```
transfer download filename webadmindcert_name.pem
```

**ステップ 5** オペレーティング システムが Web アドミネストレーション SSL キーおよび証明書の暗号化を解除できるように、.PEM ファイルのパスワードを設定するには、次のコマンドを入力します。  
**transfer download certpassword private\_key\_password**

**ステップ 6** 現在のダウンロードの設定を確認して証明書とキーのダウンロードを開始するには、次のコマンドを入力して、プロンプトに **y** と応答します。  
**transfer download start**

以下に類似した情報が表示されます。

```
Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... xxx.xxx.xxx.xxx
TFTP Path..... directory path
TFTP Filename..... webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

**ステップ 7** リブート後も変更内容が維持されるように、SSL 証明書、キー、セキュア Web パスワードを NVRAM に保存するには、次のコマンドを入力します。  
**save config**

**ステップ 8** コントローラをリブートするには、次のコマンドを入力します。  
**reset system**

## コントローラ CLI の使用方法

Cisco UWN ソリューションのコマンドライン インターフェイス (CLI) は、各コントローラに組み込まれています。CLI では、VT-100 ターミナルエミュレーションプログラムを使用して、個々のコントローラおよび各コントローラにアソシエートされた Lightweight アクセスポイントをローカルまたはリモートで設定、監視、制御することができます。この CLI は、単純なテキストベースのツリー構造のインターフェイスです。最大 5 名のユーザが Telnet 対応ターミナルエミュレーションプログラムを使用してコントローラにアクセスできます。



(注) 特定のコマンドの情報は、『Cisco Wireless LAN Controller Command Reference』を参照してください。



(注) XML 設定の文字列を CLI コマンドに入力する場合は、文字列を引用符で囲む必要があります。

## コントローラ CLI へのログイン

次の2つの方法のうちいずれかを使用して、コントローラ CLI にアクセスできます。

- コントローラ コンソール ポートへのシリアル直接接続
- 事前設定されたサービス ポートやディストリビューション システム ポートを使用したイーサネット上のリモート コンソールセッション

CLI にログインする前に、使用する接続の種類に基づいて接続および環境変数を設定しておく必要があります。

### 注意事項および制約事項

Cisco 5500 シリーズ コントローラでは、RJ-45 コンソール ポートと USB コンソール ポートのどちらでも使用できます。USB コンソール ポートを使用する場合は、5 ピン ミニ タイプ B コネクタをコントローラの USB コンソール ポートに接続し、もう一端を PC の USB タイプ A ポートに接続します。Windows PC を USB ポートに接続するのが初めての場合は、USB コンソール ドライバをインストールするための画面が表示されます。インストール画面の指示に従って、ドライバをインストールしてください。USB コンソール ドライバは PC 上の COM ポートにマッピングされるので、この COM ポートにターミナルエミュレータ アプリケーションをマッピングする必要があります。

Telnet セッションを有効にする方法については、「[Telnet および Secure Shell セッションの設定](#)」の項を参照してください。

### ローカル シリアル接続の使用方法

#### はじめる前に

シリアル ポートに接続するには次が必要です。

- VT-100 ターミナルエミュレーションプログラム (HyperTerminal、ProComm、Minicom、Tip など) を実行している PC
- ヌルモデム シリアル ケーブル

シリアル ポートを介してコントローラ CLI にログインする手順は、次のとおりです。

- 
- ステップ 1** ヌルモデム シリアル ケーブルの一端をコントローラのコンソール ポートに接続し、もう一端を PC のシリアル ポートに接続します。
  - ステップ 2** PC の VT-100 ターミナルエミュレーションプログラムを起動します。ターミナルエミュレーションプログラムのパラメータを次のとおりに設定します。
    - 9600 ボー

- 8 データ ビット
- 1 ストップ ビット
- パリティなし
- ハードウェア フロー制御なし

(注) コントローラでの最小シリアル タイムアウトは、1 分間ではなく、15 秒間です。

(注) コントローラのシリアル ポートは、9600 ボー レートおよび短いタイムアウト用に設定されています。これらの値を変更するには、`config serial baudrate baudrate` コマンドおよび `config serial timeout timeout` コマンドを使用します。 `config serial timeout 0` と入力すると、シリアルセッションはタイムアウトしなくなります。

**ステップ 3** プロンプトが表示されたら、有効なユーザ名とパスワードを入力してコントローラにログインします。設定ウィザードで作成されたユーザ名およびパスワードでは、大文字と小文字が区別されます。

(注) デフォルトのユーザ名は `admin`、デフォルトのパスワードは `admin` です。

CLI のルート レベル システム プロンプトが表示されます。

`#(system prompt)>`

(注) システム プロンプトは、最大 31 文字の任意の英数字から成る文字列です。システム プロンプトを変更するには、`config prompt` コマンドを入力します。

## リモート イーサネット接続の使用方法

### はじめる前に

リモートでコントローラに接続するには、次が必要です。

- イーサネット ネットワークを介してコントローラにアクセスできる PC
- コントローラの IP アドレス
- Telnet セッション用の VT-100 ターミナル エミュレーション プログラムまたは DOS シェル



(注) デフォルトでは、コントローラは Telnet セッションをブロックします。Telnet セッションを有効にするには、シリアルポートへのローカル接続を使用する必要があります。

**ステップ 1** VT-100 ターミナル エミュレーション プログラムまたは DOS シェル インターフェイスのパラメータが次のとおりに設定されていることを確認します。

- イーサネット アドレス
- ポート 23

**ステップ 2** コントローラの IP アドレスを使用して CLI に Telnet 接続します。

**ステップ 3** プロンプトが表示されたら、有効なユーザ名とパスワードを入力してコントローラにログインします。設定ウィザードで作成されたユーザ名およびパスワードでは、大文字と小文字が区別されます。

(注) デフォルトのユーザ名は **admin**、デフォルトのパスワードは **admin** です。

CLI のルート レベル システム プロンプトが表示されます。

(注) システム プロンプトは、最大 31 文字の任意の英数字から成る文字列です。システム プロンプトを変更するには、**config prompt** コマンドを入力します。

## CLI からのログアウト

CLI での作業が終了したら、ルート レベルに移動して **logout** と入力します。揮発性 Random-Access Memory (RAM; ランダムアクセスメモリ) への変更を保存するかどうかを確認するプロンプトが表示されます。



(注) アクティビティがない状態が 5 分間続くと、変更を保存せずに自動的に CLI からログアウトされます。**config serial timeout** コマンドを使用すると、自動ログアウト時間を 0 (自動ログアウトしない) ~ 160 分の範囲内で設定できます。

## CLI のナビゲーション

CLI のナビゲーションは、5 つのレベルに分かれています。

- ルート レベル
- レベル 2
- レベル 3
- レベル 4
- レベル 5

CLI にログインしたときは、ルート レベルです。ルート レベルでは、任意のフル コマンドを、正しいコマンド レベルに移動することなく入力できます。

次の表は、CLI のナビゲーションおよび一般的なタスク実行のためのコマンドの一覧です。

表 2: CLI のナビゲーションと共通タスクのコマンド

| コマンド         | アクション                                                                  |
|--------------|------------------------------------------------------------------------|
| help         | ルート レベルでは、システム全体のナビゲーション コマンドが表示されます。                                  |
| ?            | 現在のレベルで使用できるコマンドが表示されます。                                               |
| command ?    | 指定したコマンドのパラメータが表示されます。                                                 |
| exit         | 1 つ下のレベルに移動します。                                                        |
| Ctrl-Z       | ルート レベルに戻ります。                                                          |
| save config  | ルート レベルでは、設定変更を使用中のアクティブな RAM からリブート後も維持されるように不揮発性 RAM (NVRAM) に保存します。 |
| reset system | ルートレベルの場合、ログアウトせずにコントローラをリセットします。                                      |

## 設定のないコントローラでの AutoInstall 機能の使用

ここでは、設定なしでコントローラの AutoInstall 機能を使用する方法について説明します。

### AutoInstall 機能について

設定のないコントローラを起動するときに、AutoInstall 機能によって設定ファイルを TFTP サーバからダウンロードして設定をコントローラに自動的にロードすることができます。

ネットワーク上に（または Prime Infrastructure フィルタを介して）すでに存在するコントローラに設定ファイルを作成する場合は、TFTP サーバに設定ファイルを配置し、DHCP サーバを設定します。これによって新しいコントローラは IP アドレスと TFTP サーバの情報を取得でき、AutoInstall 機能が新しいコントローラの設定ファイルを自動的に取得できます。

コントローラを起動すると、AutoInstall プロセスが開始されます。設定ウィザードが起動したことが AutoInstall へ通知されないかぎり、コントローラは何も処理しません。設定ウィザードが起動しなければ、そのコントローラには有効な設定があります。



AutoInstall は、設定ウィザードが起動したことを通知されると（つまり、コントローラに設定がないときは）、さらに 30 秒間待機します。この間、ユーザは設定ウィザードからの最初のプロンプトに応答できます。

Would you like to terminate autoinstall? [yes]:

30 秒の中断タイムアウトが経過すると、AutoInstall は DHCP クライアントを起動します。30 秒のタイムアウトが経過した後でも、プロンプトで **Yes** と入力すれば、AutoInstall のタスクを停止できます。ただし、TFTP タスクによってフラッシュがロックされており、有効な設定ファイルのダウンロードとインストールが進行中のときは、AutoInstall を停止することはできません。

## 注意事項および制約事項

AutoInstall では次のインターフェイスが使用されます。

- Cisco 5500 シリーズ コントローラ
  - eth0 : サービス ポート (タグなし)
  - dtl0 : NPU を介したギガビット ポート 1 (タグなし)

## DHCP による IP アドレスの入手、および TFTP サーバからの設定ファイルのダウンロード

AutoInstall は DHCP プロセスが正常に終了するまで、またはユーザが AutoInstall プロセスを停止するまで DHCP サーバから IP アドレスを取得しようとします。DHCP サーバから IP アドレスを正常に取得するための最初のインターフェイスは、AutoInstall タスクに登録されます。このインターフェイスの登録によって、AutoInstall は TFTP サーバ情報の取得と、設定ファイルのダウンロードのプロセスを開始します。

インターフェイスの DHCP IP アドレスを取得した後、AutoInstall はコントローラのホスト名と TFTP サーバの IP アドレスを決定する短い一連のイベントを開始します。この一連のイベントの各段階では、デフォルト情報または暗黙的信息よりも明示的に設定された情報が優先され、明示的 IP アドレスよりも明示的ホスト名が優先されます。

そのプロセスは次のとおりです。

- DHCP を介して 1 つ以上のドメイン ネーム システム (DNS) サーバ IP アドレスが得られると、AutoInstall は `/etc/resolv.conf` ファイルを作成します。このファイルにはドメイン名、および受信された DNS サーバのリストが含まれます。Domain Name Server オプションでは、DNS サーバのリストが提供され、Domain Name オプションではドメイン名が提供されます。
- ドメイン サーバがコントローラと同じサブネット上にない場合、スタティック ルート エントリがドメインサーバごとにインストールされます。これらの静的ルートは、DHCP Router オプションを介して取得されたゲートウェイをポイントします。
- コントローラのホスト名は、次の順序で決定されます。

- DHCP Host Name オプションが受信された場合、この情報（最初のピリオド[.]で切り捨てられる）がコントローラのホスト名として使用されます。
  - DNS の逆ルックアップがコントローラの IP アドレスで実行されます。DNS がホスト名を返すと、（最初のピリオド[.]で切り捨てられた）この名前はコントローラのホスト名として使用されます。
- TFTP サーバの IP アドレスは、次の順序で決定されます。
    - AutoInstall が DHCP TFTP Server Name オプションを受信した場合、AutoInstall はこのサーバ名の DNS lookup を実行します。DNS lookup が正常に終了した場合、返された IP アドレスが TFTP サーバの IP アドレスとして使用されます。
    - [DHCP Server Host Name (sname)] テキストボックスが有効な場合は、AutoInstall はこの名前に対する DNS lookup を実行します。DNS lookup が正常に終了した場合、返された IP アドレスが TFTP サーバの IP アドレスとして使用されます。
    - AutoInstall が DHCP TFTP Server Address オプションを受信した場合、このアドレスが TFTP サーバの IP アドレスとして使用されます。
    - AutoInstall はデフォルトの TFTP サーバ名 (cisco-wlc-tftp) の DNS lookup を実行します。DNS lookup が正常に終了した場合、受信した IP アドレスが TFTP サーバの IP アドレスとして使用されます。
    - DHCP サーバの IP アドレス (siaddr) テキストボックスがゼロ以外の値である場合、このアドレスは TFTP サーバの IP アドレスとして使用されます。
    - 制限されたブロードキャストアドレス (255.255.255.255) が TFTP サーバの IP アドレスとして使用されます。
  - TFTP サーバがコントローラと同じサブセットにない場合、スタティック ルート (/32) が TFTP サーバの IP アドレスとしてインストールされます。このスタティックルートは、HDCP Router オプションを介して取得されたゲートウェイをポイントします。

## 設定ファイルの選択

ホスト名と TFTP サーバが決定されると、AutoInstall は設定ファイルのダウンロードを試行します。AutoInstall は DHCP IP アドレスを取得するインターフェイスごとに 3 回の完全なダウンロードを繰り返します。インターフェイスは、3 回の試行後に設定ファイルを正常にダウンロードできない場合、それ以上のダウンロードを試行しません。

正常にダウンロードおよびインストールされた最初の設定ファイルがコントローラのリポートをトリガーします。リポート後に、コントローラは新しくダウンロードされた設定を実行します。

AutoInstall は、名前がリストアップされる順番で設定ファイルを検索します。

- [DHCP Boot File Name] オプションによって提供されるファイル名
- [DHCP File] テキストボックスで提供されるファイル名
- *host name-config*

- *host name.cfg*
- *Base MAC Address-config* (0011.2233.4455-config など)
- *serial number-config*
- *ciscowlc-config*
- *ciscowlc.cfg*

AutoInstall は、設定ファイルが見つかるまで、このリストの順にファイルを探します。登録されているインターフェイスごとにこのリストを3回サイクルし、設定ファイルが見つからない場合、実行を停止します。



(注) ダウンロードされる設定ファイルは、完全な設定を行えることもあれば、Cisco Prime Infrastructure で管理されるコントローラに十分な程度の情報を持つ最小限の設定のこともあります。完全な設定ファイルは、Prime Infrastructure から直接展開できます。



(注) 自動インストールでは、コントローラに接続されているスイッチがチャネルのいずれかに設定されることを想定していません。Autoinstall は、LAG 設定のサービスポートで実行します。



(注) Cisco Prime Infrastructure は、コントローラに AutoInstall 機能を提供します。Cisco Prime Infrastructure 管理者はコントローラのホスト名、MAC アドレス、シリアル番号を含むフィルタを作成し、このフィルタのルールにテンプレートのグループ（設定グループ）を関連付けることができます。Prime Infrastructure は、コントローラの最初の起動時に初期設定を押します。コントローラが検出された後、Prime Infrastructure は設定グループで定義されているテンプレートをコピーします。AutoInstall 機能と Cisco Prime Infrastructure の詳細については、Cisco Prime Infrastructure のマニュアルを参照してください。

## AutoInstall の操作例

次は AutoInstall の全プロセスの一例です。

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-config'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: iteration 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ==> 'wlc-1'
```

```

AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-config'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-config'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-config'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)
Resetting system

```

## コントローラのシステムの日時の管理

ここでは、コントローラのシステムの日時を管理する方法について説明します。

### コントローラのシステムの日時について

設定ウィザードを使用してコントローラを設定する際に、コントローラのシステムの日時を設定できます。設定ウィザードの実行時にシステムの日時を設定しなかった場合や、設定を変更した場合は、この項で説明する手順に従って、日時をネットワークタイムプロトコル (NTP) サーバから取得するようにコントローラを設定するか、手動で日時を設定します。コントローラ上の時間帯は、Greenwich Mean Time (GMT; グリニッジ標準時) を基準として設定します。

また、各種 NTP サーバ間での認証方法を設定できます。

### 注意事項および制約事項

- wIPS を設定する場合、コントローラの時間帯を UTC に設定する必要があります。
- 日時が正しく設定されていない場合は、Cisco Aironet Lightweight アクセスポイントがコントローラに接続できなくなる可能性があります。アクセスポイントからコントローラへの接続を許可する前に、コントローラの日時を設定してください。
- コントローラと NTP サーバの間の認証チャンネルを設定できるようになりました。

### 日時を取得するための NTP サーバの設定

各 NTP サーバの IP アドレスは、コントローラ データベースに追加されています。すべてのコントローラは NTP サーバを検索して、リブート時およびユーザ定義ポーリング間隔ごとに (毎日から毎週)、現在時刻を取得できます。

NTP サーバから日時を取得するように設定するには、次のコマンドを使用します。

- コントローラの NTP サーバを指定するには、次のコマンドを入力します。

```
config time ntp server index ip_address
```

- ポーリングの間隔（秒）を指定するには、次のコマンドを入力します。

```
config time ntp interval
```

## NTP 認証の設定 (GUI)

- 
- ステップ 1 [Controller] > [NTP] > [Servers] の順に選択して、[NTP Servers] ページを開きます。
- ステップ 2 [New] をクリックして NTP サーバを追加します。
- ステップ 3 [Server Index (Priority)] ドロップダウン リストからサーバの優先度を選択します。
- ステップ 4 [Server IP Address] テキスト ボックスに NTP サーバの IP アドレスを入力します。
- ステップ 5 [NTP Server Authentication] チェックボックスを選択して、NTP サーバの認証を有効にします。
- ステップ 6 [Apply] をクリックします。
- ステップ 7 [Controller] > [NTP] > [Keys] を選択します。
- ステップ 8 [New] をクリックして新しいキーを作成します。
- ステップ 9 [Key Index] テキスト ボックスにキー インデックスを入力します。
- ステップ 10 [Key Format] ドロップダウン リストからキーの形式を選択します。
- ステップ 11 [Key] テキスト ボックスにそのキーを入力します。
- ステップ 12 [Apply] をクリックします。
- 

## NTP 認証の設定 (CLI)



(注) デフォルトでは MD5 が使用されます。

- **config time ntp auth enable server-index key-index**
  - **config time ntp auth disable server-index**
  - **config time ntp key-auth add key-index md5 key-format key**
  - 次のコマンドを入力して、認証キーを削除します。  
**config time ntp key-auth delete key-index**
  - 次のコマンドを入力して、NTP キー インデックスの一覧を表示します。  
**show ntp-keys**
-

## 日時の設定 (GUI)

ステップ 1 [Commands] > [Set Time] の順に選択して [Set Time] ページを開きます。

図 16 : [Set Time] ページ

The screenshot shows the Cisco Wireless Controller GUI for the 'Set Time' configuration page. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'COMMANDS' menu is active. On the left, there is a sidebar with options like 'Download File', 'Upload File', 'Reboot', 'Reset to Factory Default', and 'Set Time'. The main content area is titled 'Set Time' and contains the following fields:

- Current Time:** Mon Nov 26 09:25:08 2007
- Date:**
  - Month: November (dropdown)
  - Day: 26 (dropdown)
  - Year: 2007 (text input)
- Time:**
  - Hour: 9 (dropdown)
  - Minutes: 25 (text input)
  - Seconds: 8 (text input)
- Timezone:**
  - Delta: hours 0 mins 0
  - Location: (GMT -5:00) Eastern Time (US and Canada) (dropdown)

Buttons for 'Set Date and Time' and 'Set Timezone' are located at the top right of the configuration area.

現在の日時がページ上部に表示されます。

ステップ 2 [Timezone] エリアの [Location] ドロップダウン リストから現地の時間帯を選択します。

(注) Daylight Saving Time (DST; 夏時間) を使用する時間帯を選択すると、DST の発生時の時間変更を反映してコントローラが自動的にそのシステム クロックを設定します。米国では、DST は3月の第2日曜日から始まり、11月の第1日曜日で終わります。

(注) 時間帯デルタをコントローラ GUI で設定することはできません。ただし、コントローラ CLI で設定した場合は、その変更がコントローラ GUI の [Delta Hours] テキスト ボックスと [Mins] テキスト ボックスに反映されます。

ステップ 3 [Set Timezone] をクリックして、変更を適用します。

ステップ 4 [Date] エリアの [Month] と [Day] のドロップダウン リストから現在の現地の月と日を選択し、[Year] テキスト ボックスに年を入力します。

ステップ 5 [Time] エリアの [Hour] ドロップダウン リストから現在の現地時間を選択し、[Minutes] テキスト ボックスと [Seconds] テキスト ボックスに分と秒を入力します。

(注) 日時を設定した後に、時間帯のロケーションを変更すると、[Time] エリアの値が更新され、この新しい時間帯のロケーションが反映されます。たとえば、コントローラが東部標準時の正午に設定されていて、時間帯を太平洋標準時に変更すると、時間は自動的に午前9時に変更されます。

ステップ 6 [Set Date and Time] をクリックして、変更を適用します。

ステップ 7 [Save Configuration] をクリックして、変更を保存します。

## 日時の設定 (CLI)

ステップ 1 次のコマンドを入力して、コントローラで現在の現地日時を GMT で設定します。

**config time manual mm/dd/yy hh:mm:ss**

(注) 時刻を設定するときは、現在の現地時間を GMT で表した時間を 00:00 ~ 24:00 の範囲内の値として入力します。たとえば、午前 8 時とします。米国の太平洋標準時は GMT より 8 時間遅れているため、16:00 と入力します。

ステップ 2 コントローラに時間帯を設定するには、次のいずれかを実行します。

- 次のコマンドを入力して、夏時間 (DST) が発生時に自動的に設定されるように時間帯ロケーションを設定します。

**config time timezone location location\_index**

*location\_index* は次の時間帯ロケーションの 1 つを表す数字です。

- 1 (GMT-12:00) 日付変更線、西側
- 2 (GMT-11:00) サモア
- 3 (GMT-10:00) ハワイ
- 4 (GMT-9:00) アラスカ
- 5 (GMT-8:00) 太平洋標準時 (米国およびカナダ)
- 6 (GMT-7:00) 山岳部標準時 (米国およびカナダ)
- 7 (GMT-6:00) 中央標準時 (米国およびカナダ)
- 8 (GMT-5:00) 東部標準時 (米国およびカナダ)
- 9 (GMT-4:00) 大西洋標準時 (カナダ)
- 10 (GMT-3:00) ブエノスアイレス (アルゼンチン)
- 11 (GMT-2:00) 中部大西洋
- 12 (GMT-1:00) アゾレス諸島
- 13 (GMT) ロンドン、リスボン、ダブリン、エディンバラ (デフォルト値)
- 14 (GMT+1:00) アムステルダム、ベルリン、ローマ、ウィーン
- 15 (GMT+2:00) エルサレム

- 16 (GMT+3:00) バグダッド
- 17 (GMT+4:00) マスカット、アブダビ
- 18 (GMT+4:30) カブール
- 19 (GMT+5:00) カラチ、イスラマバード、タシュケント
- 20 (GMT+5:30) コロンボ、コルカタ、ムンバイ、ニューデリー
- 21 (GMT+5:45) カトマンズ
- 22 (GMT+6:00) アルマトイ、ノボシビルスク
- 23 (GMT+6:30) ラングーン
- 24 (GMT+7:00) サイゴン、ハノイ、バンコク、ジャカルタ
- 25 (GMT+8:00) 香港、北京、重慶
- 26 (GMT+9:00) 東京、大阪、札幌
- 27 (GMT+9:30) ダーウィン
- 28 (GMT+10:00) シドニー、メルボルン、キャンベラ
- 29 (GMT+11:00) マガダン、ソロモン諸島、ニューカレドニア
- 30 (GMT+12:00) カムチャツカ、マーシャル諸島、フィジー
- 31 (GMT+12:00) オークランド (ニュージーランド)

(注) このコマンドを入力すると、DSTに入ったときに、コントローラが自動的にそのシステムクロックをDSTに合わせて設定します。米国では、DSTは3月の第2日曜日から始まり、11月の第1日曜日で終わります。

- 次のコマンドを入力して、DSTが自動的に設定されないように時間帯を手動で設定します。

**config time timezone delta\_hours delta\_mins**

*delta\_hours* は GMT と現地時間の差の時間部分、*delta\_mins* は GMT と現地時間の差の分部分です。

時間帯を手動で設定するときは、GMTを基準とした現在の時間帯の時差を +/- を付けて入力します。たとえば、米国の太平洋標準時は、GMTの時刻より8時間遅れています。したがって、-8と入力します。

(注) 時間帯を手動で設定することで、コントローラ CLI のみで DST が設定されることを回避できます。

- ステップ 3** 次のコマンドを入力して、変更を保存します。

**save config**

- ステップ 4** 次のコマンドを入力して、コントローラが現在の現地時間を現地の時間帯で表示していることを確認します。

**show time**



以下に類似した情報が表示されます。

```
Time..... Thu Apr 7 13:56:37 2011
Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
 NTP Polling Interval..... 3600

 Index NTP Key Index NTP Server NTP Msg Auth Status

 1 1 209.165.200.225 AUTH SUCCESS
```

- (注) 時間帯ロケーションが設定済みの場合は、[Timezone]の[Delta]の値は「0:0」に設定されます。時間帯デルタを使用して時間帯を手動で設定した場合は、[Timezone]の[Location]は空白になります。

## Telnet および Secure Shell セッションの設定

ここでは、Telnet およびセキュア シェル (SSH) の設定方法について説明します。

### Telnet と SSH について

Telnet は、コントローラの CLI にアクセスするためのネットワーク プロトコルです。Secure Shell (SSH) は Telnet のセキュリティをさらに強化したプロトコルであり、データ暗号化およびセキュア チャネルを使用してデータを転送します。コントローラ GUI と CLI のどちらでも、Telnet および SSH のセッションを設定できます。

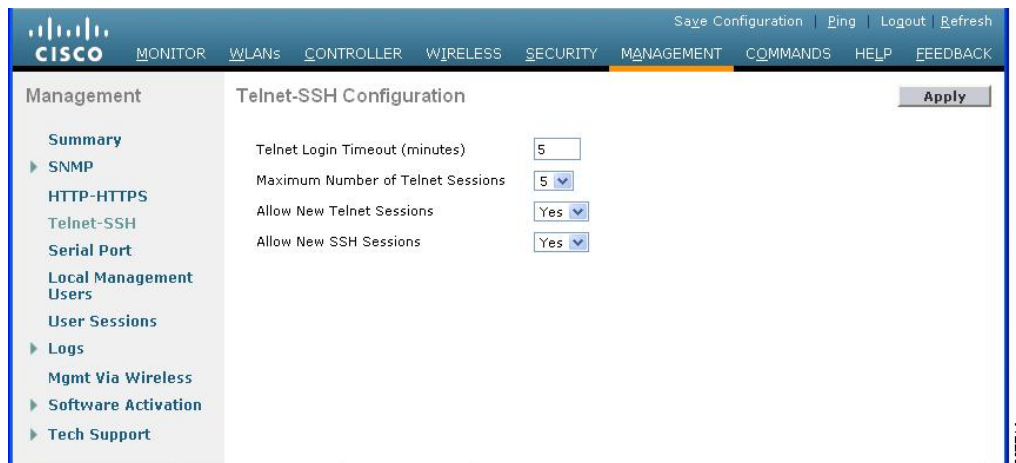
### Telnet および SSH の制約事項

- WLAN の制御に SSH を使用する場合、FIPS 認証アルゴリズム aes128-cbc のみサポートしています。
- コントローラは raw Telnet モードをサポートしていません。

## Telnet および SSH セッションの設定 (GUI)

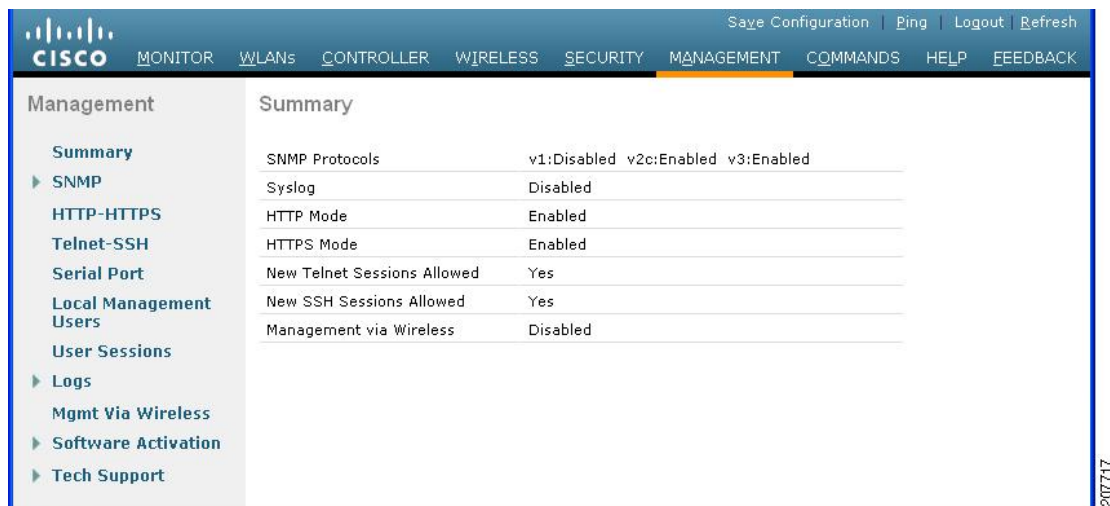
ステップ 1 [Management] > [Telnet-SSH] を選択して、[Telnet-SSH Configuration] ページを開きます。

図 17 : [Telnet-SSH Configuration] ページ



- ステップ 2** [Telnet Login Timeout] テキストボックスに、非アクティブの Telnet セッションを終了させるまでの時間を分単位で入力します。有効な値の範囲は 0 ～ 160 分で、デフォルト値は 5 分です。値 0 は、タイムアウトなしを示します。
- ステップ 3** [Maximum Number of Sessions] ドロップダウンリストから、同時 Telnet セッションまたは SSH セッションの最大数を選択します。有効な値の範囲は 0 ～ 5 セッションで、デフォルト値は 5 セッションです。値 0 は、Telnet セッションまたは SSH セッションを許可しないことを意味します。
- ステップ 4** コントローラ上での新規 Telnet セッションを許可する場合は [Allow New Telnet Sessions] ドロップダウンリストから [Yes] を選択し、許可しない場合は [No] を選択します。デフォルト値は [No] です。
- ステップ 5** コントローラ上での新規 SSH セッションを許可する場合は、ドロップダウンリストから [Yes] を選択し、許可しない場合は [No] を選択します。デフォルト値は [Yes] です。
- ステップ 6** [Apply] をクリックします。
- ステップ 7** [Save Configuration] をクリックします。
- ステップ 8** Telnet 設定の概要を表示するには、[Management] > [Summary] を選択します。[Summary] ページが表示されます。

図 18 : [Summary] ページ



Telnet および SSH の追加のセッションが許可されるかどうか、このページに表示されます。

## Telnet および SSH セッションの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、コントローラ上での新規 Telnet セッションを許可または禁止します。
- ```
config network telnet {enable | disable}
```

デフォルト値はディセーブルです。

- ステップ 2** 次のコマンドを入力して、コントローラ上での新規 SSH セッションを許可または禁止します。
config network ssh {enable | disable}

デフォルト値はイネーブルです。

- ステップ 3** 次のコマンドを入力して、非アクティブの Telnet セッションを終了させるまでの時間を分単位で指定します。

config sessions timeout timeout

timeout は、0 ～ 160 分の範囲内の値です。デフォルト値は 5 分です。値 0 は、タイムアウトなしを示します。

- ステップ 4** 次のコマンドを入力して、同時 Telnet セッションまたは SSH セッションの最大数を指定します。

config sessions maxsessions session_num

session_num は、0 ～ 5 の範囲内の値です。デフォルト値は 5 セッションです。値 0 は、Telnet セッションまたは SSH セッションを許可しないことを意味します。

- ステップ 5** 次のコマンドを入力して、変更を保存します。

save config

- ステップ 6** 次のコマンドを入力して、Telnet と SSH の設定を表示します。

show network summary

以下に類似した情報が表示されます。

```
RF-Network Name..... TestNetwork1
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Web Mode Cipher-Option SSLv2..... Disable
Secure Shell (ssh)..... Enable
Telnet..... Disable
...
```

- ステップ 7** 次のコマンドを入力して、Telnet セッションの設定を表示します。

show sessions

以下に類似した情報が表示されます。

```
CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

- ステップ 8** 次のコマンドを入力して、すべてのアクティブな Telnet セッションを表示します。

show loginsession

以下に類似した情報が表示されます。

```
ID      User Name      Connection From  Idle Time      Session Time
--  -----  -
```

00 admin EIA-232 00:00:00 00:19:04

ステップ 9 次のコマンドを入力して、すべてのアクティブな Telnet セッション、または特定の Telnet セッションを閉じることができます。

```
config loginsession close {all | session_id}
```

指定した管理ユーザの Telnet の権限の設定 (GUI)

コントローラを使用して、選択した管理ユーザに Telnet 特権を設定できます。そのためには、グローバルレベルで Telnet の特権を有効にしておく必要があります。デフォルトでは、すべての管理ユーザは、Telnet の特権が有効になっています。



(注) SSH セッションはこの機能による影響を受けません。

ステップ 1 [Management] > [Local Management Users] を選択します。

ステップ 2 [Local Management Users] ページで、管理ユーザの [Telnet Capable] チェックボックスをオンまたはオフにします。

ステップ 3 [Apply] をクリックします。

ステップ 4 [Save Configuration] をクリックします。

指定した管理ユーザの Telnet の権限の設定 (CLI)

• 次のコマンドを入力して、選択した管理ユーザに Telnet の特権を設定します。

```
config mgmtuser telnet user-name {enable | disable}
```

Telnet または SSH_old を使用したアクセスポイントのトラブルシューティング

コントローラは、Telnet プロトコルおよび Secure Shell (SSH) プロトコルを使用した Lightweight アクセスポイントのトラブルシューティングをサポートしています。これらのプロトコルを使用すると、特にアクセスポイントがコントローラに接続できない場合に、デバッグを簡単に行うことができます。

• 潜在的な競合やネットワークセキュリティの脅威を避けるために、Telnet または SSH のセッションを有効にしている間は **config terminal**、**telnet**、**ssh**、**rsh**、**ping**、**traceroute**、**clear**、**clock**、**crypto**、**delete**、**fsck**、**lwapp**、**mkdir**、**radius**、**release**、**reload**、**rename**、**renew**、**rmdir**、**save**、**set**、**test**、**upgrade** のコマンドを使用できないようになっています。

- Telnet または SSH のセッション中に使用できる主なコマンドは、**debug**、**disable**、**enable**、**help**、**led**、**login**、**logout**、**more**、**no debug**、**show**、**systat**、**undebug**、**where** です。



(注) コントローラ上で Telnet または SSH のセッションを設定する手順については、「[Telnet および Secure Shell セッションの設定](#)」セクションを参照してください。

Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (GUI)

-
- ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2 Telnet または SSH を有効にするアクセス ポイントの名前をクリックします。
- ステップ 3 [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。
- ステップ 4 [Telnet] チェックボックスをオンにして、このアクセス ポイント上の Telnet 接続を有効にします。デフォルトではオフになっています。
- ステップ 5 [SSH] チェックボックスをオンにして、このアクセス ポイント上の SSH 接続を有効にします。デフォルトではオフになっています。
- ステップ 6 [Apply] をクリックします。
- ステップ 7 [Save Configuration] をクリックします。
-

Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (CLI)

-
- ステップ 1 次のコマンドを入力して、アクセス ポイントで Telnet または SSH の接続を有効にします。
config ap {telnet | ssh} enable Cisco_AP
 デフォルト値はディセーブルです。
 (注) 次のコマンドを入力して、アクセス ポイントで Telnet または SSH の接続を無効にします。 **config ap {telnet | ssh} disable Cisco_AP**
- ステップ 2 次のコマンドを入力して、変更を保存します。
save config
- ステップ 3 次のコマンドを入力して、Telnet または SSH がアクセス ポイント上で有効かどうかを確認します。
show ap config general Cisco_AP
 以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 5
Cisco AP Name..... AP33
Country code..... Multiple Countries:US,AE,AR,AT,AU,BH
```

```
Reg. Domain allowed by Country..... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 2
MAC Address..... 00:19:2f:11:16:7a
IP Address Configuration..... Static IP assigned
IP Address..... 10.22.8.133
IP NetMask..... 255.255.248.0
Gateway IP Addr..... 10.22.8.1
Domain.....
Name Server.....
Telnet State..... Enabled
Ssh State..... Enabled
...
```

コントローラの無線管理

ワイヤレスクライアントを使用してコントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード以外のすべての管理タスクでサポートされています。

ワイヤレスクライアントデバイスから GUI または CLI を開くには、接続が許可されるようにコントローラを設定する必要があります。

ワイヤレス接続の有効化 (GUI)

-
- ステップ 1 GUI にログインします。
 - ステップ 2 [Management] > [Mgmt Via Wireless] ページを選択します。
 - ステップ 3 ワイヤレスクライアントからのアクセスが可能になるように、コントローラ管理を有効にします。
 - ステップ 4 [Apply] をクリックします。
-

ワイヤレス接続の有効化 (CLI)

- ステップ 1 CLI にログインします。
 - ステップ 2 **config network mgmt-via-wireless enable** コマンドを入力します。
 - ステップ 3 ワイヤレス クライアントを使用して、コントローラに接続されている Lightweight アクセス ポイントにアソシエートします。
 - ステップ 4 ワイヤレス クライアントで、コントローラの Telnet セッションを開くか、コントローラの GUI にブラウザからアクセスします。
-



第 3 章

ライセンスの管理

- [ライセンスのインストールおよび設定, 59 ページ](#)
- [ライセンスの再ホスト, 73 ページ](#)

ライセンスのインストールおよび設定

ライセンスのインストールおよび設定に関する情報

コントローラの基本キャパシティとして 12、25、50、100、250、または 500 台のアクセス ポイントをサポートする Cisco 5500 シリーズ コントローラを発注できます。キャパシティ Adder ライセンスによって、追加のアクセス ポイント キャパシティを追加できます。25、50、100、および 250 台のアクセス ポイント キャパシティを選択できます。キャパシティ Adder ライセンスは、任意の基本ライセンスに任意に組み合わせて追加でき、最大キャパシティはアクセス ポイント 500 台です。基本ライセンスと Adder ライセンスは、再ホストと RMA のいずれにも対応しています。基本ライセンスでは、標準の基本ソフトウェアセットがサポートされ、プレミアムソフトウェアセットが基本フィーチャセットの一部として含まれています。これには、次の機能が含まれます。

- Datagram Transport Layer Security (DTLS) データ暗号化：リモート WAN および LAN のリンク全体のセキュリティを向上させます。
- データ DTLS のアベイラビリティは次のとおりです。
 - Cisco 5500 シリーズ コントローラ：Cisco 5500 シリーズ コントローラは 2 つのライセンス オプションで使用でき、一方にはデータ DTLS 機能が含まれており、もう一方にはデータ DTLS が含まれていません。
 - 2500、WiSM2：これらのプラットフォームにはデフォルトで DTLS は含まれません。データ DTLS をオンにするには、ライセンスをインストールする必要があります。これらのプラットフォームには、データ DTLS を無効にした 1 つのイメージがあります。データ DTLS を使用するには、ライセンスが必要です。

- Cisco Flex 7500 と Cisco 8500 シリーズ コントローラ：DTLS ライセンスは組み込まれています。DTLS ライセンスを別にインストールする必要はありません。
- OfficeExtend アクセス ポイントのサポート：セキュアなモバイルテレワーキング環境を提供します。

現在、Wireless LAN Controller WPLUS ライセンスに含まれるすべての機能が基本ライセンスに含まれています。Cisco Prime Infrastructure BASE と PLUS のライセンスに変更はありません。WPlus ライセンスの機能は、基本ライセンスに含まれています。

- OfficeExtend AP
- エンタープライズ メッシュ
- CAPWAP データ暗号化

アップグレードライセンスおよびキャパシティ Adder ライセンスの詳細については、コントローラ モデルの製品データ シートを参照してください。

ライセンスの使用に関する制限

コントローラのライセンスを使用するときに留意する必要がある制限を次に示します。

- ソフトウェアリリースをアップグレードまたはダウングレードする際には、ライセンスの変更が無線 LAN 機能に影響する可能性があるため、これらのガイドラインに留意する必要があります。
 - WPlus ライセンスを所有し、6.0.x.x から 7.x.x.x にアップグレードした場合、ライセンス ファイルには、基本ライセンスと WPlus ライセンスの両方の機能が含まれます。機能のアベイラビリティと動作に問題はありません。
 - WPlus ライセンスを所有し、7.x.x.x から 6.0.196.0、6.0.188.0、または 6.0.182.0 にダウングレードした場合、ライセンスファイルには基本ライセンスのみが含まれます。WPlus 機能はすべて失われます。
 - 基本ライセンスを所有し、6.0.196.0 から 6.0.188.0 または 6.0.182.0 にダウングレードした場合、ダウングレード時に、WPlus 機能がすべて失われます。
- コントローラ ソフトウェア 7.0.116.0 以降のリリースでは、AP アソシエーション トラップは `ciscoLwappApAssociated` です。それ以前のリリースでは、トラップは `bsnAPAssociated` です。
- `ap-count` ライセンスおよび対応するイメージベース ライセンスは、同時にインストールされます。コントローラは、ライセンスを受けたアクセス ポイント数を認識しており、この数を超えるアクセス ポイントのアソシエートを許可しません。
- Cisco 5500 シリーズ コントローラには、永久と評価の両方の基本ライセンスと `base-ap-count` ライセンスが付属しています。必要に応じて、評価ライセンスをアクティブ化することもできます。このライセンスは、一時的に使用するためのものであり、60 日経過すると失効します。

- Cisco 5500 シリーズ コントローラの購入者がライセンスに関する作業を行う必要はありません。注文されたライセンスは、工場ですべてインストールされるからです。また、ライセンスおよび製品認証キー（PAK）は事前に、シリアル番号に対して登録されます。ただし、既存の無線ネットワークが拡大すると、サポート対象のアクセスポイント数の増加や、標準ソフトウェアセットから基本ソフトウェアセットへのアップグレードが必要になることがあります。その場合は、アップグレードライセンスを取得してインストールする必要があります。

アップグレードライセンスまたはキャパシティ Adder ライセンスの取得

ここでは、アップグレードライセンスまたはキャパシティ Adder ライセンスの取得方法について説明します。

アップグレードライセンスまたはキャパシティ Adder ライセンスの取得に関する情報

アップグレードライセンスを取得するには、製品認証キー（PAK）が記載された証明書が必要です。

キャパシティ Adder ライセンスを使用して、コントローラによってサポートされるアクセスポイントの数を最大 500 アクセスポイントまで増加できます。キャパシティ Adder ライセンスには、10、25、50、100、および 250 台のアクセスポイントキャパシティが用意されています。これらのライセンスは、アクセスポイントが 12、25、50、100、および 250 台の任意の基本キャパシティライセンスに追加できます。

たとえば、100 アクセスポイントのサポートを含むコントローラを最初に注文した場合（基本ライセンス AIR-CT5508-100-K9）、250 アクセスポイント、100 アクセスポイント、および 50 アクセスポイントの追加キャパシティライセンス（LIC-CT5508-250A、LIC-CT5508-100A、および LIC-CT5508-50A）を購入することにより、キャパシティを 500 アクセスポイントまで増加できます。

次の URL で、キャパシティ Adder ライセンスの注文の詳細を確認できます。http://www.cisco.com/en/US/products/ps10315/products_data_sheets_list.html



(注) アップグレード時に途中の段階をスキップした場合、たとえば -25U と -50U のライセンスをインストールしないで -100U をインストールした場合は、アップグレードしたキャパシティのライセンス登録に失敗します。

1 台のコントローラに対して、複数のアップグレードライセンス（たとえば、-25U、-50U、-100U、および -250U）を一度に注文することができます。このときに、購入者は 1 つの PAK と 1 つのライセンスを受け取ります。したがって、コントローラにインストールするライセンスは、4 つではなく 1 つだけです。

複数のコントローラを所有している場合に、すべてのコントローラをアップグレードするには、各アップグレードライセンスを複数、一度に注文することができます（たとえば、-25U、-50U、-100U、および -250U のアップグレードライセンスを 10 本ずつ注文）。このときに、購入者は 1 つの PAK と 1 つのライセンスを受け取ります。注文した数に達するまで、この PAK をコントローラのそれぞれに対して登録することができます。

基本ライセンス SKU およびキャパシティ Adder ライセンスの詳細については、各コントローラのデータシートを参照してください。

PAK 証明書の取得と登録

- ステップ 1** 担当のシスコ チャネル パートナーまたはシスコ営業担当者を通して、アップグレードライセンス用の PAK 証明書を注文します。オンラインで次の URL から注文することもできます。
<http://www.cisco.com/go/ordering>
- ステップ 2** オンラインで注文する場合は、最初にプライマリ アップグレード SKU **L-LIC-CT5508-UPG** または **LIC CT5508-UPG** を選択してください。次に、1 つの PAK で 1 つ以上のコントローラをアップグレードするために、次のオプションのうち必要なものをすべて選択します。証明書を受け取ったら、次のいずれかの方法を使用して PAK を登録します。
- **ライセンシング ポータル**：ライセンスを手動で取得してコントローラにインストールすることができます。ライセンシングポータルを使用して PAK を登録するには、ステップ 3 の手順に従ってください。
- ステップ 3** 次のようにライセンシングポータルを使用して PAK を登録します。
- a) <http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> にアクセスします。
 - b) メインの [Product License Registration] ページの [Product Authorization Key (PAK)] テキストボックスに、証明書と共に送付された PAK を入力して [Submit] をクリックします。
 - c) [Validate Features] ページで、登録するライセンス数を [Qty] テキストボックスに入力して [Update] をクリックします。
 - d) コントローラの製品 ID とシリアル番号を調べるには、コントローラ GUI で [Controller] > [Inventory] を選択するか、コントローラ CLI で **show license udi** コマンドを入力します。
次のような情報がコントローラ CLI に表示されます。
- | Device# | PID | SN | UDI |
|---------|---------------|------------|---------------------------|
| *0 | AIR-CT5508-K9 | CW1308L030 | AIR-CT5508-K9:FCW1308L030 |
- e) [Designate Licensee] ページで、ライセンスをインストールするコントローラの製品 ID とシリアル番号を入力し、エンドユーザーライセンス契約 (EULA) の条件を読んで同意し、このページの他のすべてのテキストボックスに入力して [Submit] をクリックします。
 - f) [Finish and Submit] ページで、すべての情報が正しいことを確認して [Submit] をクリックします。
 - g) 登録が完了したことを示すメッセージが表示されたら、[Download License] をクリックします。ライセンスは、電子メールで 1 時間以内に指定のアドレスへ送付されます。
 - h) 電子メールが届いたら、記載されている手順に従います。
 - i) ライセンス ファイルを TFTP サーバにコピーします。

ライセンスのインストール

ライセンスのインストール (GUI)

-
- ステップ 1** [Management] > [Software Activation] > [Commands] を選択して [License Commands] ページを開きます。
- ステップ 2** [Action] ドロップダウン リストから、[Install License] を選択します。 [Install License from a File] セクションが表示されます。
- ステップ 3** [File Name to Install] テキスト ボックスに、TFTP サーバ上のライセンス (*.lic) へのパスを入力します。
- ステップ 4** [Install License] をクリックします。 ライセンスが正常にインストールされたかどうかを示すメッセージが表示されます。 インストールに失敗した場合は、失敗の理由 (ライセンスが既存のライセンスである、パスが見つからない、ライセンスがこのデバイスのものではない、実行しているユーザにライセンスへのアクセス権がないなど) を示すメッセージが表示されます。
- ステップ 5** エンドユーザライセンス契約 (EULA) 同意のダイアログボックスが表示された場合は、内容を読んで、同意する場合は [Accept] をクリックしてください。
 (注) EULA への同意が必要になるのは一般に、評価、拡張、または再ホストのライセンスの場合です。 永久ライセンスの場合も EULA は必要ですが、同意はライセンス生成時に行われます。
- ステップ 6** 次の手順に従って、インストール済みのすべてのライセンスのバックアップ コピーを保存します。
- a) [Action] ドロップダウン リストから、[Save License] を選択します。
 - b) [File Name to Save] テキスト ボックスに、ライセンスを保存する TFTP サーバ上のパスを入力します。
 (注) 評価ライセンスは保存できません。
 - c) [Save Licenses] をクリックします。
- ステップ 7** コントローラをリブートします。
-

ライセンスのインストール (CLI)

-
- ステップ 1** このコマンドを入力して、ライセンスをコントローラにインストールします。
license install url
url は `tftp://server_ip/path/filename` です。
 (注) ライセンスをコントローラから削除するには、**license clear license_name** コマンドを入力します。 ライセンスの削除が必要になるのは、評価ライセンスの期限が切れたときや、未使用のライセンスがある場合などです。 有効期限前のライセンス、永久ベースイメージライセンス、またはコントローラによって使用されるライセンスは削除できません。
- ステップ 2** エンドユーザライセンス契約 (EULA) の画面が表示されたときは、内容を読んで同意してください。

(注) EULA への同意が必要になるのは一般に、評価、拡張、または再ホストのライセンスの場合です。永久ライセンスの場合も EULA は必要ですが、同意はライセンス生成時に行われます。

ステップ 3 このコマンドを入力して、ライセンスにコメントを追加するか、またはライセンスからコメントを削除します。

license comment {add | delete} *license_name comment_string*

ステップ 4 このコマンドを入力して、インストール済みのすべてのライセンスのバックアップコピーを保存します。

license save *url*

url は `tftp://server_ip/path/filename` です。

ステップ 5 次のコマンドを入力して、コントローラをリブートします。

reset system

ライセンスの表示

ライセンスの表示 (GUI)

ステップ 1 [Management] > [Software Activation] > [Licenses] を選択して、[Licenses] ページを開きます。このページには、コントローラにインストールされているすべてのライセンスが一覧表示されます。各ライセンスの、ライセンスタイプ、期限、カウント（このライセンスで許可されるアクセスポイント最大数）、優先度（低、中、高）、およびステータス（使用中、非使用中、非アクティブ、または EULA 未同意）が表示されます。

(注) コントローラプラットフォームは、ライセンスタイプとして「`grace period`」または「`extension`」のステータスをサポートしません。猶予期間または拡張の評価ライセンスがインストールされている場合でも、ライセンスステータスには「`evaluation`」が常に表示されます。

(注) ライセンスをコントローラから削除するには、そのライセンスの青いドロップダウン矢印の上にカーソルを置いて、[Remove] をクリックします。ライセンスの削除が必要になるのは、評価ライセンスの期限が切れたときや、未使用のライセンスがある場合などです。有効期限前のライセンス、永久ベースイメージライセンス、またはコントローラによって使用されるライセンスは削除できません。

ステップ 2 目的のライセンスのリンクをクリックして、特定のライセンスについての詳細を表示します。[License Detail] ページが表示されます。

このページには、そのライセンスに関する次のような追加情報が表示されます。

- ライセンスタイプ（永久、評価、または拡張）
- ライセンスのバージョン
- ライセンスのステータス（使用中、非使用中、非アクティブ、EULA 未同意）

- ライセンスの有効期間
 - (注) 永久ライセンスには期限はありません。
- ライセンスが組み込みライセンスかどうか
- このライセンスで許可されるアクセス ポイントの最大数
- このライセンスを現在使用しているアクセス ポイントの数

ステップ 3 このライセンスに対するコメントを入力する場合は、[Comment] テキスト ボックスに入力して [Apply] をクリックします。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

ライセンスの表示 (CLI)

はじめる前に

- 次のコマンドを入力して、コントローラのライセンス レベル、ライセンス タイプ、およびライセンスで許可されたアクセス ポイントの数を表示します。

show sysinfo

以下に類似した情報が表示されます。

```

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 7.0
RTOS Version..... 7.0
Bootloader Version..... 5.2
Emergency Image Version..... N/A
Build Type..... DATA + WPS
System Name..... Cisco 69
System Location..... na
System Contact..... abc@cisco.com
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 10.10.10.10
System Up Time..... 3 days 1 hrs 12 mins 42 secs
System Timezone Location.....
CurrentBoot License Level.....base
CurrentBoot License Type.....Permanent
NextBoot License Level.....base
NextBoot License Type.....Permanent
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +40 C
State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 4
Number of Active Clients..... 0
Burned-in MAC Address..... 00:1A:6D:DD:1E:40
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
Maximum number of APs supported..... 12

```



(注) Cisco Flex 7500 シリーズ コントローラの場合、[Operating Environment] および [Internal Temp Alarm Limits] のデータは表示されません。

- このコマンドを入力して、コントローラにインストールされているすべてのアクティブなライセンスの簡単な要約を表示します。

show license summary

以下に類似した情報が表示されます。

```
Index 1 Feature: wplus
          Period left: 0 minute 0 second
Index 2 Feature: wplus-ap-count
          Period left: 0 minute 0 second
Index3  Feature: base
          Period left: Life time
          License Type: Permanent
          License State: Active, In Use
          License Count: Non-Counted
          License Priority: Medium
Index 4 Feature: base-ap-count
          Period left: 6 weeks, 4 days
          License Type: Evaluation
          License State: Active, In Use
          License Count: 250/250/0
          License Priority: High
```

- このコマンドを入力して、コントローラにインストールされているすべてのライセンスを表示します。

show license all

以下に類似した情報が表示されます。

```
License Store: Primary License Storage
StoreIndex: 1 Feature: base Version: 1.0
          License Type: Permanent
          License State: Active, Not in Use
          License Count: Non-Counted
          License Priority: Medium

StoreIndex: 3 Feature: base-ap-count Version: 1.0
          License Type: Evaluation
          License State: Active, In Use
          Evaluation total period: 8 weeks 4 days
          Evaluation period left: 8 weeks 3 days
          License Count: 250/0/0
          License Priority: High
```

- 次のコマンドを入力して、特定のライセンスの詳細を表示します。

show license detail license_name

以下に類似した情報が表示されます。

```
Index: 1 Feature: base-ap-count Version: 1.0
          License Type: Permanent
          License State: Active, Not in Use
          License Count: 12/0/0
          License Priority: Medium
          Store Index: 0
```



```

Store Name: Primary License Storage

Index: 2      Feature: base-ap-count  Version: 1.0
License Type: Evaluation
License State: Inactive
      Evaluation total period: 8 weeks 4 days
      Evaluation period left: 8 weeks 4 days
License Count: 250/0/0
License Priority: Low
Store Index: 3
      Store Name: Evaluation License Storage

```

- このコマンドを入力して、すべての期限のあるライセンス、評価ライセンス、永久ライセンス、または使用中のライセンスを表示します。

show license {expiring | evaluation | permanent | in-use}

show license in-use コマンドの場合は、次のような情報が表示されます。

```

StoreIndex: 2  Feature: base-ap-count  Version: 1.0
License Type: Permanent
License State: Active, In Use
License Count: 12/12/0
License Priority: Medium
StoreIndex: 3  Feature: base Version: 1.0
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted License Priority: Medium

```



(注) コントローラプラットフォームは、ライセンスタイプとして「**grace period**」または「**extension**」のステータスをサポートしません。猶予期間または拡張の評価ライセンスがインストールされている場合でも、ライセンスステータスには「**evaluation**」が常に表示されます。

- このコマンドを入力して、コントローラ上のこのライセンスに対して許可されているアクセスポイントの最大数、コントローラに現在 **join** しているアクセスポイントの数、およびコントローラに追加で **join** できるアクセスポイントの数を表示します。

show license capacity

以下に類似した情報が表示されます。

Licensed Feature	Max Count	Current Count	Remaining Count
AP Count	250	4	246

- このコマンドを入力して、コントローラ上のすべてのライセンスの統計情報を表示します。

show license statistics

- 次のコマンドを入力して、ライセンスによって使用可能となった機能の要約を表示します。

show license feature

サポートされるアクセスポイントの最大数の設定

サポートされるアクセスポイントの最大数の設定 (GUI)

コントローラでサポートできる AP の最大数を設定できます。コントローラは、ライセンス情報とコントローラモデルに基づいて、サポートされる AP の最大数を制限します。ユーザが設定した値のほうがライセンスを受けている値よりも多い場合、ライセンス情報でサポートが指定されている AP の最大数のほうが、ユーザが設定する数よりも優先されます。デフォルトでは、この機能は無効になっています。設定を変更する場合、コントローラをリブートする必要があります。

ステップ 1 [Controller] > [General] を選択します。

ステップ 2 [Maximum Allowed APs] テキスト ボックスに値を入力します。

ステップ 3 [Apply] をクリックします。

ステップ 4 [Save Configuration] をクリックします。

サポートされるアクセスポイントの最大数の設定 (CUI)

- 次のコマンドを入力して、コントローラでサポートされるアクセスポイントの最大数を設定します。

```
config ap max-count count
```

- 次のコマンドを入力して、コントローラでサポートされるアクセスポイントの最大数を表示します。

```
show ap max-count summary
```

ライセンスの問題のトラブルシューティング

- このコマンドを入力して、ライセンス コア イベントおよびライセンス コア エラーのデバッグを設定します。

```
debug license core {all | errors | events} {enable | disable}
```

- このコマンドを入力して、ライセンス エラーのデバッグを設定します。

```
debug license errors {enable | disable}
```

- このコマンドを入力して、ライセンス イベントのデバッグを設定します。

```
debug license events {enable | disable}
```

ap-count 評価ライセンスのアクティブ化

ap-count 評価ライセンスのアクティブ化に関する情報

アクセスポイント数の多いライセンスにアップグレードする場合は、永久バージョンのライセンスにアップグレードする前に評価ライセンスを試すことができます。たとえば、使用している永久ライセンスのアクセスポイント数が 50 の場合に、アクセスポイント数が 100 の評価ライセンスを 60 日間試用できます。

ap-count 評価ライセンスの優先順位は、デフォルトで low に設定されるので、コントローラでは ap-count 永久ライセンスが使用されます。アクセスポイント数を増やした評価ライセンスを試す場合は、優先順位を high に変更する必要があります。そのような高容量は必要ないと判断した場合は、ap-count 評価ライセンスの優先順位を下げて、コントローラで永久ライセンスが使用されるようにすることができます。



- (注) 操作の中断を避けるために、コントローラは、評価ライセンスの有効期限が切れてもライセンスを切り替えません。永久ライセンスに戻すには、コントローラをリブートする必要があります。リブート後に、期限切れになった評価ライセンスと同じフィーチャセットレベルにコントローラがデフォルト設定されます。同じフィーチャセットレベルの永久ライセンスがインストールされていない場合、コントローラは、別のレベルの永久ライセンスまたは有効期限の切れていない評価ライセンスを使用します。

ap-count 評価ライセンスのアクティブ化 (GUI)

- ステップ 1** [Management] > [Software Activation] > [Licenses] を選択して、[Licenses] ページを開きます。
[Status] カラムは現在どのライセンスが使用されているかを示し、[Priority] カラムは各ライセンスの現在の優先度を示します。
- ステップ 2** 次のように ap-count 評価ライセンスをアクティブ化します。
- アクティブ化する ap-count 評価ライセンスのリンクをクリックします。[License Detail] ページが表示されます。
 - [Priority] ドロップダウンリストから [High] を選択して [Set Priority] をクリックします。
(注) 優先順位を設定できるのは、ap-count 評価ライセンスに限られます。ap-count 永久ライセンスの優先順位は常に medium であり、設定できません。
 - ライセンスの優先度変更についての決定を確認する画面が表示されたら、[OK] をクリックします。
 - EULA が表示されたら、契約内容を読んで [Accept] をクリックします。
 - コントローラをリブートするという画面が表示されたら、[OK] をクリックします。
 - 優先度の変更を有効にするために、コントローラをリブートします。

- g) [Licenses] をクリックして [Licenses] ページを開き、ap-count 評価ライセンスの優先度が「High」、ステータスが「InUse」であることを確認します。評価ライセンスは、期限が切れるまで使用できます。

ステップ 3 ap-count 評価ライセンスの使用を停止して再び ap-count 永久ライセンスを使用する場合の手順は次のとおりです。

- a) [Licenses] ページで、使用中の ap-count 評価ライセンスへのリンクをクリックします。
- b) [Priority] ドロップダウンリストから [Low] を選択して [Set Priority] をクリックします。
(注) 優先順位を設定できるのは、ap-count 評価ライセンスに限られます。ap-count 永久ライセンスの優先順位は常に medium であり、設定できません。
- c) ライセンスの優先度変更についての決定を確認する画面が表示されたら、[OK] をクリックします。
- d) EULA が表示されたら、契約内容を読んで [Accept] をクリックします。
- e) コントローラをリブートするという画面が表示されたら、[OK] をクリックします。
- f) 優先度の変更を有効にするために、コントローラをリブートします。
- g) [Licenses] をクリックして [Licenses] ページを開き、ap-count 評価ライセンスの優先度が「Low」、ステータスが「Not in Use」であることを確認します。ap-count 永久ライセンスのほうは「使用中」となるはずですが。

ap-count 評価ライセンスのアクティブ化 (CLI)

ステップ 1 次のコマンドを入力して、コントローラ上のすべてのライセンスの現在のステータスを確認します。
show license all

以下に類似した情報が表示されます。

```
License Store: Primary License Storage
StoreIndex: 0 Feature: base-ap-count Version: 1.0
License Type: Permanent
License State: Active, In Use
License Count: 12/0/0
License Priority: Medium
StoreIndex: 1 Feature: base Version: 1.0
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium
StoreIndex: 2 Feature: base Version: 1.0
License Type: Evaluation
License State: Inactive
Evaluation total period: 8 weeks 4 days
Evaluation period left: 8 weeks 4 days
License Count: Non-Counted
License Priority: Low
StoreIndex: 3 Feature: base-ap-count Version: 1.0
License Type: Evaluation
```

```
License State: Inactive
  Evaluation total period:  8 weeks  4 days
  Evaluation period left:  8 weeks  4 days
License Count: 250/0/0
  License Priority: Low
```

[License State] テキストボックスには使用中のライセンスが表示され、[License Priority] テキストボックスには各ライセンスの現在の優先度が表示されます。

(注) 7.2.110.0 リリースでは、接続された APS がなくてもアクティブな base-ap-count ライセンスの使用数の数が、コマンド出力にすべて表示されます。

ステップ 2 次のように ap-count 評価ライセンスをアクティブ化します。

a) 次のコマンドを入力して、base-ap-count 評価ライセンスの優先度を上げます。

```
license modify priority license_name high
```

(注) 優先順位を設定できるのは、ap-count 評価ライセンスに限られます。ap-count 永久ライセンスの優先順位は常に medium であり、設定できません。

b) 次のコマンドを入力して、優先度の変更を反映させるためにコントローラをリブートします。

```
reset system
```

c) 次のコマンドを入力して、ap-count 評価ライセンスが高い優先順位を持つようになり、使用されていることを確認します。

```
show license all
```

評価ライセンスは、期限が切れるまで使用できます。

ステップ 3 ap-count 評価ライセンスの使用を停止して再び ap-count 永久ライセンスを使用する場合の手順は次のとおりです。

a) 次のコマンドを入力して、ap-count 評価ライセンスの優先度を下げます。

```
license modify priority license_name low
```

b) 次のコマンドを入力して、優先度の変更を反映させるためにコントローラをリブートします。

```
reset system
```

c) 次のコマンドを入力して、ap-count 評価ライセンスが低い優先順位を持つようになり、使用されていないことを確認します。

```
show license all
```

ap-count 永久ライセンスのほうは「使用中」となるはずですが。

使用権ライセンスの設定

使用権ライセンスに関する情報

使用権 (RTU) ライセンスは、ライセンスが Unique Device Identifier (UDI)、製品 ID、またはシリアル番号に関連付けられていないモデルです。エンドユーザライセンス契約 (EULA) に同意

した後に、RTU ライセンスを使用して、コントローラ上での必要なライセンス数を有効にします。これにより、外部ツールとやり取りするコントローラに AP 数を追加できます。

RTU ライセンスは、Cisco Flex 7500 シリーズおよび Cisco 8500 シリーズ Wireless LAN Controller でのみサポートされます。

RTU ライセンス モデルでは、次のタイプのライセンスを使用できます。

- 永続ライセンスまたは基本ライセンス：これらのライセンスは、製造時にコントローラハードウェアにプログラムされます。これらは、削除または転送できない **base count** ライセンスです。
- Adder ライセンス：これらのライセンスは、RTU EULA に同意してアクティブ化できるワイヤレス アクセス ポイント数ライセンスです。EULA には、アクティベーション時に指定したアクセスポイント数ライセンスを購入する義務がユーザにあることが記載されています。購入したアクセスポイント数のライセンスをアクティブ化し、EULA に同意する必要があります。

1 台のコントローラから Adder ライセンスを削除して、同じ製品ファミリの別のコントローラにライセンスを転送できます。たとえば、LIC-CT7500-100A などの Adder ライセンスを、1 台の Cisco Flex 7500 シリーズ コントローラから別の Cisco Flex 7500 シリーズ コントローラに（部分的または完全に）転送できます。



(注) 出荷時にコントローラに組み込まれたライセンスは転送できません。

- 評価ライセンス：これらのライセンスは、90 日間有効なデモ モードまたは試用モードのライセンスです。90 日間の有効期限が切れる 15 日前に、永久ライセンスを購入する要件に関する通知があります。これらの評価ライセンスは、ライセンスのイメージとともにインストールされます。コマンドで評価ライセンスをいつでもアクティブ化できます。コントローラ CLI でアクティベーション コマンドを実行した後で、EULA のプロンプトが表示されます。EULA には、90 日間の使用中に、指定したライセンス数の支払いを行う義務がユーザにあることが記載されています。カウントダウンは EULA に同意した時点から開始されます。

コントローラのアクセス ポイント Adder ライセンスを追加または削除するたびに、RTU EULA のプロンプトが表示されます。それぞれの追加操作または削除操作について、RTU EULA の同意または拒否を行えます。

ハイアベイラビリティ (HA) コントローラでは HA を有効にすると、コントローラは、有効にしたプライマリコントローラのライセンス数と同期し、プライマリコントローラ上で有効にしたライセンス数までのハイアベイラビリティをサポートします。

コントローラ GUI またはコントローラ CLI を使用して、RTU ライセンスを表示できます。また、Cisco Prime Infrastructure を使用して、複数のワイヤレス コントローラのライセンスを表示することもできます。

使用権ライセンスの設定 (GUI)

-
- ステップ 1** [Management] > [Software Activation] > [Licenses] を選択して、[Licenses] ページを開きます。
- ステップ 2** [Adder License] 領域で、AP ライセンスがサポートできる AP 数を選択して追加または削除し、[Set Count] をクリックします。
- ステップ 3** [Save Configuration] をクリックします。
-

使用権ライセンスの設定 (CLI)

- 次のコマンドを入力して、AP ライセンスがサポートできる APS 数を追加または削除します。
license {add | delete} ap-count count
- 次のコマンドを入力して、機能のライセンスを追加または削除します。
license {add | delete} feature license_name
- 次のコマンドを入力して、評価 AP 数ライセンスをアクティブ化または非アクティブ化します。
license {activate | deactivate} ap-count eval



(注) ライセンスをアクティブ化すると、指定したライセンスのエンド ユーザ ライセンス契約 (EULA) の同意または拒否を求めるプロンプトが表示されます。コントローラに接続された現在の AP 数より少ない APS 数をサポートするライセンスをアクティブ化した場合、アクティベーション コマンドは失敗します。

- 次のコマンドを入力して、機能のライセンスをアクティブ化または非アクティブ化します。
license {activate | deactivate} feature license_name
- 次のコマンドを入力して、ライセンス情報を表示します。
show license all

ライセンスの再ホスト

ここでは、ライセンスを再ホストする方法について説明します。

ライセンスの再ホストについて

あるコントローラのライセンスを無効にして、別のコントローラにインストールする操作を再ホストと呼びます。コントローラの目的を変更するために、ライセンスの再ホストが必要になる場合があります。たとえば、OfficeExtend または屋内メッシュアクセス ポイントを別のコントローラに移動する場合、あるコントローラから同じモデルの別のコントローラに Adder ライセンスを移行できます（モデル内移行）。これは、ライセンスをアプライアンス間で移動する必要がある RMA またはネットワークの再構築で実行できます。ネットワークを再構築する通常のシナリオで、基本ライセンスを再ホストすることはできません。RMA について、基本ライセンスの転送が許可される唯一の例外は、既存のアプライアンスに障害があるときに交換用ハードウェアを取得する場合です。

評価ライセンスを再ホストすることはできません。

ライセンスを再ホストするには、コントローラからクレデンシャルを生成する必要があります。このクレデンシャルを使用して取得した許可チケットを使用して、シスコのライセンシング サイトへのライセンス登録を取り消します。次に、再ホストチケットを取得し、そのチケットを使用して、ライセンスをインストールするコントローラ用のライセンスインストールファイルを取得します。



(注) 取り消したライセンスを同じコントローラに再インストールすることはできません。



(注) リリース 7.3 より、使用ライセンスは Cisco Flex 7500 シリーズ コントローラでサポートされており、これらのコントローラでは再ホスト動作が変更されています。ライセンスを再ホストする必要がある場合、インストール済みの Adder ライセンスをアップグレードする前に再ホストを実行する必要があります。

ライセンスの再ホスト

ライセンスの再ホスト (GUI)

- ステップ 1 [Management] > [Software Activation] > [Commands] を選択して、[License Commands] ページを開きます。
- ステップ 2 [Action] ドロップダウンリストから [Rehost] を選択します。[Revoke a License from the Device and Generate Rehost Ticket] 領域が表示されます。
- ステップ 3 [File Name to Save Credentials] テキスト ボックスに、デバイス クレデンシャルを保存する TFTP サーバ上のパスを入力して [Save Credentials] をクリックします。
- ステップ 4 ライセンスを取り消すための許可チケットを取得するには、次の手順を実行します。
 - a) [Cisco Licensing] (<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet>) をクリックします。
 - b) [Product License Registration] ページで、[Manage Licenses] の下の [Look Up a License] をクリックします。

- c) コントローラの製品 ID とシリアル番号を入力します。
(注) コントローラの製品 ID とシリアル番号を調べるには、コントローラ GUI で [Controller] > [Inventory] を選択します。
- d) **ステップ 3** で保存したデバイス クレデンシャルのファイルを開いて内容をコピーし、[Device Credentials] テキスト ボックスにペーストします。
- e) セキュリティ コードを空のボックスに入力して [Continue] をクリックします。
- f) このコントローラから取り消すライセンスを選択して [Start License Transfer] をクリックします。
- g) [Rehost Quantities] ページで、取り消すライセンスの数を [To Rehost] テキスト ボックスに入力して [Continue] をクリックします。
- h) [Designate Licensee] ページで、ライセンスを取り消すコントローラの製品 ID とシリアル番号を入力し、エンド ユーザ ライセンス契約 (EULA) の条件を読んで同意し、このページの他のすべてのテキスト ボックスに入力して [Continue] をクリックします。
- i) [Review and Submit] ページで、すべての情報が正しいことを確認して [Submit] をクリックします。
- j) 登録が完了したことを示すメッセージが表示されたら、[Download Permission Ticket] をクリックします。再ホスト許可チケットは、電子メールで 1 時間以内に指定のアドレスへ送付されます。
- k) 電子メールが届いたら、再ホスト許可チケットを TFTP サーバにコピーします。

ステップ 5 次の手順に従って、再ホスト許可チケットを使用してライセンスをこのコントローラから取り消し、再ホスト チケットを生成します。

- a) [Enter Saved Permission Ticket File Name] テキスト ボックスに、**ステップ 4** で生成した再ホスト許可チケットの TFTP パスとファイル名 (*.lic) を入力します。
- b) [Rehost Ticket File Name] テキスト ボックスに、このライセンスを別のコントローラに再ホストするためのチケットの TFTP パスとファイル名 (*.lic) を入力します。
- c) [Generate Rehost Ticket] をクリックします。
- d) エンド ユーザ ライセンス契約 (EULA) 同意のダイアログボックスが表示された場合は、内容を読んで、同意する場合は [Accept] をクリックしてください。

ステップ 6 次の手順に従って、**ステップ 5** で生成された再ホスト チケットを使用してライセンス インストール ファイル (後で別のコントローラにインストールするのに使用します) を取得します。

- a) [Cisco Licensing] をクリックします。
- b) [Product License Registration] ページの [Manage Licenses] の下にある [Upload Rehost Ticket] をクリックします。
- c) [Upload Ticket] ページの [Enter Rehost Ticket] テキスト ボックスに、**ステップ 5** で生成した再ホスト チケットを入力して [Continue] をクリックします。
- d) [Validate Features] ページで、コントローラのライセンス情報が正しいことを確認して、再ホストの数を入力し、[Continue] をクリックします。
- e) [Designate Licensee] ページで、ライセンスを使用するコントローラの製品 ID とシリアル番号を入力し、エンド ユーザ ライセンス契約 (EULA) の条件を読んで同意し、このページの他のすべてのテキスト ボックスに入力して [Continue] をクリックします。
- f) [Review and Submit] ページで、すべての情報が正しいことを確認して [Submit] をクリックします。
- g) 登録が完了したことを示すメッセージが表示されたら、[Download License] をクリックします。再ホスト ライセンス キーは、電子メールで 1 時間以内に指定のアドレスへ送付されます。
- h) 電子メールが届いたら、再ホスト ライセンス キーを TFTP サーバにコピーします。

- i) 「ライセンスのインストール」の項の手順に従って、これを別のコントローラ上にインストールします。

ライセンスの再ホスト (CLI)

ステップ 1 次のコマンドを入力して、デバイス クレデンシャル情報をファイルに保存します。

license save credential url

url は `tftp://server_ip/path/filename` です。

ステップ 2 次の手順に従って、ライセンスを取り消すための許可チケットを取得します。

- a) <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> にアクセスします。 [Product License Registration] ページが表示されます。
- b) [Manage Licenses] の下の [Look Up a License] をクリックします。
- c) コントローラの製品 ID とシリアル番号を入力します。
(注) コントローラの製品 ID とシリアル番号を調べるには、コントローラ CLI で **show license udi** コマンドを入力します。
- d) **ステップ 1** で保存したデバイス クレデンシャルのファイルを開いて内容をコピーし、[Device Credentials] テキスト ボックスにペーストします。
- e) セキュリティ コードを空のボックスに入力して [Continue] をクリックします。
- f) このコントローラから取り消すライセンスを選択して [Start License Transfer] をクリックします。
- g) [Rehost Quantities] ページで、取り消すライセンスの数を [To Rehost] テキスト ボックスに入力して [Continue] をクリックします。
- h) [Designate Licensee] ページで、ライセンスを取り消すコントローラの製品 ID とシリアル番号を入力し、エンドユーザ ライセンス契約 (EULA) の条件を読んで同意し、このページの他のすべてのテキスト ボックスに入力して [Continue] をクリックします。
- i) [Review and Submit] ページで、すべての情報が正しいことを確認して [Submit] をクリックします。
- j) 登録が完了したことを示すメッセージが表示されたら、[Download Permission Ticket] をクリックします。再ホスト許可チケットは、電子メールで 1 時間以内に指定のアドレスへ送付されます。
- k) 電子メールが届いたら、再ホスト許可チケットを TFTP サーバにコピーします。

ステップ 3 次の手順に従って、再ホスト許可チケットを使用してライセンスをこのコントローラから取り消し、再ホストチケットを生成します。

- a) 次のコマンドを入力して、コントローラからライセンスを取り消します。

license revoke permission_ticket url

permission_ticket_url は `tftp://server_ip/path/filename` です。

- b) 次のコマンドを入力して、再ホスト チケットを生成します。

license revoke rehost rehost_ticket url

rehost_ticket_url は `tftp://server_ip/path/filename` です。

c) エンドユーザライセンス契約（EULA）が表示されたら、内容を読んで同意します。

ステップ 4 次の手順に従って、**ステップ 3** で生成された再ホストチケットを使用してライセンスインストールファイル（後で別のコントローラにインストールするのに使用します）を取得します。

- a) <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet> にアクセスします。
- b) [Product License Registration] ページの [Manage Licenses] の下にある [Upload Rehost Ticket] をクリックします。
- c) [Upload Ticket] ページの [Enter Rehost Ticket] テキストボックスに、**ステップ 3** で生成した再ホストチケットを入力して [Continue] をクリックします。
- d) [Validate Features] ページで、コントローラのライセンス情報が正しいことを確認して、再ホストの数を入力し、[Continue] をクリックします。
- e) [Designate Licensee] ページで、ライセンスを使用するコントローラの製品 ID とシリアル番号を入力し、エンドユーザライセンス契約（EULA）の条件を読んで同意し、このページの他のすべてのテキストボックスに入力して [Continue] をクリックします。
- f) [Review and Submit] ページで、すべての情報が正しいことを確認して [Submit] をクリックします。
- g) 登録が完了したことを示すメッセージが表示されたら、[Download License] をクリックします。再ホストライセンスキーは、電子メールで 1 時間以内に指定のアドレスへ送付されます。
- h) 電子メールが届いたら、再ホストライセンスキーを TFTP サーバにコピーします。
- i) **ライセンスのインストール (GUI)**、**(63 ページ)** の項の手順に従って、このライセンスを別のコントローラにインストールします。

RMA 後にライセンスを交換コントローラに転送する

RMA 後の交換コントローラへのライセンスの転送について

Return Material Authorization（RMA）プロセスの中で Cisco 5500 シリーズ コントローラをシスコに返却した場合は、そのコントローラのライセンスを 60 日以内に、シスコから受け取った交換コントローラに転送する必要があります。

交換コントローラに事前インストールされるライセンスは、永久 base と評価 base、base-ap-count です。これ以外の永久ライセンスはインストールされていません。交換コントローラの SKU は AIR-CT5508-CA-K9 です。

ライセンスはコントローラのシリアル番号に対して登録されるので、返却したコントローラのライセンスを取り消して交換コントローラで使用するには、Cisco.com のライセンシングポータルを使用して、この許可を要求します。要求が承認されたら、古いライセンスを交換コントローラにインストールします。返却したコントローラにインストールした場合は、追加の ap-count ライセンスを交換コントローラ上で再ホストする必要があります。開始する前に、返却したコントローラと交換コントローラの両方の製品 ID とシリアル番号を用意してください。この情報は、購入記録に含まれています。



- (注) 交換コントローラにインストールされている評価ライセンスは一時的な使用を目的としているので、60日後に失効します。操作の中断を避けるために、コントローラは、評価ライセンスの有効期限が切れてもライセンスを切り替えません。永久ライセンスに戻すには、コントローラをリブートする必要があります。故障したコントローラのライセンスを交換コントローラにインストールする前に評価ライセンスの期限が切れた場合は、交換コントローラは引き続き永久 base ライセンスを使用して動作しますが、そのコントローラにアクセスポイントが join することはできなくなります。

RMA 後の交換コントローラへのライセンスの転送

- ステップ 1 <http://cisco.com/go/license> にブラウザからアクセスします。
- ステップ 2 [Product License Registration] ページで、[Transfer] > [License for RMA] を選択します。
- ステップ 3 [Specify Device] をクリックし、[Product Family] ドロップダウンリストからコントローラ モデルを選択します。
- ステップ 4 画面の指示を完了して、ライセンス ファイルを生成します。
ライセンスはオンラインまたは電子メールで提供されます。
- ステップ 5 ライセンス ファイルを TFTP サーバにコピーします。
- ステップ 6 [Management] > [Software Activation] > [Commands] > [Action] > [Install License] を選択して、ライセンスをインストールします。



第 4 章

802.11 帯域の設定

- [802.11 帯域の設定, 79 ページ](#)
- [帯域選択の設定, 84 ページ](#)

802.11 帯域の設定

802.11 帯域の設定について

自国の法的な規制基準を遵守するために、コントローラの 802.11b/g/n (2.4GHz) 帯域と 802.11a/n/ac (5GHz) 帯域を設定できます。デフォルトでは、802.11b/g/n と 802.11a/n/ac の両方がイネーブルになっています。

コントローラが 802.11g トラフィックだけを許可するように設定されている場合、802.11b クライアントデバイスはアクセスポイントに正常に接続できますが、トラフィックを送信できません。802.11g トラフィック専用コントローラを設定する場合、必須として 11g レートをマークする必要があります。

802.11 帯域の設定 (GUI)

- ステップ 1** [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] を選択して、[Global Parameters] ページを開きます。
- ステップ 2** [802.11a (または 802.11b/g) Network Status] チェックボックスをオンにして、802.11a または 802.11b/g 帯域を有効にします。帯域を無効にするには、チェックボックスをオフにします。デフォルト値はイネーブルです。802.11a 帯域と 802.11b/g 帯域の両方を有効にすることができます。
- ステップ 3** ステップ 2 で 802.11b/g 帯域を有効にした場合、802.11g ネットワーク サポートを有効にするときは、[802.11g Support] チェックボックスをオンにします。デフォルト値はイネーブルです。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。
- ステップ 4** 20 ~ 1000 ミリ秒の範囲内の値を [Beacon Period] テキストボックスに入力して、アクセスポイントが SSID のブロードキャストを行う周期を指定します。デフォルト値は 100 ミリ秒です。
- (注) コントローラ内でのビーコン period はミリ秒の単位で示されます。ビーコン周期の単位には、単位時間 (TU) も使用できます。その場合は、1 TU が 1024 マイクロ秒、または 100 TU が 102.4 ミリ秒になります。ビーコン間隔がコントローラ内で 100 ミリ秒として示されている場合、これは単に 102.4 ミリ秒を丸めた値です。一部の無線におけるハードウェアの制限により、ビーコン間隔がたとえば 100 TU であっても、その間隔は 102 TU に調整されます。これは、約 104.448 ミリ秒になります。ビーコン周期が TU で表現される場合、その値は、最も近い 17 の倍数に調整されます。
- ステップ 5** 256 ~ 2346 バイトの範囲内の値を [Fragmentation Threshold] テキストボックスに入力して、パケットをフラグメントするサイズを指定します。接続不良や多くの無線干渉が発生している領域では、この値を小さくします。
- ステップ 6** アクセスポイントが自身のチャネルと送信電力レベルを、CCX クライアントのビーコンおよびプローブ応答でアドバタイズするようにします。[DTPC Support] チェックボックスをオンにします。有効にしない場合には、このチェックボックスをオフにします。デフォルト値はイネーブルです。
- Dynamic Transmit Power Control (DTPC; 送信電力の動的制御) を使用するクライアントデバイスは、アクセスポイントからチャネルおよび電力レベル情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアントデバイスをイタリアに移送し、そのネットワークに join した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。
- (注) シスコ IOS ソフトウェアを実行しているアクセスポイントでは、この機能はワールドモードと呼ばれます。
- (注) DTPC と 801.11h 電力制約を同時に有効にすることはできません。
- ステップ 7** 1 ~ 200 の範囲内の値を [Maximum Allowed Client] テキストボックスに入力して、最大許容クライアント数を指定します。デフォルト値は 200 です。
- ステップ 8** [RSSI Low Check] チェックボックスをオンまたはオフにして、RSSI Low Check 機能を有効または無効にします。
- サービスプロバイダーは RSSI Low Check 機能を使用して、クライアントが有効な接続を持たない場合に Wi-Fi ネットワークへの接続ができないようにすることができます。多くの場合、クライアントがビーコンを受信して Wi-Fi に接続できたとしても、信号の強度が不十分で安定した接続をサポートできないことが

あります。この機能を使用して、Wi-Fi ネットワークにアソシエートするためにどの程度の信号強度でクライアントを受信する必要があるかを指定することができます。

RSSI Low Check 機能を有効にした場合、クライアントがアソシエーション要求を AP に送信したときにコントローラは RSSI 値をアソシエーションメッセージから取得し、設定されている RSSI しきい値と比較します。アソシエーションメッセージの RSSI 値が RSSI しきい値より小さい場合は、コントローラはそのアソシエーション要求を拒否します。

デフォルトの RSSI Low Check 値は -80 dBm です。つまり、AP が -80 dBm より弱い信号を持つクライアントを受信した場合に、そのクライアントからのアソシエーション要求が拒否される可能性があります。この値を -90 dBm に下げると、クライアントはより離れた場所から接続できますが、同時に接続品質が低下する可能性も高くなります。値を -80 dBm より大きく (-70 dBm など) しないことを推奨します。-80 dBm より大きくすると、セルサイズが大幅に縮小するためです。

ステップ 9 [RSSI Threshold] の値を入力します。

デフォルト値は -80 dBm です。

ステップ 10 アクセスポイントとクライアントとの間のデータ送信レートを指定するには、[Data Rates] のオプションを使用します。次のデータ レートが使用可能です。

- 802.11a : 6、9、12、18、24、36、48、および 54Mbps
- [802.11b/g] : 1、2、5.5、6、9、11、12、18、24、36、48、または 54Mbps

各データ レートに対して、次のオプションのいずれかを選択します。

- [Mandatory] : クライアントは、このコントローラ上のアクセスポイントにアソシエートするにはこのデータ レートをサポートしている必要があります。
- [Supported] : アソシエートしたクライアントは、このデータレートをサポートしていれば、このレートを使用してアクセスポイントと通信することができます。ただし、クライアントがこのレートを使用できなくても、アソシエートは可能です。
- [Disabled] : 通信に使用するデータ レートは、クライアントが指定します。

ステップ 11 [Apply] をクリックします。

ステップ 12 [Save Configuration] をクリックします。

802.11 帯域の設定 (CLI)

ステップ 1 次のコマンドを入力して、802.11a 帯域を無効にします。

config 802.11a disable network

- (注) 802.11a 帯域を無効にしてから、この項の 802.11a ネットワーク パラメータを設定してください。

ステップ 2 次のコマンドを入力して、802.11b/g 帯域を無効にします。

config 802.11b disable network

(注) 802.11b 帯域を無効にしてから、この項の 802.11b ネットワーク パラメータを設定してください。

ステップ 3 次のコマンドを入力して、アクセス ポイントが SSID のブロードキャストを行うレートを指定します。

config {802.11a | 802.11b} beaconperiod time_unit

time_unit は、単位時間 (TU) でのビーコン間隔です。1 TU は 1024 マイクロ秒です。20 ~ 1000 ミリ秒ごとにビーコンを送信するように、アクセス ポイントを設定できます。

ステップ 4 次のコマンドを入力して、パケットをフラグメントするサイズを指定します。

config {802.11a | 802.11b} fragmentation threshold

threshold の値は、256 ~ 2346 バイト (両端の値を含む) です。接続不良や多くの無線干渉が発生している領域では、この値を小さくします。

ステップ 5 次のコマンドを入力して、アクセス ポイントが自身のチャネルと送信電力レベルをビーコンおよびプローブ応答でアダプタイズするようにします。

config {802.11a | 802.11b} dtpc {enable | disable}

デフォルト値はイネーブルです。Dynamic Transmit Power Control (DTPC; 送信電力の動的制御) を使用するクライアント デバイスは、アクセス ポイントからチャネルおよび電力レベル情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアント デバイスをイタリアに移送し、そのネットワークに join した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。

(注) シスコ IOS ソフトウェアを実行しているアクセス ポイントでは、この機能はワールドモードと呼ばれます。

ステップ 6 次のコマンドを入力して、設定可能な最大許容クライアント数を指定します。

config {802.11a | 802.11b} max-clients max_allow_clients

有効な範囲は 1 ~ 200 です。

ステップ 7 次のコマンドを入力して、RSSI Low Check 機能を設定します。

config 802.11{a | b} rssi-check {enable | disable}

ステップ 8 次のコマンドを入力して、RSSI しきい値を設定します。

config 802.11{a | b} rssi-threshold value-in-dBm

(注) デフォルト値は -80 dBm です。

ステップ 9 次のコマンドを入力して、コントローラとクライアントとの間のデータ送信レートを指定します。

config {802.11a | 802.11b} rate {disabled | mandatory | supported} rate

値は次のとおりです。

- **disabled** : 通信に使用するデータ レートをクライアントが指定します。
- **mandatory** : コントローラ上のアクセス ポイントにアソシエートするために、クライアントがこのデータ レートをサポートします。

- **supported** : アソシエートしたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信することができます。ただし、クライアントがこのレートを
使用できなくても、アソシエートは可能です。
- **rate** : データが送信されるときのレートです。
 - 6、9、12、18、24、36、48、および 54Mbps (802.11a)
 - 1、2、5.5、6、9、11、12、18、24、36、48、または 54Mbps (802.11b/g)

ステップ 10 次のコマンドを入力して、802.11a 帯域を有効にします。

config 802.11a enable network

デフォルト値はイネーブルです。

ステップ 11 次のコマンドを入力して、802.11b 帯域を有効にします。

config 802.11b enable network

デフォルト値はイネーブルです。

ステップ 12 次のコマンドを入力して、802.11g ネットワーク サポートを有効または無効にします。

config 802.11g 11gSupport {enable | disable}

デフォルト値はイネーブルです。このコマンドは、802.11b 帯域が有効になっている場合のみ使用できます。この機能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。

ステップ 13 **save config** コマンドを入力して、変更を保存します。

ステップ 14 次のコマンドを入力して、802.11a または 802.11b/g 帯域の設定を表示します。

show {802.11a | 802.11b}

以下に類似した情報が表示されます。

```
802.11a Network..... Enabled
11nSupport..... Enabled
    802.11a Low Band..... Enabled
    802.11a Mid Band..... Enabled
    802.11a High Band..... Enabled
802.11a Operational Rates
    802.11a 6M Rate..... Mandatory
    802.11a 9M Rate..... Supported
    802.11a 12M Rate..... Mandatory
    802.11a 18M Rate..... Supported
    802.11a 24M Rate..... Mandatory
    802.11a 36M Rate..... Supported
    802.11a 48M Rate..... Supported
    802.11a 54M Rate..... Supported
...
Beacon Interval..... 100
...
Default Channel..... 36
Default Tx Power Level..... 1
DTPC Status..... Enabled
```

Fragmentation Threshold..... 2346
Maximum Number of Clients per AP..... 200

帯域選択の設定

帯域選択の設定について

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、混雑の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャンネル干渉も発生します。802.11b/g では、重複しないチャンネルが 3 つしかないからです。これらの干渉の原因を防止して、ネットワーク全体のパフォーマンスを向上させるには、コントローラで帯域選択を設定できます。

帯域選択は、デフォルトではグローバルで有効になっています。

帯域選択のしくみは、クライアントへのプローブ応答を規制するというものです。5 GHz チャンネルへクライアントを誘導するために、2.4 GHz チャンネルでのクライアントへのプローブ応答を遅らせます。

帯域選択の制約事項

- 帯域選択が有効になっている WLAN では、ローミングの遅延が発生するので、音声やビデオのような、遅延に敏感なアプリケーションはサポートされません。
- 帯域選択は、Cisco Aironet 1040、1140、1250、1260、3500、および 3600 シリーズ アクセス ポイントでのみ使用できます。



(注) OEAP 600 シリーズ アクセス ポイントは、帯域選択をサポートしません。

- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。

- コントローラ GUI または コントローラ CLI を使用して、帯域選択とクライアントロードバランシングをグローバルで有効または無効にすることはできません。ただし、特定の WLAN の帯域選択とクライアントロードバランシングを有効または無効にできます。帯域選択とクライアントロードバランシングは、デフォルトではグローバルで有効になっています。

帯域選択の設定

帯域選択の設定 (GUI)

-
- ステップ 1** [Wireless] > [Advanced] > [Band Select] の順に選択して、[Band Select] ページを開きます。
 - ステップ 2** [Probe Cycle Count] テキストボックスに、1～10の値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は2です。
 - ステップ 3** [Scan Cycle Period Threshold (milliseconds)] テキストボックスに、スキャンサイクル期間しきい値を1～1000ミリ秒の値で入力します。この設定は、クライアントからの新しいプローブ要求が新しいスキャンサイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は200ミリ秒です。
 - ステップ 4** [Age Out Suppression (seconds)] テキストボックスに、10～200秒の値を入力します。エージングアウト抑制は、以前に認識されていた802.11b/g/nクライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は20秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
 - ステップ 5** [Age Out Dual Band (seconds)] テキストボックスに、10～300秒の値を入力します。エージングアウト期間は、以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は60秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
 - ステップ 6** [Acceptable Client RSSI (dBm)] テキストボックスに、-20～-90 dBmの値を入力します。このパラメータにより、クライアントがプローブに응答するための最小RSSIが設定されます。デフォルト値は-80 dBmです。
 - ステップ 7** [Apply] をクリックします。
 - ステップ 8** [Save Configuration] をクリックします。
 - ステップ 9** 特定の WLAN 上で帯域選択を有効または無効にするには、[WLANs] > [WLAN ID] の順に選択します。[WLANs > Edit] ページが表示されます。
 - ステップ 10** [Advanced] タブをクリックします。
 - ステップ 11** 帯域選択を有効にする場合は、[Load Balancing and Band Select] テキスト領域で [Client Band Select] チェックボックスをオンにします。帯域選択を無効にするには、チェックボックスをオフにしておいてください。デフォルト値はディセーブルです。
 - ステップ 12** [Save Configuration] をクリックします。
-

帯域選択の設定 (CLI)

ステップ 1 次のコマンドを入力して、帯域選択用のプローブ サイクル回数を設定します。

config band-select cycle-count *cycle_count*

cycle_count パラメータには、1 ~ 10 の範囲内の値を入力できます。

ステップ 2 次のコマンドを入力して、新しいスキャン サイクル期間用の時間しきい値を設定します。

config band-select cycle-threshold *milliseconds*

milliseconds パラメータには、しきい値として 1 ~ 1000 の範囲内の値を入力できます。

ステップ 3 次のコマンドを入力して、帯域選択の失効抑制期間を設定します。

config band-select expire suppression *seconds*

seconds パラメータには、抑制期間として 10 ~ 200 の範囲内の値を入力できます。

ステップ 4 次のコマンドを入力して、デュアルバンドの失効を設定します。

config band-select expire dual-band *seconds*

seconds パラメータには、デュアルバンド用に 10 ~ 300 の範囲内の値を入力できます。

ステップ 5 次のコマンドを入力して、クライアント RSSI しきい値を設定します。

config band-select client-rssi *client_rssi*

client_rssi パラメータには、プローブに応答するクライアント RSSI の最小 dBm として 20 ~ 90 の範囲内の値を入力できます。

ステップ 6 **save config** コマンドを入力して、変更を保存します。

ステップ 7 次のコマンドを入力して、特定の WLAN 上の帯域選択を有効または無効にします。

config wlan band-select allow {**enable** | **disable**} *wlan_ID*

wlan_ID パラメータには、1 ~ 512 の範囲内の値を入力できます。

ステップ 8 次のコマンドを入力して、設定を確認します。

show band-select

以下に類似した情報が表示されます。

```
Band Select Probe Response..... Enabled
  Cycle Count..... 3 cycles
  Cycle Threshold..... 300 milliseconds
  Age Out Suppression..... 20 seconds
  Age Out Dual Band..... 20 seconds
  Client RSSI..... -30 dBm
```

ステップ 9 **save config** コマンドを入力して、変更を保存します。



第 5 章

802.11 パラメータの設定

- [802.11n パラメータの設定, 87 ページ](#)
- [802.11h のパラメータの設定, 91 ページ](#)
- [802.11ac パラメータの設定, 93 ページ](#)

802.11n パラメータの設定

802.11n パラメータの設定について

この項では、ネットワーク上の 802.11n デバイス（Cisco Aironet 1140 および 3600 シリーズ アクセスポイントなど）を管理する手順を説明します。802.11n デバイスでは、2.4GHz 帯域と 5GHz 帯域をサポートしており、高スループットデータ レートを提供します。

802.11n の高スループットデータ レートは、すべての 802.11n アクセスポイントで使用できます。この場合、WLAN で WMM が使用されていることと、レイヤ 2 暗号化なしであるか WPA2/AES 暗号化が有効化されていることが必要です。

リリース 7.4 より、802.11n 専用アクセス ポイントは、アソシエーション要求に関する高スループットの情報要素がないクライアントを除外できます。802.11n 専用アクセス ポイントは、高スループットの情報要素（11n）がないクライアントからのアソシエーション要求を拒否します。

802.11n 高スループット モードでは、同じチャネルを使用する 802.11a/b/g ステーションがありません。802.11a/b/g デバイスは 802.11n 高スループット モードのアクセス ポイントと通信できません。一方 802.11n 専用アクセス ポイントはビーコンまたは管理フレーム用に 802.11a/g レートを使用します。



(注) Cisco 802.11n AP は、偽の wIPS アラームをトリガーする可能性がある誤ったビーコンフレームを断続的に送信する場合があります。これらのアラームを無視することをお勧めします。この問題は Cisco 802.11n AP の 1140、1250、2600、3500、および 3600 で確認されています。

802.11n パラメータの設定 (GUI)

- ステップ 1** [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [High Throughput] を選択して、(5 GHz または 2.4 GHz) の [High Throughput] ページを開きます。
- ステップ 2** [11n Mode] チェックボックスをオンにして、ネットワーク上での 802.11n サポートを有効にします。デフォルト値はイネーブルです。
802.11n と 802.11ac の両方のモードが有効になっているときに 802.11n モードを無効にする場合は、最初に 802.11ac モードを無効にします。
- ステップ 3** 必要なレートのチェックボックスをオンにして、アクセスポイントとクライアントの間のデータ送信に使用可能な変調および符号化方式 (MCS) レートを指定します。使用できるデータ レートは次のとおりです。これらは、チャンネル幅 20MHz、ガードインターバル「short」の場合の計算値です。

- 0 (7 Mbps)
- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)

選択したレートをクライアントがサポートしていれば、アソシエートしたクライアントはそのレートを使用してアクセスポイントと通信することができます。ただし、クライアントがこのレートを使用できなくても、アソシエートは可能です。MCS 設定では、使用する空間ストリーム数、変調、符号化レート、およびデータ レートの値を定めます。

ステップ 4 [Apply] をクリックします。

ステップ 5 次の手順に従って、WLAN 上で WMM を有効にすることにより、設定した 802.11n データ レートを使用します。

- a) [WLANs] を選択して、[WLANs] ページを開きます。
- b) WMM モードを設定する WLAN の ID 番号をクリックします。
- c) [WLANs] > [Edit] ページが表示されたら、[QoS] タブを選択して [WLANs > Edit (QoS)] ページを開きます。
- d) クライアント デバイスに WMM の使用を要求するには [WMM Policy] ドロップダウン リストから [Required] を選択し、使用を許可するには [Allowed] を選択します。WMM をサポートしていないデバイスは WLAN に join できません。
[Allowed] を選択した場合は、WMM をサポートしていないデバイスが WLAN に join できますが、802.11n レートによるメリットはありません。
- e) [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

(注) アクセス ポイントが 802.11n をサポートしているかどうかを判断するには、[802.11a/n/ac (または 802.11b/g/n) Cisco APs > Configure] ページまたは [802.11a/n/ac (または 802.11b/g/n) AP Interfaces > Details] ページの [11n Supported] テキスト ボックスを確認します。

802.11n パラメータの設定 (CLI)

- 次のコマンドを入力して、ネットワーク上での 802.11n サポートを有効にします。
config {802.11a | 802.11b} 11nsupport {enable | disable}
- 次のコマンドを入力して、アクセス ポイントとクライアントの間のデータ送信に使用可能な変調および符号化方式 (MCS) レートを指定します。
config {802.11a | 802.11b} 11nsupport mcs tx {0-15} {enable | disable}
- 次の手順に従って、WLAN 上で WMM を有効にすることにより、設定した 802.11n データ レートを使用します。
config wlan wmm {allow | disable | require} wlan_id
require パラメータは、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に join できません。
allow に設定した場合は、WMM をサポートしていないデバイスが WLAN に join できますが、802.11n レートによるメリットはありません。
- 次の手順に従って、802.11n パケットに使用される集約方法を指定します。
 - a) 次のコマンドを入力して、ネットワークを無効にします。
config {802.11a | 802.11b} disable network
 - b) 次のコマンドを入力して、集約方法を指定します。
config {802.11a | 802.11b} 11nsupport {a-mpdu | a-msdu} tx priority {0-7 | all} {enable | disable}

集約は、パケットデータフレームを個別に伝送するのではなく、グループにまとめるプロセスです。集約の方法には、Aggregated MAC Protocol Data Unit (A-MPDU; 集約 MAC プロトコルデータユニット) と Aggregated MAC Service Data Unit (A-MSDU; 集約 MAC サービスデータユニット) の 2 つがあります。A-MSDU はハードウェアで実行されるため、デフォルトの方法になります。



(注) 802.11ac の場合、すべてのパケットが A-MPDU です。A-MSDU オプションは 802.11ac には適用されません。

集約方法は、アクセスポイントからクライアントへのトラフィックのタイプごとに指定できます。次の表に、トラフィックタイプごとに割り当てられている優先レベル (0 ~ 7) を示します。

表 3: トラフィックタイプの優先レベル

ユーザ優先度	トラフィックタイプ
0	ベストエフォート
1	バックグラウンド
2	予備
3	エクセレントエフォート
4	制御された負荷
5	ビデオ、遅延およびジッタは 100 ミリ秒未満
6	音声、遅延およびジッタは 10 ミリ秒未満
7	ネットワーク制御

各優先レベルを個別に設定するか、**all** パラメータを使用して一度にすべての優先レベルを設定できます。**enable** コマンドを使用する場合は、その優先レベルにアソシエートされたトラフィックでは A-MPDU 送信が使用されます。**disable** コマンドを使用する場合は、その優先レベルにアソシエートされたトラフィックでは A-MSDU 送信が使用されません。クライアントが使用する集約方法に合わせて優先度を設定します。デフォルトでは、A-MPDU は、優先レベル 0、4、および 5 に対して有効になっており、それ以外は無効になっています。デフォルトでは、A-MSDU は、6 と 7 以外のすべての優先度に対して有効になっています。

- c) 次のコマンドを入力して、ネットワークを再び有効にします。
config {802.11a | 802.11b} enable network

- 次のコマンドを入力して、802.11n の 5 GHz の A-MPDU 送信集約スケジューラを設定します。
config 802.11 {a | b} 11nsupport a-mpdu tx scheduler {enable | disable | timeout rt timeout-value}
タイムアウト値はミリ秒単位です。有効範囲は 1 ~ 1000 ミリ秒です。
- 次のコマンドを入力して、ネットワークのガードインターバルを設定します。
config 802.11 {a | b} 11nsupport guard_interval {any | long}
- 次のコマンドを入力して、ネットワークの Reduced Interframe Space (RIFS) を設定します。
config 802.11 {a | b} 11nsupport rifs rx {enable | disable}
- 次のコマンドを入力して、変更を保存します。
save config
- 次のコマンドを入力して、802.11 ネットワークの設定を表示します。
show {802.11a | 802.11b}

802.11h のパラメータの設定

802.11h パラメータの設定について

802.11h では、チャンネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。

802.11h のパラメータの設定 (GUI)

-
- ステップ 1** 次の手順で、802.11 帯域を無効にします。
- a) [Wireless] > [802.11a/n]/ac > [Network] の順に選択して、[802.11a Global Parameters] ページを開きます。
 - b) [802.11a Network Status] チェックボックスをオフにします。
 - c) [Apply] をクリックします。
- ステップ 2** [Wireless] > [802.11a/n]/ac > [DFS (802.11h)] を選択して、[802.11h Global Parameters] ページを開きます。
- ステップ 3** [Power Constraint] 領域で、ローカル電力制約を入力します。有効な範囲は 0 dBm ~ 30 dBm です。
- ステップ 4** アクセスポイントが新しいチャンネルに切り替えたときに新しいチャンネル番号がアナウンスされるようになる場合は、[Channel Switch Announcement] 領域で、[Channel Announcement] チェックボックスをオンにします。チャンネルアナウンスを無効にする場合は、このチェックボックスをオフにします。デフォルト値はディセーブルです。
- ステップ 5** チャンネルアナウンスを有効にした場合は、[Channel Quiet Mode] チェックボックスが表示されます。現在のチャンネルでのアクセスポイントからの送信を停止する (クワイエットモード) には、このチェックボッ

クスをオンにします。クワイエットモードを無効にするには、オフにします。デフォルト値はディセーブルです。

ステップ 6 [Apply] をクリックします。

ステップ 7 次の手順に従って、802.11a 帯域を有効にします。

- a) [Wireless] > [802.11a/n/ac] > [Network] の順に選択して、[802.11a Global Parameters] ページを開きます。
- b) [802.11a Network Status] チェックボックスをオンにします。
- c) [Apply] をクリックします。

ステップ 8 [Save Configuration] をクリックします。

802.11h のパラメータの設定 (CLI)

ステップ 1 次のコマンドを入力して、802.11a ネットワークを無効にします。

config 802.11a disable network

ステップ 2 次のコマンドを入力して、アクセスポイントが新しいチャンネルに切り替えたときの新しいチャンネル番号のアナウンスを有効または無効にします。

config 802.11h channelswitch {enable {loud | quiet} | disable}

enable パラメータに **quiet** または **loud** を入力します。待機モードが有効になっている場合、802.11h チャンネル切り替えアナウンスを有効にできるすべてのクライアントは、パケット送信をただちに停止する必要があります。これは、干渉を減らすためにレーダーおよびクライアントデバイスも送信を終了する必要があることが AP によって検出されるためです。デフォルトでは、チャンネル切り替え機能は無効の状態です。

ステップ 3 次のコマンドを入力して、802.11h チャンネルアナウンスを使用する新しいチャンネルを設定します。

config 802.11h setchannel channel channel

ステップ 4 次のコマンドを入力して、802.11h 電力制約値を設定します。

config 802.11h powerconstraint value

AP の電力レベルが一度に 1 だけ低下するように、3 dB 単位の値を使用します。

ステップ 5 次のコマンドを入力して、802.11a ネットワークを有効にします。

config 802.11a enable network

ステップ 6 次のコマンドを入力して、802.11h パラメータのステータスを表示します。

show 802.11h

以下に類似した情報が表示されます。

```
Power Constraint..... 0
Channel Switch..... Disabled
Channel Switch Mode..... 0
```

802.11ac パラメータの設定

802.11ac パラメータの設定に関する情報

Cisco Aironet 3600 シリーズ アクセス ポイントの 802.11ac 無線モジュールは、エンタープライズクラスの信頼性と有線ネットワーク同様のパフォーマンスを提供します。最大データ レート 1.3 Gbps に対応する 3 つの空間ストリームと 80 MHz 広帯域チャネルをサポートします。これは、現在のハイエンドのエンタープライズ 802.11n アクセス ポイントの最大データ レートの 3 倍です。

スロット 2 の 802.11ac 無線は、特定のパラメータを設定できるスレーブ無線です。802.11ac はスレーブ無線であるため、スロット 1 の 802.11a/n メイン無線から多数のプロパティを継承します。802.11ac 無線に設定できるパラメータは次のとおりです。

- **Admin status** : 有効または無効にできる無線のインターフェイス ステータス。デフォルトでは、[Admin status] は有効になっています。802.11n を無効にすると、802.11ac 無線も無効になります。
- **Channel width** : 20 MHz、40 MHz、80 MHz として RF のチャネル幅を選択できます。80 MHz としてチャネル幅を選択する場合、[High Throughput] ページで 802.11ac モードを有効にする必要があります。



(注) スロット 2 の 802.11ac スレーブ無線で表示される [11ac Supported] フィールドのパラメータは設定できません。

この項では、ネットワーク上の 802.11ac デバイス (Cisco Aironet 3600 シリーズ アクセス ポイントなど) を管理する手順を説明します。



(注) 802.11ac モジュールを備えた AP3600 は 5 GHz 無線の最初の 8 つの WLAN のみをアドバタイズできます。

802.11n 無線チャネルを変更すると、802.11ac チャネルも変更されます。

Cisco WLC GUI で、802.11n 無線に接続された 802.11ac クライアントは 802.11an クライアントと表示され、802.11ac 無線に接続された 802.11ac クライアントは 802.11ac クライアントと表示されます。

WLAN で WMM が有効であり機能している、または 802.11ac の WPA2/AES がサポートされていることを確認します。そうではない場合、802.11ac クライアントであっても 802.11ac の速度を得られません。

Cisco Aironet 3600 シリーズ アクセス ポイントの 802.11ac モジュールの詳細については、http://www.cisco.com/en/US/products/ps11983/products_relevant_interfaces_and_modules.htmlを参照してください。

802.11ac サポートの制約事項

- 802.11ac モジュールは、Cisco Aironet 3600 シリーズ アクセス ポイントでのみサポートされています。
- 組み込みの 5 GHz 無線がオフになると、802.11ac モジュールもオフになります。
- 802.11ac モジュールのチャンネル、電力値およびモードの設定は、AP の組み込み 5 GHz 無線と同じにする必要があります。また、802.11ac モジュールは 802.11ac クライアントとしてのみ機能します。
- 802.11ac モジュールのメイン チャンネルは個別に変更できません。
- この 802.11ac サポートは、次のコントローラ プラットフォームにだけ適用されます。
 - Cisco 2500 シリーズ Wireless LAN Controller
 - Cisco 5500 シリーズ Wireless LAN Controller
 - Cisco Flex 7500 シリーズ ワイヤレス LAN コントローラ
 - Cisco 8500 シリーズ ワイヤレス LAN コントローラ
- コントローラは 802.11ac モジュールのハイ アベイラビリティをサポートしていません。コントローラの 802.11ac 設定 (802.11ac データ レートと 802.11ac グローバル モード) はスタンバイ コントローラと同期されません。これにより、アクティブ コントローラでこれらの設定を明示的に無効にした場合に、クライアントのスループット変動および再アソシエーションが発生することがあります。

さらに 802.11ac グローバルモード設定により、無線モジュールが有効かどうかはコントローラされます。802.11ac グローバルモードが 1 台のコントローラ上のみで有効にされている場合、アクセス ポイントが 802.11ac グローバルモードが無効になっているコントローラとアソシエートすると、802.11ac モジュールは無効になる可能性があります。
- AP をスタティックから自動チャンネル割り当てに変更すると、デフォルトによって AP は無線と有効なチャンネルによってサポートされる最適な帯域幅に移動します。チャンネル番号と帯域幅の割り当ては、次の DCA サイクルが開始されるまで最適ではない場合があります。

802.11ac 高スループット パラメータの設定 (GUI)

ステップ 1 [Wireless] > [802.11a/n/ac] > [High Throughput (802.11n/ac)] を選択します。

ステップ 2 [11ac mode] チェックボックスをオンにして、ネットワーク上での 802.11ac サポートを有効にします。

(注) 802.11n モードが有効な場合にのみ 802.11ac ステータスを変更できません。

ステップ 3 必要なレートをチェックボックスをオンにして、アクセスポイントとクライアントの間のデータ送信に使用可能な変調および符号化方式 (MCS) レートを指定します。

MCS インデックス 8 および 9 は 802.11ac に固有です。インデックス 9 の MCS データ レートを有効にすると、自動的に MCS インデックス 8 のデータ レートが有効になります。MCS インデックス 9 が無効の場合にのみ、MCS インデックス 8 を有効または無効にできます。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

802.11ac 高スループット パラメータの設定 (CLI)

- 次のコマンドを入力して、802.11ac サポートを有効または無効にします。
config 802.11a 11acSupport {enable | disable}
- 次のコマンドを入力して、MCS 送信速度を設定します。
config 802.11a 11acSupport mcs tx {rate-8 | rate-9} ss spatial-stream-value {enable | disable}



(注) MCS インデックス 9 を持つ MCS データを有効にすると、MCS インデックス 8 を持つデータ レートが自動的に有効になります。



第 6 章

DHCP プロキシの設定

- DHCP プロキシの設定について, 97 ページ
- DHCP プロキシの使用に関する制限, 98 ページ
- DHCP プロキシの設定 (GUI), 98 ページ
- DHCP プロキシの設定 (CLI), 99 ページ
- DHCP タイムアウトの設定 (GUI), 100 ページ
- DHCP タイムアウトの設定 (CLI), 100 ページ

DHCP プロキシの設定について

DHCP プロキシがコントローラ上で有効になっている場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。少なくとも 1 つの DHCP サーバが、WLAN にアソシエートされたインターフェイスか WLAN 自体で設定されている必要があります。

DHCP プロキシがコントローラ上で無効になっている場合は、クライアントとの間で送受信されるそれらの DHCP パケットは、パケットの IP 部分に変更されることなくコントローラによってブリッジされます。クライアントから受信したパケットは CAPWAP トンネルから削除され、アップストリーム VLAN 上で送信されます。クライアント宛の DHCP パケットは、アップストリーム VLAN 上で受信され、802.11 に変換されて、CAPWAP トンネルを通過してクライアントに送信されます。したがって、DHCP プロキシが無効になっている場合は、内部 DHCP サーバは使用できません。DHCP プロキシを無効にする機能を利用すると、シスコのネイティブプロキシ動作モードをサポートしない DHCP サーバを使用できるようになります。既存のインフラストラクチャによって必要とされる場合のみ、無効にするようにしてください。



(注) DHCP プロキシは、デフォルトで有効になっています。

DHCP プロキシの使用に関する制限

- DHCP オプション 82 を正しく動作させるには、DHCP プロキシが有効になっている必要があります。
- 通信するすべてのコントローラの DHCP プロキシ設定は同じでなければなりません。

DHCP プロキシの設定 (GUI)

-
- ステップ 1 [Controller] > [Advanced] > [DHCP] の順に選択して、[DHCP Parameters] ページを開きます。
- ステップ 2 [Enable DHCP Proxy] チェックボックスをオンにして、DHCP プロキシをグローバルで有効にします。それ以外の場合は、このチェックボックスをオフにします。デフォルト値はオンです。
- ステップ 3 [Apply] をクリックして、変更を確定します。
- ステップ 4 [Save Configuration] をクリックして、変更を保存します。
-

DHCP プロキシの設定 (GUI)

-
- ステップ 1 [Controller] > [Interfaces] の順に選択します。
- ステップ 2 DHCP プロキシを設定するインターフェイスを選択します。
 コントローラの管理、仮想、AP マネージャ、または動的インターフェイスに DHCP プロキシを設定できます。
 [Interfaces > Edit] ページに、コントローラ上で設定されているプライマリおよびセカンダリ DHCP サーバの DHCP 情報が表示されます。プライマリおよびセカンダリ サーバが表示されない場合は、このウィンドウに表示されるテキストボックスに DHCP サーバの IP アドレスの値を入力する必要があります。
- ステップ 3 選択した管理インターフェイスの DHCP プロキシを有効にするには、プロキシモードドロップダウンで次のオプションから選択します。[Global] : コントローラでグローバル DHCP プロキシモードを使用します。[Enabled] : インターフェイスで DHCP プロキシモードを有効にします。コントローラ上で DHCP プロキシを有効にした場合は、コントローラによってクライアントから設定済みサーバへ DHCP 要求がユニキャストされます。WLAN に関連付けられたインターフェイスまたは WLAN のいずれかに少なくとも 1 台の DHCP サーバを設定する必要があります。[Disabled] : インターフェイスで DHCP プロキシモードを無効にします。コントローラ上で DHCP プロキシを無効にすると、クライアントとの間で送受信される DHCP パケットは、パケットの IP 部分に変更されることなくコントローラによってブリッジされます。クライアントから受信したパケットは CAPWAP トンネルから削除され、アップストリーム VLAN 上で送信されます。クライアント宛の DHCP パケットは、アップストリーム VLAN 上で受信され、802.11 に変

換されて、CAPWAP トンネルを通してクライアントに送信されます。したがって、DHCP プロキシが無効になっている場合は、内部 DHCP サーバは使用できません。

- ステップ 4** ネットワーク アドレスの割り当てに DHCP が使用されている場合、[Enable DHCP option 82] チェックボックスをオンにして、追加のセキュリティを確保します。
- ステップ 5** [Apply] をクリックして、設定を保存します

DHCP プロキシの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、DHCP プロキシを有効または無効にします。
config dhcp proxy {enable | disable}

- ステップ 2** 次のコマンドを入力して、DHCP プロキシの設定を表示します。
show dhcp proxy

以下に類似した情報が表示されます。

```
DHCP Proxy Behavior: enabled
```

DHCP プロキシの設定 (CLI)

- ステップ 1** インターフェイスで DHCP のプライマリおよびセカンダリ サーバを設定します。これを設定するには、次のコマンドを入力します。

- **config interface dhcp management primary primary-server**
- **config interface dhcp dynamic-interface interface-name primary primary-s**

- ステップ 2** コントローラの管理または動的インターフェイスで DHCP プロキシを設定します。これを設定するには、次のコマンドを入力します。

- **config interface dhcp management proxy-mode enableglobaldisable**
- **config interface dhcp dynamic-interface interface-name proxy-mode enableglobaldisable.**

(注) DHCP が設定されている場合に追加のセキュリティを確保するには、**config interface dhcp interface typeoption-82 enable** コマンドを使用します。

- ステップ 3** **save config** コマンドを入力します。

- ステップ 4** コントローラインターフェイスのプロキシ設定を表示するには、**show dhcp proxy** コマンドを入力します。

DHCP タイムアウトの設定 (GUI)

-
- ステップ 1 [Controller] > [Advanced] > [DHCP] の順に選択して、[DHCP Parameters] ページを開きます。
- ステップ 2 [DHCP Timeout (5 - 120 seconds)] チェックボックスをオンにして、DHCP タイムアウトをグローバルで有効にします。それ以外の場合は、このチェックボックスをオフにします。有効な範囲は 5 ~ 120 秒です。
- ステップ 3 [Apply] をクリックして、変更を確定します。
- ステップ 4 [Save Configuration] をクリックして、変更を保存します。
-

DHCP タイムアウトの設定 (CLI)

DHCP タイムアウトを設定するには、次のコマンドを入力します。

```
config dhcp timeout seconds
```



第 7 章

[DHCP Link Select] および [VPN Select] の設定

- [\[DHCP Link Select\] および \[VPN Select\] の設定の前提条件](#), 101 ページ
- [\[DHCP Link Select\] と \[VPN Select\] の設定について](#), 101 ページ
- [\[DHCP Link Select\] および \[VPN Select\] の設定 \(CLI\)](#), 103 ページ
- [\[DHCP Link Select\] および \[VPN Select\] の設定 \(GUI\)](#), 104 ページ

[DHCP Link Select] および [VPN Select] の設定の前提条件

- DHCP モードは proxy に設定する必要があります。
- DHCP の外部サーバを設定する必要があります。
- DHCP Option 82 は、コントローラ上で有効にしておく必要があります。
- 設定中のインターフェイスは、サービスまたは仮想のタイプにしてはいけません。
- リレーソースのインターフェイス名は、IPアドレスが設定された、有効なインターフェイスにする必要があります。



(注) プロキシモードは IPv6 ではサポートされません。

[DHCP Link Select] と [VPN Select] の設定について

ワイヤレス環境で、クライアントが DHCP アドレスを要求する場合は、DHCP DISCOVER パケットの giaddr フィールドを使用して、IP アドレスを割り当てるサブネットを DHCP サーバに指定します。giaddr フィールドは、DHCP サーバが DHCP リレー エージェント (コントローラ) と通信するためのアドレスを指定するためにも使用できます。サブネットのコントローラ IP アドレスが DHCP サーバから到達可能かどうかを判断するのは困難です。そのため、コントローラ到達可能

アドレスとは異なるリンク選択情報を DHCP サーバに送信する必要があります。コントローラインターフェイス上に設定された DHCP Link Select (DHCP オプション 82、サブオプション 5) を使用して、コントローラ到達可能アドレスとは異なるリンク選択情報が DHCP サーバに送信されません。

大規模ネットワークのワイヤレス環境では、DHCP サーバである Cisco Network Registrar (CNR) サーバに VPN ID または VRF 名に基づいて作成された複数のプールが割り当てられます。これらのプールを使用すれば、DHCP VPN Select オプション (DHCP オプション 82 とサブオプション 151) を通して、IP アドレスをクライアントに割り当てることができます。コントローラインターフェイス上で DHCP VPN Select (DHCP オプション 82 とサブオプション 151) が有効になっている場合は、コントローラが、クライアントに IP アドレスを割り当てるプールの VPN ID または VRF 名を送信します。DHCP VPN Select オプションを使用すれば、中央の DHCP サーバを共有して簡単に運用できるため、コスト削減につながります。

DHCP Link Select

コントローラの管理インターフェイスと動的インターフェイスの DHCP Link Select (DHCP オプション 82、サブオプション 5) を設定します。コントローラインターフェイスの DHCP Link Select を設定する前に、そのインターフェイスの DHCP プロキシと DHCP オプション 82 を有効にします。

コントローラインターフェイスで Link Select オプションが有効になると、対応するクライアントに適切なサブネットアドレスを含む IP アドレス情報と一緒にサブオプション 5 がパケットに追加されます。サブネットアドレスは、クライアント VLAN インターフェイスにマッピングされたコントローラインターフェイスアドレスです。DHCP サーバは、このサブネットアドレスを使用して、DHCP クライアントに IP アドレスを割り当てます。

DHCP VPN Select

コントローラの管理インターフェイスと動的インターフェイスの DHCP VPN Select (DHCP オプション 82、サブオプション 151) を設定します。コントローラインターフェイスの DHCP VPN Select を設定する前に、そのインターフェイスの DHCP プロキシと DHCP オプション 82 を有効にします。

同じコントローラ上で別の VPN ID または VRF 名を設定することも、コントローラインターフェイスに設定された VPN Select 機能を使用して別のコントローラを設定することもできます。VPN Select 機能を設定すると、アドレスが重複してしない DHCP サーバ VPN プールになります。

VSS サブオプション 151 が DHCP サーバに送信される度に、VSS Control サブオプション 152 を追加する必要があります。DHCP サーバが VSS サブオプション 151 を認識してそれに従って機能している場合は、DHCP 確認応答から VSS Control サブオプション 152 が除外されます。DHCP サーバが DHCP 確認応答で VSS Control サブオプション 152 をコピーバックした場合は、DHCP サーバに VSS サブオプションに対する必要なサポートがないことを意味します。

モビリティに関する考慮事項

同じサブネット内での

WLAN にマッピングする VPN ID または VRF 名は、モビリティ グループのすべてのコントローラで同じである必要があります。たとえば、WLC A 上で WLAN1 インターフェイスが VPN ID 1 にマップし、WLAN2 インターフェイスが VPN ID 2 にマップしている場合、WLC B も、WLAN1 インターフェイスが VPN ID 1 にマップしており、WLAN2 インターフェイスが VPN ID 2 にマップしているはずですが、このようにクライアント L2 が別の WLC へ移動すると、移動した WLC の DHCP 設定では、同じ VPN のアドレスがクライアントに必ず割り当てられます。

異なるサブネットのモビリティ

L3 モビリティでは、すべての DHCP DISCOVER パケットがアンカーに送信され、元の VPN の割り当てが保証されます。

自動アンカー モビリティ

すべての DHCP DISCOVER パケットがアンカーに送信され、元の VPN の割り当てが保証されます。

[DHCP Link Select] および [VPN Select] の設定 (CLI)

ステップ 1 次のコマンドを使用して、動的インターフェイスを設定します。

- **config interface dhcp dynamic-interface *interface-name* {option-82 |primary|proxy-mode}**

ステップ 2 次のコマンドを使用して、動的インターフェイスで DHCP オプション 82 を設定します。

- **config interface dhcp dynamic-interface *interface-name* option-82 {enable|disable |linksel |vpnsel}**

ステップ 3 次のコマンドを使用して、動的インターフェイスでリンク選択サブオプション 5 を設定します。

- **config interface dhcp dynamic-interface *interface-name* option-82linksel {enable |disable |relaysrc}**
- 動的インターフェイスでリンク選択を有効にするには、初めに **config interface dhcp dynamic-interface *interface-name* option-82 linksel relaysrc** コマンドを入力し、続いて **config interface dhcp dynamic-interface *interface-name* option-82 linksel enable** コマンドを入力する必要があります。

ステップ 4 次のコマンドを使用して、動的インターフェイスで VPN 選択サブオプション 151 を設定します。

- **config interface dhcp dynamic-interface *interface-name* option-82vpnsel {enable |disable |vrfname *vrf-name*|vpnid*vpn-id*}**
vpn-id の値は、*oui:vpn-ndex* 形式 *xxxxxx:xxxxxxxx* で表記します。

動的インターフェイスの VPN 選択では、VPN ID または VRF 名のどちらかを設定できます。VPN ID がすでに設定されている場合、VRF 名を設定しようとすると、以前の設定は VPN 選択が無効のときに削除されます。

VRF 名は 7 オクテットの文字列として表記します。

動的インターフェイスで VPN 選択を有効にするには、初めに **config interface dhcp dynamic-interface *interface-name* option-82 vpnsel *vpnid* *vpn-id*** コマンドまたは **config interface dhcp**

dynamic-interface*interface-name***option-82 vpsel vrfname vrfname** コマンドを入力し、続けて **config interface dhcp dynamic-interface***interface-name***option-82 vpsel enable** コマンドを入力する必要があります。

ステップ 5 次のコマンドを使用して、管理インターフェイスでリンク選択サブオプション 5 を設定します。

- **config interface dhcp management option-82 linkselect {enable|disable|relaysrc}***interface-name*
- 管理インターフェイスでリンク選択を有効にするには、**config interface dhcp management option-82 linkselect relaysrc** コマンドを入力し、続けて **config interface dhcp management option-82 linkselect enable** コマンドを入力します。

ステップ 6 次のコマンドを使用して、管理インターフェイスで VPN 選択サブオプション 151 を設定します。

- **config interface dhcp management option-82 vpnselect {enable|disable|vpnid***vpn-id***|vrfname vrf-name}**
VPN ID 値は、*oui:vpn-ndex* 形式 *xxxxxx:xxxxxxxx* で表記します。

管理インターフェイスの VPN 選択では、VPN ID または VRF 名のどちらかを設定できます。VPN ID がすでに設定されている場合、VRF 名を設定しようとする、以前の設定は VPN 選択が無効のときに削除されます。

VRF 名は 7 オクテットの文字列として表記します。

管理インターフェイスで VPN 選択を有効にするには、**config interface dhcp management option-82 vpsel vpnid***vpn-id* コマンドまたは **config interface dhcp management option-82 vpnselect vrfname vrf-name** コマンドを入力し、続けて **config interface dhcp management option-82 vpsel enable** コマンドを入力します。

ステップ 7 **save config** コマンドを入力して設定を保存します。

ステップ 8 リンク選択設定または VPN 選択インターフェイス設定の詳細を表示するには、**show interface detailed** コマンドを入力します。

[DHCP Link Select] および [VPN Select] の設定 (GUI)

ステップ 1 [Controller] > [Interfaces] を選択します。

ステップ 2 DHCP オプション 82 リンク選択または VPN 選択を設定するインターフェイスを選択します。コントローラの管理インターフェイスまたは動的インターフェイスで DHCP オプション 82 リンク選択を設定できます。

[Interfaces > Edit] ページに、コントローラ上で設定されているプライマリおよびセカンダリ DHCP サーバの DHCP 情報が表示されます。プライマリおよびセカンダリ サーバが表示されない場合は、このウィンドウに表示されるテキストボックスに DHCP サーバの IP アドレスの値を入力する必要があります。

- ステップ 3** [Enable DHCP Option 82] チェックボックスをオンにして、インターフェイスで DHCP オプション 82 を有効にします。
- ステップ 4** [Enable DHCP Option 82-Link Select] チェックボックスをオンにして、インターフェイスでリンク選択を有効にします。
- ステップ 5** [Link Select relay source] ドロップダウンリストから、[management] または [dynamic] を選択して、インターフェイスでリンク選択を有効にします。
リンク選択が有効な場合、コントローラ上で設定されるリレーソース管理および動的インターフェイスとして任意のインターフェイスを選択できます。
- ステップ 6** [Enable DHCP Option 82-VPN Select] チェックボックスをオンにして、管理インターフェイスで VPN 選択を有効にします。
VPN 選択が有効な場合、VRF 名または VPN ID のどちらかを設定できます。両方のオプションを設定しようとする、エラーメッセージが表示されて入力を促されます。
- ステップ 7** [VPN Select - VRF name] テキストボックスに、VRF 名を入力します。
- ステップ 8** [VPN Select - VPN ID] テキストボックスに、VPN ID を入力します。
VPN ID は xxxxxx:xxxxxxx の形式で入力する必要があります。
- ステップ 9** [Apply] をクリックして、設定を保存します
-



第 8 章

SNMP の設定

- [SNMP の設定 \(CLI\)](#) , 107 ページ
- [SNMP コミュニティストリング](#) , 109 ページ
- [リアルタイム統計情報の設定 \(CLI\)](#) , 111 ページ

SNMP の設定 (CLI)



(注) コントローラ トラップ ログを表示するには、コントローラ GUI の [Monitor] を選択してから [Most Recent Traps] の下の [View All] をクリックします。

- 次のコマンドを入力して、SNMP コミュニティ名を作成します。
config snmp community create name
- 次のコマンドを入力して、SNMP コミュニティ名を削除します。
config snmp community delete name
- 次のコマンドを入力して、読み取り専用権限を持つ SNMP コミュニティ名を設定します。
config snmp community accessmode ro name
- 次のコマンドを入力して、読み取り/書き込み権限を持つ SNMP コミュニティ名を設定します。
config snmp community accessmode rw name
- 次のコマンドを入力して、SNMP コミュニティの IP アドレスとサブネット マスクを設定します。
config snmp community ipaddr ip-address ip-mask name



(注) このコマンドは、SNMP アクセス リストのように動作します。デバイスは、このコマンドで指定された IP アドレスから、アソシエートされたコミュニティ付きの SNMP パケットを受け入れます。要求元エンティティの IP アドレスとサブネット マスクの間で AND 演算が行われた後、IP アドレスが比較されます。サブネット マスクが 0.0.0.0 に設定されている場合、IP アドレス 0.0.0.0 はすべての IP アドレスに一致します。デフォルト値は 0.0.0.0 です。



(注) コントローラが 1 つの SNMP コミュニティの管理に使用できる IP アドレス範囲は 1 つだけです。

- 次のコマンドを入力して、コミュニティ名を有効または無効にします。
config snmp community mode {enable | disable}
- 次のコマンドを入力して、トラップの宛先を設定します。
config snmp trapreceiver create name ip-address
- 次のコマンドを入力して、トラップを削除します。
config snmp trapreceiver delete name
- 次のコマンドを入力して、トラップの宛先を変更します。
config snmp trapreceiver ipaddr old-ip-address name new-ip-address
- 次のコマンドを入力して、トラップを有効または無効にします。
config snmp trapreceiver mode {enable | disable}
- 次のコマンドを入力して、SNMP コンタクトの名前を設定します。
config snmp syscontact syscontact-name
担当者名には、最大 31 文字の英数字を使用できます。
- 次のコマンドを入力して、SNMP システムの場所を設定します。
config snmp syslocation syslocation-name
場所の名前には、最大 31 文字の英数字を使用できます。
- 次のコマンドを入力して、SNMP トラップおよびコミュニティが正しく設定されていることを確認します。
show snmpcommunity
show snmptrap
- 次のコマンドを入力して、有効および無効にされたトラップ フラグを表示します。
show trapflags
必要に応じて、**config trapflags** コマンドを使用して、トラップ フラグを有効または無効にします。
- 次のコマンドを入力することで、コントローラに関連付けられたクライアントまたは RFID の数がしきい値レベル付近になった後、警告メッセージが表示される条件を設定します。
config trapflags {client | rfid} max-warning-threshold {threshold-between-80-to-100 | enable | disable}
警告メッセージは 600 秒 (10 分) ごとに表示されます。

- 次のコマンドを入力して、SNMP エンジン ID を設定します。
config snmp engineID engine-id-string



(注) エンジン ID の文字列には、最大 24 文字を使用できます。

- 次のコマンドを入力して、エンジン ID を表示します。
show snmpengineID
- 次のコマンドを入力して、SNMP バージョンを設定します。
config snmp version {v1 | v2c | v3} {enable | disable}

SNMP コミュニティストリング

読み取り専用および読み取り/書き込みの SNMP コミュニティストリングに対するコントローラのデフォルト値には、「public」と「private」という一般に知られた値が使用されています。これらの標準値を使用すると、セキュリティ上のリスクが発生します。デフォルトのコミュニティ名のままだと、それらは知られているので、SNMP を使用したコントローラとの通信に利用されるおそれがあります。したがって、これらの値を変更することを強く推奨します。

SNMP コミュニティストリングのデフォルト値の変更 (GUI)

- ステップ 1 [Management] を選択してから、[SNMP] の下の [Communities] を選択します。[SNMP v1 / v2c Community] ページが表示されます。
- ステップ 2 [Community Name] カラムに「public」または「private」が表示されている場合は、そのコミュニティの青いドロップダウン矢印の上にカーソルを置き、[Remove] を選択してそのコミュニティを削除します。
- ステップ 3 [New] をクリックして、新しいコミュニティを作成します。[SNMP v1 / v2c Community > New] ページが表示されます。
- ステップ 4 [Community Name] テキストボックスに、16 文字以内の英数字から成る一意の名前を入力します。「public」または「private」を入力しないでください。
- ステップ 5 次の 2 つのテキストボックスには、IP アドレスと IP マスクを指定します。デバイスは、この IP アドレスから、アソシエートされたコミュニティ付きの SNMP パケットを受け入れます。
- ステップ 6 [Access Mode] ドロップダウンリストから [Read Only] または [Read/Write] を選択して、このコミュニティのアクセス レベルを指定します。
- ステップ 7 [Status] ドロップダウンリストから [Enable] または [Disable] を選択して、このコミュニティのステータスを指定します。
- ステップ 8 [Apply] をクリックして、変更を確定します。
- ステップ 9 [Save Configuration] をクリックして設定を保存します。
- ステップ 10 「public」または「private」というコミュニティがまだ [SNMP v1 / v2c Community] ページに表示されている場合には、この手順を繰り返します。

SNMP コミュニティストリングのデフォルト値の変更 (CLI)

- ステップ 1 次のコマンドを入力して、このコントローラに対する SNMP コミュニティの最新のリストを表示します。
show snmp community
- ステップ 2 [SNMP Community Name] カラムに「public」または「private」と表示されている場合は、次のコマンドを入力してこのコミュニティを削除します。
config snmp community delete name
name パラメータがコミュニティ名です（この場合は「public」または「private」）。
- ステップ 3 次のコマンドを入力して、新しいコミュニティを作成します。
config snmp community create name
name パラメータに、16 文字以内の英数字を入力します。「public」または「private」を入力しないでください。

- ステップ 4** 次のコマンドを入力して、このデバイスが、アソシエートされたコミュニティ付きの SNMP パケットをどの IP アドレスから受け入れるかを指定します。
config snmp community ipaddr ip_address ip_mask name
- ステップ 5** 次のコマンドを入力して、このコミュニティのアクセス レベルを指定します。ここで、**ro** は読み取り専用モードで、**rw** は読み書きモードです。
config snmp community accessmode {ro | rw} name
- ステップ 6** 次のコマンドを入力して、この SNMP コミュニティを有効または無効にします。
config snmp community mode {enable | disable} name
- ステップ 7** 次のコマンドを入力して、変更を保存します。
save config
- ステップ 8** 「public」または「private」コミュニティ スtring のデフォルト値を変更する必要がある場合は、この手順を繰り返します。

リアルタイム統計情報の設定 (CLI)

SNMP トラップは、AP とコントローラの CPU およびメモリ使用率に対して定義されます。SNMP トラップは、しきい値を超過したときに送信されます。サンプリング期間および統計情報の更新間隔は、SNMP と CLI を使用して設定できます。

- 次のコマンドを入力して、サンプリング間隔を設定します。
config service statistics sampling-interval seconds
- 次のコマンドを入力して、統計間隔を設定します。
config service statistics statistics-interval seconds
- 次のコマンドを入力して、サンプリング間隔とサービス間隔の統計を表示します。
show service statistics interval

SNMP トラップの拡張

この機能は、設定可能なしきい値がホールドタイムを呼び出した後、SNMP トラップのソークとトラップの再送信を行います。ホールドタイムは、間違ったトラップ生成の抑制にも役立ちます。サポートされるトラップは、AP コントローラの CPU とメモリ使用率用です。トラップの再送信はトラップが削除されるまで実行されます。

- 次のコマンドを使用して、SNMP トラップが再送信されるまでのホールドタイムを設定します。
config service alarm hold-time seconds
- 次のコマンドを入力して、トラップの再送信間隔を設定します。
config service alarm trap retransmit-interval seconds

- 次のコマンドを入力して、トラップ デバッグを設定します。
debug service alarm {enable | disable}



第 9 章

アグレッシブ ロード バランシングの設定

- [アグレッシブ ロード バランシングの設定について](#), 113 ページ
- [アグレッシブなロード バランシングの設定 \(GUI\)](#), 114 ページ
- [アグレッシブなロード バランシングの設定 \(CLI\)](#), 115 ページ

アグレッシブ ロード バランシングの設定について

コントローラ上でアグレッシブ ロード バランシングを有効にすると、ワイヤレス クライアントの負荷を Lightweight アクセス ポイント間で分散することができます。アグレッシブ ロード バランシングはコントローラを使用して有効にできます。



(注) クライアントの負荷は、同じコントローラ上のアクセス ポイント間で分散されます。別のコントローラ上のアクセス ポイントとの間では、ロード バランシングは行われません。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。コード 17 は AP がビジー状態であることを示します。AP のしきい値が満たされていない場合、AP は「success」を示すアソシエーション応答で応答します。AP 使用率のしきい値に達した、またはしきい値を超過した場合は、コード 17 (AP ビジー) で応答し、よりビジー状態の度合いが低い別の AP がクライアント要求を受け取ります。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウの和を上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントが AP1 にアソシエートしようとする、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。アクセスポイントの負荷が高いことがこのステータスコードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

コントローラは、クライアント アソシエーションを 10 回まで拒否するように設定できます (クライアントがアソシエーションを 11 回試みた場合、11 回目の試行時にアソシエーションが許可されます)。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指

定できます。これは、特定のクライアント グループ (遅延に敏感な音声クライアントなど) に対してロード バランシングを無効にする場合に便利です。

パッシブ スキャン クライアントは、ロード バランシングが有効か無効かに関係なく、AP に関連付けられます。



(注) Cisco 600 シリーズ OfficeExtend アクセス ポイントはクライアント ロード バランシングをサポートしません。

7.4 リリースでは、FlexConnect アクセス ポイントはクライアント ロード バランシングをサポートします。

隣接 AP の WAN インターフェイスの使用率を分析するようにコントローラを設定して、負荷が軽い AP 間のクライアントをロード バランスすることができます。これを設定するには、ロード バランシングしきい値を定義します。しきい値の定義することによって、WAN インターフェイスの使用率 (%) を測定できます。たとえば、50 というしきい値を設定すると、AP-WAN インターフェイスで 50% 以上の使用率を検出した場合にロード バランシングがトリガされます。

アグレッシブなロード バランシングの設定 (GUI)

ステップ 1 [Wireless] > [Advanced] > [Load Balancing] を選択して、[Load Balancing] ページを開きます。

ステップ 2 [Client Window Size] テキスト ボックスに、1 ~ 20 の値を入力します。
このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアント ウィンドウ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこのしきい値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数がしきい値を下回るアクセス ポイントだけとなります。

ステップ 3 [Maximum Denial Count] テキスト ボックスに、0 ~ 10 の値を入力します。
拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

ステップ 6 特定の WLAN 上でアグレッシブ ロード バランシングを有効または無効にするには、次の手順を実行します。

a) [WLANs] > [WLAN ID] を選択します。[WLANs > Edit] ページが表示されます。

- b) [Advanced] タブで、[Client Load Balancing] チェックボックスをオンまたはオフにします。
- c) [Apply] をクリックします。
- d) [Save Configuration] をクリックします。

アグレッシブなロード バランシングの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、アグレッシブロードバランシング用のクライアントウィンドウを設定します。
config load-balancing window client_count
client_count パラメータには、0 ~ 20 の範囲内の値を入力できます。
- ステップ 2** 次のコマンドを入力して、ロードバランシング用の拒否回数を設定します。
config load-balancing denial denial_count
denial_count パラメータには、1 ~ 10 の範囲内の値を入力できます。
- ステップ 3** 次のコマンドを入力して、変更を保存します。
save config
- ステップ 4** 次のコマンドを入力して、特定の WLAN 上のアグレッシブロードバランシングを有効または無効にします。
config wlan load-balance allow {enable | disable} wlan_ID
wlan_ID パラメータには、1 ~ 512 の範囲内の値を入力できます。
- ステップ 5** 次のコマンドを入力して、設定を確認します。
show load-balancing
- ステップ 6** 次のコマンドを入力して、変更を保存します。
save config
- ステップ 7** 次のコマンドを入力して、WLAN のロードバランシングモードを設定します。
config wlan load-balance mode {client-count | uplink-usage} wlan-id
この機能では、AP がコントローラにアップリンクの使用状況の統計情報を定期的にアップロードする必要があります。次のコマンドを入力して、これらの統計を確認してください。
show ap stats system cisco-AP



第 10 章

高速 SSID 変更の設定

- [高速 SSID 変更の設定について](#) , 117 ページ
- [高速 SSID 変更の設定 \(GUI\)](#) , 117 ページ
- [高速 SSID 変更の設定 \(CLI\)](#) , 118 ページ

高速 SSID 変更の設定について

コントローラで Fast SSID Change が有効になっている場合、クライアントは SSID 間で移動することができます。高速 SSID が有効になっている場合、クライアント エントリがクリアされず、遅延は適用されません。

高速 SSID 変更が無効になっている場合、コントローラは一定の遅延時間が経過した後でクライアントに新しい SSID への移動を許可します。高速 SSID が無効になっており、クライアントが異なる SSID の新しいアソシエーションを送信すると、コントローラの接続テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。

高速 SSID 変更の設定 (GUI)

- ステップ 1** [Controller] を選択して [General] ページを開きます。
 - ステップ 2** この機能を有効にするには、[Fast SSID Change] ドロップダウン リストから [Enabled] を選択します。無効にするには、[Disabled] を選択します。デフォルト値はディセーブルです。
 - ステップ 3** [Apply] をクリックして、変更を確定します。
 - ステップ 4** [Save Configuration] をクリックして、変更を保存します。
-

高速 SSID 変更の設定 (CLI)

ステップ 1 次のコマンドを入力して、高速 SSID 変更を有効または無効にします。
config network fast-ssid-change {enable | disable}

ステップ 2 次のコマンドを入力して、変更を保存します。
save config



第 11 章

802.3 ブリッジの設定

- [802.3 ブリッジの設定, 119 ページ](#)
- [802.3X のフロー制御の有効化, 120 ページ](#)

802.3 ブリッジの設定

802.3 ブリッジの設定について

コントローラでは、802.3 のフレームおよびそれらを使用するアプリケーションをサポートしています。このようなアプリケーションには、キャッシュ レジスタやキャッシュ レジスタ サーバなどがあります。ただし、これらのアプリケーションをコントローラとともに使用するには、802.3 のフレームがコントローラ上でブリッジされている必要があります。

Cisco Prime Network Control System を使用して 802.3 ブリッジを設定することもできます。手順については、『*Cisco Prime Network Control System Configuration Guide*』を参照してください。

802.3 ブリッジの制限

- 802.3 Raw フレームのサポートを有効にすると、IP 上では実行されないアプリケーションの非 IP フレームをコントローラがブリッジできるようになります。
802.3 Raw フレームには、宛先 MAC アドレス、送信元 MAC アドレス、総パケット長、およびペイロードが含まれます。
- デフォルトでは、Cisco 5500 シリーズ コントローラでは、すべての非 IPv4 パケット（AppleTalk、IPv6 など）がブリッジされます。ACL を使用してこれらのプロトコルのブリッジングをブロックすることもできます。

802.3 ブリッジの設定

802.3 ブリッジの設定 (GUI)

-
- ステップ 1 [Controller] > [General] の順に選択して、[General] ページを開きます。
 - ステップ 2 802.3ブリッジをコントローラ上で有効にする場合は、[802.3 Bridging] ドロップダウンリストから [Enabled] を選択し、無効にする場合は [Disabled] を選択します。デフォルト値は [Disabled] です。
 - ステップ 3 [Apply] をクリックして、変更を確定します。
 - ステップ 4 [Save Configuration] をクリックして、変更を保存します。
-

802.3 ブリッジの設定 (CLI)

-
- ステップ 1 次のコマンドを入力して、すべての WLAN の 802.3 ブリッジの現在のステータスを表示します。
show network
 - ステップ 2 次のコマンドを入力して、すべての WLAN でグローバルに 802.3 ブリッジを有効または無効にします。
config network 802.3-bridging {enable | disable}
デフォルト値はディセーブルです。
 - ステップ 3 次のコマンドを入力して、変更を保存します。
save config
-

802.3X のフロー制御の有効化

802.3X のフロー制御は、デフォルトでは無効にされています。有効にするには、**configswitchconfig flowcontrol enable** コマンドを入力します。



第 12 章

マルチキャストの設定

- [マルチキャストモードの設定, 121 ページ](#)
- [マルチキャストドメインネームシステムの設定, 128 ページ](#)

マルチキャストモードの設定

マルチキャストモードについて

ネットワークがパケットマルチキャストをサポートしている場合は、コントローラで使用されるマルチキャストの方法を設定できます。コントローラは次の2つのモードでマルチキャストを実行します。

- **ユニキャストモード**：コントローラにアソシエートしているすべてのアクセスポイントに、すべてのマルチキャストパケットがユニキャストされます。このモードは非効率的ですが、マルチキャストをサポートしないネットワークでは必要な場合があります。
- **マルチキャストモード**：マルチキャストパケットはCAPWAPマルチキャストグループに送信されます。この方法では、コントローラプロセッサのオーバーヘッドが軽減され、パケットレプリケーションの作業はネットワークに移されます。これは、ユニキャストを使った方法より、はるかに効率的です。

マルチキャストモードが有効な場合に、コントローラがマルチキャストパケットを有線LANから受信すると、コントローラはCAPWAPを使用してパケットをカプセル化し、CAPWAPマルチキャストグループアドレスへ転送します。コントローラは、必ず管理インターフェイスを使用してマルチキャストパケットを送信します。マルチキャストグループのアクセスポイントはパケットを受け取り、クライアントがマルチキャストトラフィックを受信するインターフェイスにマップされたすべてのBSSIDにこれを転送します。アクセスポイントからは、マルチキャストはすべてのSSIDに対するブロードキャストのように見えます。

コントローラは、IPv6マルチキャスト用にマルチキャストリスナー検出(MLD)v1スヌーピングをサポートします。この機能により、IPv6マルチキャストフローが追跡され、フローを要求し

たクライアントにそれらが配信されます。IPv6 マルチキャストをサポートするには、グローバルマルチキャストモードを有効にする必要があります。



(注) グローバルマルチキャストモードを無効にしても、ルータの通知や DHCPv6 要求などの IPv6 ICMP メッセージは IPv6 が機能するために必要であるため、コントローラはそれらを転送します。このため、コントローラでグローバルマルチキャストモードを有効にしても、ICMPv6 と DHCPv6 のメッセージに影響は及ぼされません。これらのメッセージは、グローバルマルチキャストモードが有効であるかどうかにかかわらず、常に転送されます。

コントローラ ソフトウェア 4.2 以降のリリースでは、マルチキャストパケットのダイレクトを向上させるために、インターネットグループ管理プロトコル (IGMP) スヌーピングを導入しています。この機能が有効になっている場合、コントローラは IGMP レポートをクライアントから収集して処理し、レイヤ 3 マルチキャストアドレスと VLAN 番号を選択した後に IGMP レポートから一意なマルチキャストグループ ID (MGID) を作成し、その IGMP レポートをインフラストラクチャスイッチへ送信します。コントローラから送信されるレポートの送信元アドレスには、コントローラがレポートをクライアントから受信したインターフェイスのアドレスが使用されます。次に、コントローラは、アクセスポイント上のアクセスポイント MGID テーブルを、クライアント MAC アドレスを使用して更新します。コントローラが特定のマルチキャストグループのマルチキャストトラフィックを受信した場合、それをすべてのアクセスポイントに転送します。ただし、アクティブなクライアントでリッスンしているアクセスポイント、またはそのマルチキャストグループへ加入しているアクセスポイントだけは、その特定の WLAN 上でマルチキャストトラフィックを送信します。IP パケットは、入力 VLAN および宛先マルチキャストグループの一意の MGID を使用して転送されます。レイヤ 2 マルチキャストパケットは、入力インターフェイスの一意の MGID を使用して転送されます。

IGMP スヌーピングが無効になっている場合は、次のようになります。

- コントローラは、マルチキャストデータをアクセスポイントへ送信する際は必ずレイヤ 2 MGID を使用します。作成された各インターフェイスは、1 つのレイヤ 2 MGID を割り当てられます。たとえば、管理インターフェイスの MGID は 0 となります。また、作成された 1 つ目の動的インターフェイスに割り当てられる MGID は 8 となり、動的インターフェイスが作成されるにつれて 1 増えます。
- クライアントからの IGMP パケットはルータへ転送されます。それにより、ルータの IGMP テーブルは、最後のレポートとしてクライアントの IP アドレスで更新されます。

IGMP スヌーピングが有効になっている場合は、次のようになります。

- コントローラは、アクセスポイントへ送信されるすべてのレイヤ 3 マルチキャストトラフィックに必ずレイヤ 3 MGID を使用します。すべてのレイヤ 2 マルチキャストトラフィックについては、引き続きレイヤ 2 MGID を使用します。
- ワイヤレスクライアントからの IGMP レポートパケットは、クライアントに対するクエリーを生成するコントローラによって消費または吸収されます。ルータによって IGMP クエリーが送信されると、コントローラによって IGMP レポートが送信されます。このレポートでは、コントローラのインターフェイス IP アドレスがマルチキャストグループのリスナー IP

アドレスとして設定されています。それにより、ルータのIGMPテーブルは、マルチキャストリスナーとしてコントローラ IP アドレスで更新されます。

- マルチキャストグループをリッスンしているクライアントが、あるコントローラから別のコントローラへローミングしたときは、リッスンしているクライアント用のすべてのマルチキャストグループ情報が、最初のコントローラから2番目のコントローラへ送信されます。それにより、2番目のコントローラは、クライアント用のマルチキャストグループ情報をただちに作成できます。2番目のコントローラでは、クライアントがリッスンしていた全マルチキャストグループのネットワークにIGMPレポートが送信されます。このプロセスは、クライアントへのマルチキャストデータのシームレスな転送に役立ちます。
- リッスンしているクライアントが、別のサブネットのコントローラにローミングした場合は、マルチキャストパケットは、Reverse Path Filtering (RPF; 逆方向パス転送) のチェックを避けるために、クライアントのアンカーコントローラへトンネリングされます。アンカーは、マルチキャストパケットをインフラストラクチャスイッチへ転送します。



(注) MGID はコントローラ固有です。2つの異なるコントローラの同一 VLAN から送られて来る同一マルチキャストグループのパケットは、2つの異なる MGID へマップされる可能性があります。



(注) レイヤ2 マルチキャストが有効になっている場合は、同じインターフェイスから送信されるすべてのマルチキャストアドレスに単一の MGID が割り当てられます。



(注) Cisco WLC の VLAN ごとにサポートされるマルチキャストアドレス数は 100 です。

マルチキャストモード設定の制限

- Cisco Unified Wireless Network ソリューションでは、特定の目的に対して次の IP アドレス範囲を使用します。マルチキャストグループを設定する場合は、この範囲を覚えておいてください。
 - 224.0.0.0 ~ 224.0.0.255 : 予約済みリンクのローカルアドレス
 - 224.0.1.0 ~ 238.255.255.255 : グローバルスコープのアドレス
 - 239.0.0.0 ~ 239.255.x.y /16 : 限定スコープのアドレス
- コントローラ上でマルチキャストモードを有効にする場合は、CAPWAP マルチキャストグループアドレスも設定する必要があります。アクセスポイントは、IGMPを使用してCAPWAPマルチキャストグループに加入します。

- Cisco アクセスポイント 1100、1130、1200、1230、および 1240 は、IGMP バージョン 1、2、および 3 を使用します。
- 監視モード、スニファ モード、または不正検出モードのアクセス ポイントは、CAPWAP マルチキャスト グループ アドレスには加入しません。
- コントローラ上で設定されている CAPWAP マルチキャスト グループは、コントローラごとに異なっている必要があります。
- 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を送信し、最も低い必須 Basic レートで管理フレームを送信し、信頼性の問題が発生する可能性があります。 LWAPP または自律 Cisco 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信します。このような動作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、セルの端のクライアント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、マルチキャストフレームを低いデータ 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フレーム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。

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る場合、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 レートとして設定できます。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。
- マルチキャストモードは、ゲスト トンネリングなどのサブネット間のモビリティ イベントでは動作しません。ただし、RADIUS を使用したインターフェイスの上書き (IGMP スヌーピングが有効になっている場合のみ) またはサイト専用の VLAN (アクセスポイントグループ VLAN) では動作します。
- LWAPP では、コントローラは UDP 制御ポート 12223 に送信されたマルチキャスト パケットをドロップします。CAPWAP では、コントローラは UDP 制御ポート 5246 とデータ ポート 5247 に送信されたマルチキャスト パケットをドロップします。したがって、これらのポート番号をネットワーク上のマルチキャストアプリケーションで使用しないようにしてください。
- ネットワーク上のマルチキャストアプリケーションには、コントローラ上で CAPWAP マルチキャスト グループ アドレスとして設定されたマルチキャスト アドレスを使用しないことをお勧めします。

- 2500 シリーズ コントローラ上でマルチキャストが動作するには、マルチキャスト IP アドレスを設定する必要があります。
- マルチキャストモードは Cisco Flex 7500 シリーズのコントローラではサポートされません。

マルチキャストモードの有効化 (GUI)

-
- ステップ 1** [Controller]>[Multicast] の順に選択して [Multicast] ページを開きます。
- ステップ 2** [Enable Global Multicast Mode] チェックボックスをオンにして、マルチキャストパケットの送信を設定します。デフォルト値はディセーブルです。
- (注) FlexConnect では、ユニキャストモードのみがサポートされています。
- ステップ 3** IGMP スヌーピングを有効にする場合は、[Enable IGMP Snooping] チェックボックスをオンにします。IGMP スヌーピングを無効にする場合は、チェックボックスをオフのままにします。デフォルト値はディセーブルです。
- ステップ 4** IGMP タイムアウトを設定するには、30 ~ 7200 秒の範囲内の値を [IGMP Timeout] テキストボックスに入力します。特定のマルチキャストグループに対してクライアントが存在するかどうかを確認するために、コントローラから、1つのタイムアウト値につき3つのクエリーが $timeout/3$ の間隔で送信されます。クライアントから、IGMP レポートを通じて応答を受け取らなかった場合、コントローラはこのクライアントのエントリを MGID テーブルからタイムアウトします。特定のマルチキャストグループに対するクライアントが残されていない場合、クライアントは IGMP タイムアウト値が経過するまで待ってから、コントローラから MGID エントリを削除します。一般的な IGMP クエリー (つまり、宛先アドレス 224.0.0.1) がコントローラによって必ず生成され、MGID 値 1 を使用してすべての WLAN 上で送信されます。
- ステップ 5** IGMP クエリー間隔 (秒数) を入力します。
- ステップ 6** [Enable MLD Snooping] チェックボックスをオンにして、IPv6 の転送先の決定をサポートします。
- (注) MLD スヌーピングを有効にするには、コントローラのグローバルマルチキャストモードを有効にする必要があります。
- ステップ 7** [MLD Timeout] テキストボックスで、30 ~ 7200 秒の範囲内の値を入力して MLD タイムアウトを設定します。
- ステップ 8** [MLD Query Interval] (秒数) を入力します。有効な範囲は、15 ~ 2400 秒です。
- ステップ 9** [Apply] をクリックして、変更を確定します。
- ステップ 10** [Save Configuration] をクリックして、変更を保存します。
-

マルチキャストモードの有効化 (CLI)

-
- ステップ 1** 次のコマンドを入力して、コントローラ上でマルチキャストを有効または無効にします。

config network multicast global {enable | disable}

デフォルト値はディセーブルです。

(注) **config network broadcast {enable | disable}** コマンドを使用すると、マルチキャストを有効または無効にしなくても、ブロードキャストを有効または無効にできます。このコマンドは、現在コントローラで使用されているマルチキャストモードを使用して動作します。

ステップ 2 次のいずれかを実行します。

a) 次のコマンドを入力して、マルチキャストパケットを送信するために、ユニキャスト方式を使用するようにコントローラを設定します。

config network multicast mode unicast

b) 次のコマンドを入力して、マルチキャストパケットを CAPWAP マルチキャストグループに送信するために、マルチキャスト方式を使用するようにコントローラを設定します。

config network multicast mode multicast multicast_group_ip_address

ステップ 3 次のコマンドを入力して、IGMP スヌーピングを有効または無効にします。

config network multicast igmp snooping {enable | disable}

デフォルト値はディセーブルです。

ステップ 4 次のコマンドを入力して、IGMP タイムアウト値を設定します。

config network multicast igmp timeout timeout

timeout には、30 ～ 7200 秒の値を入力できます。特定のマルチキャストグループに対してクライアントが存在するかどうかを確認するために、コントローラから、1つのタイムアウト値につき3つのクエリが *timeout/3* の間隔で送信されます。クライアントから、IGMP レポートを通じて応答を受け取らなかった場合、コントローラはこのクライアントのエントリを MGID テーブルからタイムアウトします。特定のマルチキャストグループに対するクライアントが残されていない場合、クライアントは IGMP タイムアウト値が経過するまで待ってから、コントローラから MGID エントリを削除します。一般的な IGMP クエリー（つまり、宛先アドレス 224.0.0.1）がコントローラによって必ず生成され、MGID 値 1 を使用してすべての WLAN 上で送信されます。

ステップ 5 次のコマンドを入力して、MLD スヌーピングを有効または無効にします。

config network multicast mld snooping {enable | disable}

デフォルト値はディセーブルです。

(注) MLD スヌーピングを有効にするには、コントローラのグローバルマルチキャストモードを有効にする必要があります。

ステップ 6 次のコマンドを入力して、MLD タイムアウト値を設定します。

config network multicast mld timeout timeout

[MLD Query Interval] (秒数) を入力します。有効な範囲は、15 ～ 2400 秒です。

ステップ 7 次のコマンドを入力して、変更を保存します。

save config

マルチキャストグループの表示 (GUI)

- ステップ 1** [Monitor] > [Multicast] の順に選択します。 [Multicast Groups] ページが表示されます。
このページには、すべてのマルチキャストグループとそれらに対応する MGID が表示されます。
- ステップ 2** 特定の MGID (MGID 550 など) のリンクをクリックすると、その MGID のマルチキャストグループに接続されているすべてのクライアントの一覧が表示されます。

マルチキャストグループの表示 (CLI)

はじめる前に

- 次のコマンドを入力して、すべてのマルチキャストグループとそれらに対応する MGID を表示します。

show network multicast mgid summary

以下に類似した情報が表示されます。

```
Layer2 MGID Mapping:
-----
InterfaceName          vlanId  MGID
-----
management             0       0
test                   0       9
wired                   20      8

Layer3 MGID Mapping:
-----
Number of Layer3 MGIDs..... 1

  Group address      Vlan  MGID
  -----
  239.255.255.250   0     550
```

- 次のコマンドを入力して、特定の MGID のマルチキャストグループに join しているすべてのクライアントを表示します。

show network multicast mgid detail mgid_value

mgid_value パラメータは、550 ~ 4095 の数値です。

以下に類似した情報が表示されます。

```
Mgid..... 550
Multicast Group Address..... 239.255.255.250
Vlan..... 0
Rx Packet Count..... 807399588
No of clients..... 1
Client List.....
  Client MAC          Expire Time (mm:ss)
  00:13:02:23:82:ad  0:20
```

アクセスポイントのマルチキャストクライアントテーブルの表示 (CLI)

ローミングイベントのトラブルシューティングに役立つ、アクセスポイントのマルチキャストクライアントテーブルを表示するには、アクセスポイントのリモートデバッグをコントローラから実行します。

-
- ステップ 1** 次のコマンドを入力して、アクセスポイントのリモートデバッグを開始します。
- ```
debug ap enable Cisco_AP
```
- ステップ 2** 次のコマンドを入力して、アクセスポイント上のすべての MGID の一覧と、WLAN ごとのクライアント数を表示します。
- ```
debug ap command "show capwap mcast mgid all" Cisco_AP
```
- ステップ 3** 次のコマンドを入力して、アクセスポイント上の MGID ごとのクライアント一覧と、WLAN ごとのクライアント数を表示します。
- ```
debug ap command "show capwap mcast mgid id mgid_value" Cisco_AP
```
- 

## マルチキャストドメインネームシステムの設定

### マルチキャストドメインネームシステムについて

マルチキャストドメインネームシステム (mDNS) サービスディスカバリは、ローカルネットワークでサービスを検出する手段を提供します。mDNS サービスディスカバリによって、ワイヤレスクライアントは別のレイヤ 3 ネットワークにアダプタイズされた Apple プリンタおよび Apple TV などの Apple サービスにアクセスすることができます。mDNS は IP マルチキャストを介した DNS クエリーを実行します。mDNS はゼロ設定 IP ネットワーキングをサポートします。通常どおり、mDNS は宛先アドレスとしてマルチキャスト IP アドレス 224.0.0.251 を使用し、UDP 宛先ポートとして 5353 を使用します。

#### ロケーション固有サービス

mDNS サービスアダプタイズメントの処理および mDNS クエリーパケットは、ロケーション固有サービス (LSS) をサポートしています。コントローラが受信するすべての有効な mDNS サービスアダプタイズメントは、新しいエントリをサービスプロバイダーのデータベースに挿入する際に、サービスプロバイダーからのサービスアダプタイズメントに関連付けられた AP の MAC アドレスにタグ付けされます。クライアントクエリーに対する応答記述では、クエリー送信するクライアントに関連付けられた AP の MAC アドレスを使用して SP-DB のワイヤレスエントリをフィルタリングします。ワイヤレスサービスプロバイダーのデータベースエントリは、LSS がサービスに対して有効になっている場合、AP-NEIGHBOR-LIST に基づいてフィルタリングされます。LSS がサービスに対して無効になっている場合、ワイヤレスサービスプロバイダーのデー

データベースエントリは、そのサービスに対するワイヤレスクライアントからのクエリに応答する場合、フィルタリング対象ではありません。

LSS は、ワイヤレス サービス プロバイダーのデータベース エントリだけに適用されます。有線サービス プロバイダー デバイスのロケーションは認識されません。

LSS の状態は、ORIGIN が有線に設定されているサービスに対して有効にすることはできません。この逆も同じです。

### mDNS AP

mDNS AP 機能により、コントローラは、表示されない VLAN 上の有線サービス プロバイダーに対する可視性を獲得できます。mDNS AP として AP を設定し、AP がコントローラに mDNS パケットを転送するようにできます。コントローラの VLAN の可視性は、AP が mDNS アドバタイズメントをコントローラに転送することで実現されます。AP とコントローラ間の mDNS パケットは、ワイヤレスクライアントからの mDNS パケットと同様に、Control and Provisioning of Wireless Access Points (CAPWAP) データトンネルで転送されます。CAPWAP v4 のトンネルのみがサポートされます。AP をアクセスポートまたはトランクポートに設置して有線側からの mDNS パケットを学習し、コントローラに転送することができます。

特定の AP からの mDNS パケット転送を開始または停止する際、コントローラで提供される設定可能なノブを使用できます。また、この設定を使用して、AP が有線側から mDNS アドバタイズメントをスヌープする必要のある VLAN を指定できます。AP がスヌープできる VLAN の最大数は 10 です。

AP がアクセスポートに設置されている場合、スヌープするように AP の VLAN を設定しないでください。クエリが送信されると、AP はタグ付けされていないパケットを送信します。mDNS アドバタイズメントが mDNS AP によって受信されると、VLAN 情報はコントローラに渡されません。mDNS AP のアクセス VLAN 経由で学習されるサービスプロバイダーの VLAN は、コントローラで 0 として保持されます。

デフォルトでは、mDNS AP はネイティブ VLAN でスヌープします。mDNS AP が有効な場合、ネイティブ VLAN のスヌーピングはデフォルトで有効になっており、VLAN 情報はネイティブ VLAN で受信したアドバタイズメントに対して 0 として渡されます。

mDNS AP 機能は、ローカルモードとモニタモードの AP でのみサポートされます。

mDNS AP 設定は、グローバル mDNs スヌーピングを無効にしてもそれぞれの mDNS AP で保持されます。



(注) 同じサービスの同じトラフィックを複製している 2 つの mDNS AP がないことを保証するための検査はありません。ただし、同じ VLAN に対しては、そのようなチェックが行われます。

mDNS AP がリセットされるか、同じコントローラまたは別のコントローラに関連付けられている場合は、次のいずれかが発生します。

- グローバル スヌーピングがコントローラで無効になっている場合、ペイロードが AP に送信されて mDNS スヌーピングは無効になります。

- グローバル スヌーピングがコントローラで有効になっている場合、リセットまたはアソシエーションの手順より前の AP の設定が保持されます。

mDNS AP 機能のプロセス フローは次のとおりです。

- アップリンク (有線インフラストラクチャ - AP - コントローラ)
  - 1 設定された VLAN で mDNS 802.3 パケットを受信します。
  - 2 受信した mDNS パケットを CAPWAP を介して転送します。
  - 3 受信した VLAN に基づいてマルチキャストグループ ID (MGID) を入力します。
- ダウンリンク (コントローラ - AP - 有線インフラストラクチャ)
  - 1 コントローラから CAPWAP を介して mDNS クエリーを受信します。
  - 2 有線インフラストラクチャに 802.3 パケットとしてクエリーを転送します。
  - 3 VLAN は専用 MGID で識別されます。

### サービスごとの SP カウント制限

次のリストに、グローバルサービスプロバイダーの制限をコントローラモデルごとに示します。

- Cisco 8500 シリーズ ワイヤレス LAN コントローラ : 16000
- Cisco Flex 7500 シリーズ ワイヤレス LAN コントローラ : 16000
- Cisco 5500 シリーズ ワイヤレス LAN コントローラ : 6400
- Cisco 2500 シリーズ ワイヤレス LAN コントローラ : 6400

すべてのサービスのサービスプロバイダーの総数が指定制限内である場合、サービスが他のサービスを学習または検出できる数に制限はありません。サービスごとの条件または制限がなく、すべてのサービスで他のサービスに関してより多くのサービスプロバイダーに柔軟に対応できません。

### プライオリティ MAC サポート

サービスごとに最大 50 の MAC アドレスを設定できます。これらの MAC アドレスは、プライオリティを必要とするサービスプロバイダーの MAC アドレスです。これによって、サービスプロバイダーのデータベースがフルであっても、サービスプロバイダー数が最多であるサービスから最新の非プライオリティサービスプロバイダーを削除することによって、設定されたサービスの MAC アドレスから発信されるあらゆるサービスアドバタイズメントが学習されることが保証されます。サービスのプライオリティ MAC アドレスを設定する場合は、**ap-group** と呼ばれるオプションのパラメータがあります。これは有線サービスプロバイダーにのみ適用され、有線サービスプロバイダーデバイスにロケーションの特定を関連付けます。クライアントの mDNS クエリーがこの **ap-group** から発信されると、プライオリティ MAC および **ap-group** による有線エントリが検索されて、集約応答の最初に表示されます。



### Origin-Based Service Discovery

発信元（有線または無線）に基づいて着信トラフィックをフィルタするようにサービスを設定できます。mDNS AP から学習されたすべてのサービスは有線として扱われます。認識元が有線である場合、LSS は無線サービスにのみ適用されるため、LSS サービスに対して有効にすることはできません。

LSS ステータスがサービスに対して有効である場合、LSS は無線サービス プロバイダーのデータベースのみに適用されるため、発信元が無線に設定されたサービスを有線に変更することはできません。発信元を有線と無線で変更した場合、変更前の発信元タイプを持つサービス プロバイダーのデータベース エントリは削除されます。

## マルチキャスト DNS の設定の制限

- IPv6 を介した mDNS はサポートされません。
- ローカル側で切り替えられた WLAN およびメッシュ アクセス ポイントでは、FlexConnect モードのアクセス ポイントで mDNS はサポートされていません。
- mDNS はリモート LAN ではサポートされません。
- mDNS は Cisco AP1240 および Cisco AP1130 ではサポートされていません。
- サードパーティの mDNS サーバまたはアプリケーションは mDNS 機能を使用する Cisco WLC ではサポートされていません。 サードパーティ サーバまたはアプリケーションによってアドバタイズされるデバイスは、Cisco WLC で mDNS のサービスまたはデバイス テーブルに正しく入力されません。
- ビデオは、WMM が有効な状態の Apple iOS 6 ではサポートされていません。
- mDNS AP は同じサービスまたは VLAN に対して同じトラフィックを複製することはできません。
- LSS フィルタリングはワイヤレス サービスのみに制限されます。
- LSS、mDNS AP、プライオリティ MAC アドレスおよび送信元ベースの検出機能は、コントローラの GUI を使用して設定できません。

## マルチキャスト DNS の設定 (GUI)

- ステップ 1** 次の手順に従って、グローバル mDNS パラメータおよびマスター サービス データベースを設定します。
- a) [Controller] > [mDNS] > [General] を選択します。
  - b) [mDNS Global Snooping] チェックボックスをオンまたはオフにすることで、mDNS パケットのスヌーピングをイネーブルまたはディセーブルにします。
  - c) 分単位で mDNS クエリー間隔を入力します。クエリー間隔はコントローラがサービスを検索する頻度です。
  - d) [Select Service] ドロップダウン リストからサービスを選択します。

(注) mDNS がサポートされた新しいサービスをリストに追加するには、[Other] を選択します。サービス名およびサービス スtring を指定します。コントローラは、マスター サービス データベースで mDNS サービスが利用できる場合にのみ、このサービスのアドバタイズメントをスヌーピングおよび学習します。コントローラは、最大 64 のサービスをスヌープおよび認識できます。

- e) [Query Status] チェックボックスをオンまたはオフにすることで、サービスの mDNS クエリーをイネーブルまたはディセーブルにします。
- f) [Add] をクリックします。
- g) [Apply] をクリックします。
- h) mDNS サービスの詳細を確認するには、そのサービスの青いドロップダウン矢印の上にカーソルを置いて、[Details] を選択します。

**ステップ 2** 次の手順に従って、mDNS プロファイルを設定します。

- a) [Controller] > [mDNS] > [Profiles] を選択します。  
コントローラにはデフォルトの mDNS プロファイルがあります。これは、デフォルトの mdns プロファイルです。デフォルト プロファイルを削除することはできません。
- b) 新しいプロファイルを作成するには、[New] をクリックして、プロファイル名を入力し、[Apply] をクリックします。
- c) プロファイルを編集するには、[mDNS Profiles] ページでプロファイル名をクリックして、[Service Name] ドロップダウンリストからプロファイルに関連付けるサービスを選択し、[Apply] をクリックします。プロファイルには複数のサービスを追加できます。

**ステップ 3** [Save Configuration] をクリックします。

### 次の作業

新しいプロファイルを作成した後、インターフェイスグループ、インターフェイス、または WLAN にプロファイルをマッピングする必要があります。クライアントはプロファイルに関連付けられたサービスだけのサービス アドバタイズメントを受信します。インターフェイスグループに関連付けられたプロファイルに最高の優先順位が与えられます。次にインターフェイスプロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。

- 次の手順に従って、インターフェイスグループに mDNS プロファイルをマッピングします。
  - 1 [Controller] > [Interface Groups] を選択します。
  - 2 対応するインターフェイスグループ名をクリックします。  
[Interface Groups > Edit] ページが表示されます。
  - 3 [mDNS Profile] ドロップダウンリストから、プロファイルを選択します。
- 次の手順に従って、インターフェイスに mDNS プロファイルをマッピングします。
  - 1 [Controller] > [Interfaces] を選択します。

- 2 対応するインターフェイス名をクリックします。  
[Interfaces > Edit] ページが表示されます。
  - 3 [mDNS Profile] ドロップダウン リストから、プロファイルを選択します。
- 次の手順に従って、WLAN に mDNS プロファイルをマッピングします。
    - 1 [WLANs] を選択します。WLAN ID をクリックして、[WLANs > Edit] ページを開きます。
    - 2 対応する WLAN ID をクリックします。  
[WLANs > Edit] ページが表示されます。
    - 3 [Advanced] タブをクリックします。
    - 4 [mDNS Snooping] チェックボックスをオンにします。
    - 5 [mDNS Profile] ドロップダウン リストから、プロファイルを選択します。

## マルチキャスト DNS の設定 (CLI)

- 次のコマンドを入力して、mDNS スヌーピングを設定します。  
**config mdns snooping {enable | disable}**
- 次のコマンドを入力して、mDNS サービスを設定します。  
**config mdns service {{create *service-name service-string origin* {wireless | wired | all} lss {enable | disable} [query] [enable | disable]} | delete *service-name*}**
- 次のコマンドを入力して、mDNS サービスのクエリーを設定します。  
**config mdns service query {enable | disable} *service-name***
- 次のコマンドを入力して、mDNS サービスに対するクエリー間隔を設定します。  
**config mdns query interval *value-in-minutes***
- 次のコマンドを入力して、mDNS プロファイルを設定します。  
**config mdns profile {create | delete} *profile-name***




---

(注) インターフェイスグループ、インターフェイス、または WLAN にすでに関連付けられている mDNS プロファイルを削除しようとする、エラーメッセージが表示されます。

---

- 次のコマンドを入力して、プロファイルに mDNS サービスを設定します。  
**config mdns profile service {add | delete} *profile-name service-name***
- 次のコマンドを入力して、インターフェイスグループに mDNS プロファイルをマッピングします。  
**config interface group mdns-profile {*interface-group-name* | all} {*mdns-profile-name* | none}**



(注) mDNS プロファイル名が **none** である場合、インターフェイスグループにプロファイルは関連付けられません。関連付けられる既存のすべてのプロファイルが削除されます。

- 次のコマンドを入力して、インターフェイスグループに関連付けられた mDNS プロファイルに関する情報を表示します。

```
show interface group detailed interface-group-name
```

- 次のコマンドを入力して、インターフェイスに mDNS プロファイルをマッピングします。

```
config interface mdns-profile {management | {interface-name | all}} {mdns-profile-name | none}
```

- 次のコマンドを入力して、インターフェイスに関連付けられた mDNS プロファイルに関する情報を表示します。

```
show interface detailed interface-name
```

- 次のコマンドを入力して、WLAN に対して mDNS を設定します。

```
config wlan mdns {enable | disable} {wlan-id | all}
```

- 次のコマンドを入力して、WLAN に mDNS プロファイルをマッピングします。

```
config wlan mdns profile {wlan-id | all} {mdns-profile-name | none}
```

- 次のコマンドを入力して、WLAN に関連付けられた mDNS プロファイルに関する情報を表示します。

```
show wlan wlan-id
```

- 次のコマンドを入力して、すべての mDNS プロファイルまたは特定の mDNS プロファイルに関する情報を表示します。

```
show mdns profile {summary | detailed mdns-profile-name}
```

- 次のコマンドを入力して、すべての mDNS サービスまたは特定の mDNS サービスに関する情報を表示します。

```
show mdns service {summary | detailed mdns-service-name}
```

- 次のコマンドを入力して、学習済みの mDNS ドメイン名に関する情報を表示します。

```
show mdns domain-name-ip summary
```

- 次のコマンドを入力して、クライアントの mDNS プロファイルを表示します。

```
show client detail client-mac-address
```

- 次のコマンドを入力して、ネットワークの mDNS の詳細を表示します。

```
show network summary
```

- 次のコマンドを入力して、mDNS サービス データベースを消去します。

```
clear mdns service-database {all | service-name}
```

- 次のコマンドを入力して、mDNS に関連するイベントを表示します。

**debug mdns message {enable | disable}**

- 次のコマンドを入力して、イベントの mDNS の詳細を表示します。

**debug mdns detail {enable | disable}**

- 次のコマンドを入力して、mDNS 処理に関連するエラーを表示します。

**debug mdns error {enable | disable}**

- 次のコマンドを入力して、すべての mDNS 詳細のデバッグを設定します。

**debug mdns all {enable | disable}**

- ロケーション固有サービス関連のコマンド

- このコマンドを入力して、特定の mDNS サービスまたはすべての mDNS サービスのロケーション固有サービスを有効または無効にします。

**config mdns service lss {enable | disable} {service-name | all}**



(注)

デフォルトでは、LSS はディセーブルの状態です。

高可用性への影響: スタンバイ コントローラと同期する必要があります。

- 次のコマンドを入力して、LSS のステータスを表示します。

Summary—**show mdns service summary**

Detailed—**show mdns service detailed service-name**

- 次のコマンドを入力して、HA 関連 mDNS のトラブルシューティングを設定します。

**debug mdns ha {enable | disable}**

- 発信元ベースのサービス検出関連のコマンド

- 次のコマンドを入力して、有線、無線、または両方からのサービスの学習を設定します。

**config mdns service origin {Wireless | Wired | All} {service-name | all}**

LSS が有効である場合は有線サービスを設定することはできません。逆に、有線サービスが設定されている場合に LSS を有効にすることもできません。有線のためのサービス認識元に対して、LSS を有効にすることはできません。

高可用性への影響: スタンバイ コントローラと同期する必要があります。

- 次のコマンドを入力して、発信元ベースのサービス検出のステータスを表示します。

Summary—**show mdns service summary**

Detailed—**show mdns service detailed service-name**

- 次のコマンドを入力して、サービスの学習の制限により、コントローラに存在していても検出されなかったすべてのサービス アドバタイズメントを表示します。

**show mdns service not-learnt**

学習されないすべての VLAN と発信元タイプ間のサービス アドバタイズメントが表示されます。

## • プライオリティ MAC アドレス関連のコマンド

- 次のコマンドを入力して、サービス提供デバイスのサービスごとの MAC アドレスを設定し、サービスプロバイダーのデータベースがフルでも、スヌープおよび検出されることを確認します。

```
config mdns service priority-mac {add | delete} priority-mac-addr service-name ap-group ap-group-name
```

場所の特定のためにオプションの AP グループを有線サービスプロバイダーのデバイスにのみ適用できます。これらのサービスプロバイダーは、他の有線デバイスより優先度が高くなります。

- 次のコマンドを入力して、プライオリティ MAC アドレスのステータスを表示します。  
**Detailed—show mdns service detailed** *service-name*

## • mDNS AP 関連のコマンド

- 次のコマンドを入力して、コントローラに関連付けられた AP 上の mDNS 転送をイネーブルまたはディセーブルにします。

```
config mdns ap {enable | disable} {ap-name | all} vlan vlan-id
```

デフォルトの mDNS AP はありません。VLAN ID はオプション ノードです。

高可用性への影響: 静的設定がスタンバイ コントローラに同期されます。

- 次のコマンドを入力して、AP が mDNS パケットのスヌープおよび転送を実行する VLAN を設定します。

```
config mdns ap vlan {add | delete} vlan-id ap-name
```

- 次のコマンドを入力して、mDNS 転送がイネーブルになっているすべての AP を表示します。

```
show mdns ap summary
```



# 第 13 章

## クライアント ローミングの設定

- [クライアント ローミングについて](#), 137 ページ
- [注意事項および制約事項](#), 140 ページ
- [CCX クライアント ローミング パラメータの設定 \(GUI\)](#), 140 ページ
- [CCX クライアント ローミング パラメータの設定 \(CLI\)](#), 141 ページ
- [CCX クライアント ローミング情報の取得 \(CLI\)](#), 141 ページ
- [CCX クライアント ローミング問題のデバッグ \(CLI\)](#), 142 ページ

### クライアント ローミングについて

Cisco UWN ソリューションは、同じコントローラで管理されている Lightweight アクセス ポイント間、同一サブネット上の同じモビリティ グループに属しているコントローラ間、および異なるサブネット上の同じモビリティ グループに属しているコントローラ間において、シームレスなクライアント ローミングをサポートします。また、コントローラ ソフトウェア リリース 4.1 以降のリリースでは、マルチキャスト パケットでのクライアント ローミングがサポートされています。

GUI または CLI を使用してデフォルトの RF 設定 (RSSI、ヒステリシス、スキャンのしきい値、および遷移時間) を調整することで、クライアント ローミングの動作を微調整できます。

### コントローラ間ローミング

マルチコントローラ展開では、同一モビリティ グループ内および同一サブネット上のコントローラによって管理されるアクセス ポイント間のクライアント ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じ DHCP 割り当てまたはクライアント割り当て IP アドレスを引き続き使用できるため、このローミングもクライアントには透過的に行われます。IP アドレス 0.0.0.0、または自動 IP アドレス 169.254.\*.\* のクライアントが DHCP Discover を送信するか、オペレータが

設定したセッション時間が経過してタイムアウトになると、トンネルが切断され、クライアントの再認証が必要になります。

## コントローラ内ローミング

すべてのコントローラは、同じコントローラで管理されているアクセスポイント間での同一コントローラクライアントローミングをサポートします。セッションはそのまま持続され、クライアントは同じDHCP割り当てまたはクライアント割り当てIPアドレスを引き続き使用するため、このローミングはクライアントには透過的に行われます。コントローラには、リレー機能を備えているDHCP機能があります。同一コントローラローミングは、シングルコントローラ展開とマルチコントローラ展開でサポートされています。

## サブネット間ローミング

同様に、マルチコントローラ展開では、異なるサブネット上の同一モビリティグループ内のコントローラによって管理されるアクセスポイント間のクライアントローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、クライアントは同じDHCP割り当てまたはクライアント割り当てIPアドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。IPアドレス0.0.0.0、または自動IPアドレス169.254.\*.\*のクライアントがDHCP Discoverを送信するか、オペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、クライアントの再認証が必要になります。

## VoIPによる通話ローミング

802.11 Voice-over-IP (VoIP) 通話は、RF 信号が最も強いアソシエーションを見つけ出すことで、最適な Quality of Service (QoS) と最高のスループットを実現します。VoIP 通話には、ローミングハンドオーバーの遅延時間が20ミリ秒以下という最小要件がありますが、Cisco Unified Wireless Network (Cisco UWN) ソリューションならばこの要件を容易に満たすことができます。このソリューションでは、オープン認証が使用されていれば、平均ハンドオーバー遅延時間は5ミリ秒以下です。この短い遅延時間は、個々のアクセスポイントにローミングハンドオーバーのネゴシエートを許可せずにコントローラによって制御されます。

Cisco UWN ソリューションでは、コントローラが同一のモビリティグループに属している場合、異なるサブネット上のコントローラによって管理される lightweight アクセスポイント間での802.11 VoIP 通話ローミングをサポートします。セッションがアクティブである限り、セッションはそのまま持続され、コントローラ間のトンネルによって、VoIP 通話は同じDHCP 割り当て IP アドレスを引き続き使用できるため、このローミングはクライアントには透過的に行われます。VoIP 通話 IP アドレス 0.0.0.0、または VoIP 通話自動 IP アドレス 169.254.\*.\* のクライアントが DHCP Discover を送信するか、オペレータが設定した時間が経過してタイムアウトになると、トンネルが切断され、VoIP クライアントの再認証が必要になります。



## CCX レイヤ2 クライアント ローミング

コントローラでは、次の5つの CCX レイヤ2 クライアント ローミング拡張機能がサポートされています。

- **アクセスポイント経由ローミング**：この機能により、クライアントはスキャン時間を節約できます。CCXv2 クライアントがアクセスポイントにアソシエートする際、新しいアクセスポイントに以前のアクセスポイントの特徴をリストする情報パケットを送信します。各クライアントがアソシエートされていた以前のアクセスポイントと、アソシエーション直後にクライアントに送信（ユニキャスト）されていた以前のアクセスポイントをすべてまとめて作成したアクセスポイントのリストがクライアントによって認識および使用されると、ローミング時間が短縮します。アクセスポイントのリストには、チャンネル、クライアントの現在の SSID をサポートしているネイバーアクセスポイントの BSSID、およびアソシエーション解除以来の経過時間が含まれています。
- **拡張ネイバーリスト**：特に音声アプリケーションを提供する際に、CCXv4 クライアントのローミング能力とネットワークエッジのパフォーマンスを向上させるための機能です。アクセスポイントは、ネイバーリストのユニキャスト更新メッセージを使用して、アソシエートされたクライアントのネイバーに関する情報を提供します。
- **拡張ネイバーリスト要求 (E2E)**：End-2-End 仕様は、音声/ローミング能力の全体的向上のために新しいプロトコルとインターフェイスを定義する、Cisco と Intel の共同プログラムです。これは、CCX 環境の Intel クライアントにのみ適用されます。これにより、Intel クライアントは自由にネイバーリストを要求できるようになります。要求すると、アクセスポイントはコントローラに要求を転送します。コントローラは要求を受信し、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に対するネイバーの現在の CCX ローミングサブリストで応答します。



(注) 特定のクライアントが E2E をサポートするかどうかを調べるには、コントローラの GUI で [Wireless] > [Clients] の順に選択し、そのクライアントの [Detail] リンクをクリックして、[Client Properties] 領域の [E2E Version] テキストボックスを確認します。

- **ローミング理由レポート**：CCXv4 クライアントが新しいアクセスポイントにローミングした理由を報告するための機能です。また、ネットワーク管理者はローミング履歴を作成およびモニタできるようになります。
- **ダイレクトされたローミング要求**：クライアントがアソシエートしているアクセスポイントよりもサービス能力が高いアクセスポイントが他にある場合に、ローミング要求をコントローラからクライアントに送信できるようになります。この場合、コントローラはクライアントに join できる最適なアクセスポイントの一覧を送信します。クライアントはダイレクトされたローミング要求を受け入れることも、無視することもできます。CCX 以外のクライアントおよび CCXv3 以下を実行するクライアントは、どちらの操作も行う必要がありません。この機能を使用するために設定する必要はありません。

## 注意事項および制約事項

- コントローラ ソフトウェア リリース 4.2 以降のリリースでは、CCX バージョン 1 ~ 5 がサポートされます。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。コントローラは、クライアントの CCX バージョンを自身のクライアント データベースに格納します。この情報に基づいて、CCX フレームを生成するとともに、CCX フレームに応答します。これらのローミング拡張機能を使用するには、クライアントで CCXv4 か CCXv5（または、アクセス ポイント経由ローミングの場合 CCXv2）がサポートされている必要があります。

上記に説明するローミング拡張機能は、適切な CCX サポートで自動的に有効化されます。

- スタンドアロンモードでの FlexConnect アクセス ポイントでは、CCX レイヤ 2 ローミングはサポートされません。
- 600 シリーズ アクセス ポイント間のクライアント ローミングはサポートされません。

## CCX クライアント ローミング パラメータの設定（GUI）

- 
- ステップ 1** [[Wireless]> [802.11a/n/ac（または 802.11b/g/n）]> [Client Roaming]]を選択します。[802.11a（802.11b）> Client Roaming] ページが表示されます。
- ステップ 2** クライアント ローミングに影響を与える RF パラメータを調整する場合は、[Mode] ドロップダウン リストから [Custom] を選択し、ステップ 3 に進みます。RF パラメータをデフォルト値のままにする場合は、[Default] を選択して、ステップ 8 に進みます。
- ステップ 3** [Minimum RSSI] テキスト ボックスに、クライアントがアクセス ポイントにアソシエートするときに必要な受信信号強度インジケータ（RSSI）の最小値を入力します。クライアントの平均の受信信号の強度がこのしきい値より低い場合、通常、信頼できる通信はできません。したがって、最小の RSSI 値に達する前に、クライアントはより強い信号のある別のアクセス ポイントをすでに見つけてローミングしている必要があります。
- 範囲は -90 ~ -50 dBm です。
- デフォルトは -85 dBm です。
- ステップ 4** [Hysteresis] テキスト ボックスに、クライアントが近隣のアクセス ポイントにローミングするために必要なアクセス ポイント信号強度を示す値を入力します。このパラメータは、クライアントが 2 つのアクセス ポイント間のボーダー近くに物理的に存在している場合に、アクセス ポイント間のローミングの量を減らすことを意図しています。
- 範囲は 3 ~ 20 dB です。
- デフォルトは 3 dB です。
- ステップ 5** [Scan Threshold] テキスト ボックスに、クライアントが条件の良い別のアクセス ポイントへまだローミングしなくてもよい最小 RSSI を入力します。RSSI が指定された値より低い場合、クライアントは指定遷移時間内により強い信号のあるアクセス ポイントへローミングできる必要があります。このパラメータは

また、クライアントがアクティブまたはパッシブ スキャンで費やす時間を最小限に抑えるための節電方法も提供します。たとえば、クライアントは RSSI がしきい値よりも高いときにはゆっくりとスキャンし、しきい値よりも低いときにはより速くスキャンすることができます。

範囲は -90 ~ -50 dBm です。

デフォルトは -72 dBm です。

**ステップ 6** [Transition Time] テキスト ボックスに、クライアントがアソシエートしているアクセス ポイントからの RSSI がスキャンしきい値を下回ったときに、近隣の適切なアクセス ポイントを見つけてローミングを完了するまでの最大許容時間を入力します。

[Scan Threshold] パラメータと [Transition Time] パラメータは、クライアントのローミング パフォーマンスの最低レベルを保証します。これらのパラメータを使用すると、最も高いクライアント速度とローミング ヒステリシスが得られるだけでなく、アクセス ポイント間の一定の最小オーバーラップ距離を確保することにより、ローミングをサポートする無線 LAN ネットワークを設計することが可能となります。

値の範囲は 1 ~ 5 秒です。

デフォルトは 5 秒です。

**ステップ 7** [Apply] をクリックします。

**ステップ 8** [Save Configuration] をクリックします。

**ステップ 9** 別の無線帯域に対してクライアント ローミングの設定をする場合、この手順を繰り返します。

## CCX クライアント ローミング パラメータの設定 (CLI)

次のコマンドを入力して、CCX レイヤ 2 クライアント ローミング パラメータを設定します。

```
config {802.11a | 802.11b} l2roam rf-params {default | custom min_rssi roam_hyst scan_thresh trans_time}
```

## CCX クライアント ローミング情報の取得 (CLI)

**ステップ 1** 次のコマンドを入力して、802.11a または 802.11b/g ネットワークのクライアント ローミングに対して設定されている現在の RF パラメータを表示します。

```
show {802.11a | 802.11b} l2roam rf-param
```

**ステップ 2** 次のコマンドを入力して、特定のアクセス ポイントに対する CCX レイヤ 2 クライアント ローミング統計を表示します。

```
show {802.11a | 802.11b} l2roam statistics ap_mac
```

このコマンドは、次の情報を提供します。

- 受信したローミング理由レポートの数
- 受信したネイバー リスト要求の数

- 送信したネイバー リスト レポートの数
- 送信したブロードキャスト ネイバー更新の数

**ステップ 3** 次のコマンドを入力して、特定のクライアントのローミング履歴を表示します。

**show client roam-history** *client\_mac*

このコマンドは、次の情報を提供します。

- レポートを受信した時刻
- クライアントが現在アソシエートされているアクセス ポイントの MAC アドレス
- クライアントが以前アソシエートされていたアクセス ポイントの MAC アドレス
- クライアントが以前アソシエートされていたアクセス ポイントのチャンネル
- クライアントが以前アソシエートされていたアクセス ポイントの SSID
- 以前のアクセス ポイントからクライアントがアソシエーション解除した時刻
- クライアントがローミングする理由

---

## CCX クライアント ローミング問題のデバッグ (CLI)

CCX レイヤ 2 クライアント ローミングで問題が発生した場合は、次のコマンドを入力します。

**debug l2roam** [**detail** | **error** | **packet** | **all**] {**enable** | **disable**}



## 第 14 章

# IP-MAC アドレス バインディングの設定

- [IP-MAC アドレス バインディングの設定について](#), 143 ページ
- [IP-MAC アドレス バインディングの設定 \(CLI\)](#), 144 ページ

## IP-MAC アドレス バインディングの設定について

コントローラソフトウェアリリース 5.2 以降のリリースでは、コントローラが、クライアントパケット内で IP アドレスと MAC アドレスの厳密なバインディングを要求します。コントローラは、パケット内の IP アドレスおよび MAC アドレスを確認し、これらのアドレスとコントローラに登録されているアドレスを比較します。パケットは、両方が一致した場合に限り転送されます。以前のリリースでは、クライアントの MAC アドレスだけが確認され、IP アドレスは無視されていました。

アクセス ポイントが 5500 シリーズ コントローラ、2500 シリーズ コントローラ、またはコントローラ ネットワーク モジュールにアソシエートされている場合は、IP-MAC アドレス バインディングを無効にして、そのアクセス ポイントをスニファモードで使用する必要があります。IP-MAC アドレス バインディングを無効にするには、**config network ip-mac-binding disable** を入力します。

アクセス ポイントが 5500 シリーズ コントローラ、2500 シリーズ コントローラ、またはコントローラ ネットワーク モジュールにアソシエートされている場合は、WLAN を有効にして、そのアクセス ポイントをスニファモードで使用する必要があります。WLAN が無効の場合は、アクセス ポイントはパケットを送信できません。



(注) パケットの IP アドレスまたは MAC アドレスがスプーフィングされている場合は検査不合格となり、パケットは破棄されます。スプーフィングされたパケットがコントローラを通過できるのは、IP アドレスと MAC アドレスの両方がスプーフィングされて、同じコントローラ上の別の有効なクライアントのものに変更されている場合だけです。

## IP-MAC アドレス バインディングの設定 (CLI)

**ステップ 1** 次のコマンドを入力して、IP-MAC アドレス バインディングを有効または無効にします。

```
config network ip-mac-binding {enable | disable}
```

デフォルト値はイネーブルです。

(注) Workgroup Bridge (WGB) の背後にルーテッドネットワークが存在する場合は、このバインディング チェックを無効にすることを推奨します。

(注) アクセス ポイントが Cisco 5500 シリーズ コントローラに join している場合に、そのアクセス ポイントを使用するためには、このバインディング 検査を無効にする必要があります。

**ステップ 2** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 3** 次のコマンドを入力して、IP-MAC アドレス バインディングのステータスを表示します。

```
show network summary
```

以下に類似した情報が表示されます。

```
RF-Network Name..... ctrl14404
Web Mode..... Disable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Web Mode Cipher-Option SSLv2..... Disable
...
```

```
IP/MAC Addr Binding Check Enabled
```

```
...<?Line-Break?><?HardReturn?>
```



# 第 15 章

## Quality of Service の設定

---

- [Quality of Service の設定, 145 ページ](#)
- [Quality of Service ロールの設定, 149 ページ](#)

### Quality of Service の設定

#### QoS について

Quality of Service (QoS) とは、選択したネットワークトラフィックにさまざまなテクノロジーに渡る優れたサービスを提供する、ネットワークの機能を意味します。QoS の主要な目的は、専用の帯域幅の確保、ジッタおよび遅延の制御（ある種のリアルタイムトラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。

コントローラでは次の 4 つの QoS レベルがサポートされています。

- **Platinum/音声**：無線を介して転送される音声のために高品質のサービスを保証します。
- **Gold/ビデオ**：高品質のビデオアプリケーションをサポートします。
- **Silver/ベストエフォート**：クライアント用に通常の帯域幅をサポートします。これがデフォルト設定です。
- **Bronze/バックグラウンド**：ゲストサービス用に最低帯域幅を提供します。



---

(注) VoIP クライアントは「Platinum」に設定する必要があります。

---

QoS プロファイルを使用して各 QoS レベルの帯域幅を設定してから、そのプロファイルを WLAN に適用できます。プロファイル設定は、その WLAN にアソシエートされたクライアントに組み込まれます。また、QoS ロールを作成して、通常ユーザとゲストユーザに異なる帯域幅レベルを指定できます。QoS プロファイルと QoS ロールを設定するには、この項の手順に従ってください。

い。QoS プロファイルを WLAN に割り当てるときは、ユニキャストおよびマルチキャスト トラフィックに対して最大およびデフォルトの QoS レベルを定義することもできます。

ワイヤレスレート制限は、アップストリームおよびダウンストリーム トラフィックの両方に定義できます。レート制限は SSID ごとに定義するか、または最大レート制限としてすべてのクライアントに対して指定できます（あるいは両方を行えます）。これらのレート制限は個別に設定できます。

## Quality of Service プロファイルの設定

Platinum、Gold、Silver、および Bronze QoS プロファイルを設定できます。

### QoS プロファイルの設定 (GUI)

- 
- ステップ 1** QoS プロファイルを設定できるように、802.11a および 802.11b/g ネットワークを無効にします。無線ネットワークを無効にするには、[Wireless] > [802.11a/n/ac] (または [802.11b/g/n]) > [Network] の順に選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオフにして、[Apply] をクリックします。
- ステップ 2** [Wireless] > [QoS] > [Profiles] の順に選択して [QoS Profiles] ページを開きます。
- ステップ 3** 設定するプロファイルの名前をクリックして [Edit QoS Profile] ページを開きます。
- ステップ 4** [Description] テキストボックスの内容を変更して、プロファイルの説明を変更します。
- ステップ 5** 次の手順で、ユーザごとのデータ レートを定義します。
- a) [Average Data Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
  - b) [Burst Data Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックのピークデータ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
 

(注) burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレスクライアントとのトラフィックがブロックされることがあります。

バーストデータ レートを設定する前に平均データ レートを設定してください。
  - c) [Average Real-Time Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
 

(注) 平均リアルタイム レートが UDP トラフィック用に使用されているとき、平均データ レートは TCP トラフィックの測定に使用されます。すべてのエントリーに対してキロビット/秒の単位で測定されます。平均データ レートと平均リアルタイム レートは、TCP や UDP などの上位層プロトコルに適用されているので、これらの値は異なる場合があります。これらの異なるレートの値は帯域幅に影響を与えません。



- d) [Burst Real-Time Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックのピークリアルタイムレートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

(注) バーストリアルタイムレートは平均リアルタイムレート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレスクライアントとのトラフィックがブロックされることがあります。

**ステップ 6** 次の手順で、SSID ごとのデータレートを定義します。

- a) [Average Data Rate] テキストボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックの平均データレートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

- b) [Burst Data Rate] テキストボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックのピークデータレートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

(注) burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。

- c) [Average Real-Time Rate] テキストボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックの平均リアルタイムレートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

- d) [Burst Real-Time Rate] テキストボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックのピークリアルタイムレートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

(注) バーストリアルタイムレートは平均リアルタイムレート以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。

**ステップ 7** QoS プロファイルを WLAN に割り当てる場合、ユニキャストおよびマルチキャストトラフィックに対する最大およびデフォルトの QoS レベルを定義します。

- a) [Maximum Priority] ドロップダウンリストから、WLAN 内で AP から任意のステーションに送信される任意のデータフレームに対する最大 QoS 優先度を選択します。

たとえば、ビデオアプリケーションをターゲットにした「gold」という名前の QoS プロファイルでは、デフォルトで最大優先度が video に設定されます。

- b) [Unicast Default Priority] ドロップダウンリストから、WLAN 内で AP から非 WMM ステーションに送信されるユニキャストデータフレームに対する QoS 優先度を選択します。

- c) [Multicast Default Priority] ドロップダウンリストから、WLAN 内で AP からステーションに送信されるマルチキャストデータフレームに対する QoS 優先度を選択します。

(注) 混合 WLAN 内の非 WMM クライアントに対してデフォルトのユニキャスト優先度を使用することはできません。

**ステップ 8** [Protocol Type] ドロップダウンリストから [802.1p] を選択し、[802.1p Tag] テキストボックスに最大優先値を入力して、このプロファイルに該当するパケットに関連付けられる優先タグの最大値 (0 ~ 7) を定義します。

タグが付けられるパケットには、CAPWAP データパケット (アクセスポイントとコントローラの間) や、コアネットワークに向けて送信されるパケットなどがあります。

(注) 802.1p タギングが設定された QoS プロファイルが、コントローラ上のタグ付けなしのインターフェイスを使用する WLAN に割り当てられると、クライアントトラフィックがブロックされま

ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

ステップ 11 802.11 ネットワークを再度有効にします。

無線ネットワークを有効にするには、[Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] の順に選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオンにして、[Apply] をクリックします。

## QoS プロファイルの設定 (CLI)

ステップ 1 次のコマンドを入力して、802.11a および 802.11b/g ネットワークを無効にし、QoS プロファイルを設定できるようにします。

```
config 802.11 {a | b} disable network
```

ステップ 2 次のコマンドを入力して、プロファイルの説明を変更します。

```
config qos description {bronze | silver | gold | platinum} description
```

ステップ 3 このコマンドを入力して、ユーザまたは SSID ごとの TCP トラフィックの平均データ レートを定義します。

```
config qos average-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} rate
```

(注) *rate* パラメータには、0 ~ 512,000 Kbps (両端の値を含む) の値を入力できます。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

ステップ 4 このコマンドを入力して、ユーザまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。

```
config qos burst-data-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} rate
```

ステップ 5 このコマンドを入力して、ユーザまたは SSID ごとの UDP トラフィックの平均リアルタイム データ レートを定義します。

```
config qos average-realtime-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} rate
```

ステップ 6 このコマンドを入力して、ユーザまたは SSID ごとの UDP トラフィックのピーク リアルタイム データ レートを定義します。

```
config qos burst-realtime-rate {bronze | silver | gold | platinum} {per-ssid | per-client} {downstream | upstream} rate
```

ステップ 7 QoS プロファイルを WLAN に割り当てる場合、次のコマンドを入力して、ユニキャストおよびマルチキャストトラフィックに対する最大およびデフォルトの QoS レベルを定義します。

```
config qos priority {bronze | gold | platinum | silver} {maximum priority} {default unicast priority} {default multicast priority}
```

*maximum priority*、*default unicast priority*、および *default multicast priority* パラメータは、次のオプションの中から選択します。

- **besteffort**
- **background**
- **video**
- **voice**

**ステップ 8** 次のコマンドを入力して、このプロファイルに該当するパケットに関連付けられる優先タグの最大値 (0 ~ 7) を定義します。

```
config qos protocol-type {bronze | silver | gold | platinum} dot1p
```

```
config qos dot1p-tag {bronze | silver | gold | platinum} tag
```

タグが付けられるパケットには、CAPWAP データ パケット (アクセス ポイントとコントローラの間) や、コア ネットワークに向けて送信されるパケットなどがあります。

(注) 802.1p タギングは、有線パケットに対してのみ影響します。ワイヤレス パケットは、QoS プロファイルに設定された最大優先レベルによってのみ影響を受けます。

(注) 802.1p タギングが設定された QoS プロファイルが、コントローラ上のタグ付けなしのインターフェイスを使用する WLAN に割り当てられると、クライアントトラフィックがブロックされません。

**ステップ 9** 次のコマンドを入力して、802.11a および 802.11b/g ネットワークを有効にし、QoS プロファイルを設定できるようにします。

```
config 802.11 {a | b} enable network
```

## Quality of Service ロールの設定

### Quality of Service ロールについて

QoS プロファイルを設定して WLAN に適用すると、その WLAN にアソシエートされたクライアントの帯域幅レベルが制限されます。複数の WLAN を同じ QoS プロファイルにマップできますが、通常ユーザ (従業員など) とゲストユーザの間で帯域幅のコンテンションが発生する可能性があります。ゲストユーザが通常ユーザと同じレベルの帯域幅を使用しないようにするには、異なる帯域幅コントラクト (恐らく下位) で QoS ロールを作成して、ゲストユーザに割り当てます。

ゲストユーザ用に最大 10 個の QoS ロールを設定できます。



- (注) RADIUS サーバ上にゲストユーザ用のエントリを作成するように選択し、ゲストユーザをコントローラからローカルユーザデータベースに追加するのではなく、Web 認証が実行される WLAN に対して RADIUS 認証を有効にする場合は、QoS ロールをその RADIUS サーバ自体に割り当てる必要があります。そのためには、「guest-role」Airespace 属性を、データ型「string」、戻り値「11」で RADIUS サーバに追加する必要があります。この属性は、認証の際にコントローラへ送信されます。RADIUS サーバから返された名前付きのロールがコントローラ上で設定されていることが判明した場合は、認証が正常に完了した後に、そのロールへアソシエートされた帯域幅がゲストユーザに対して強制されます。

## QoS ロールの設定

### QoS の設定 (GUI)

- ステップ 1** [Wireless] > [QoS] > [Roles] の順に選択して [QoS Roles for Guest Users] ページを開きます。このページには、ゲストユーザ用の既存の QoS ロールが表示されます。
- (注) QoS ロールを削除するには、そのロールの青いドロップダウン矢印の上にカーソルを置いて [Remove] を選択します。
- ステップ 2** [New] をクリックして新しい QoS ロールを作成します。[QoS Role Name > New] ページが表示されます。
- ステップ 3** [Role Name] テキストボックスに、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意で識別できるように付けてください (Contractor、Vendor、など)。
- ステップ 4** [Apply] をクリックします。
- ステップ 5** QoS ロールの名前をクリックして、QoS ロールの帯域幅を編集します。[Edit QoS Role Data Rates] ページが表示されます。
- (注) ユーザごとの帯域幅コントラクトの設定値の影響を受けるのは、ダウンストリーム方向 (アクセスポイントからワイヤレスクライアントへ) の帯域幅の大きさのみです。アップストリームトラフィック (クライアントからアクセスポイントへ) の帯域幅には影響しません。
- (注) アップストリーム (クライアントからアクセスポイントへ) に対するユーザごとの帯域幅コントラクトをサポートするアクセスポイントは、AP1140、AP1040、AP3500、AP3600、AP1250 および AP1260 です。
- ステップ 6** [Average Data Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックの平均データレートを定義します。0 ~ 60,000Kbps (両端の値を含む) の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。
- ステップ 7** [Burst Data Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックのピークデータレートを定義します。0 ~ 60,000Kbps (両端の値を含む) の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。
- (注) burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレスクライアントとのトラフィックがブロックされることがあります。
- バーストデータレートを設定する前に平均データレートを設定してください。

- ステップ 8** [Average Real-Time Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックの平均リアルタイム レートを定義します。0 ~ 60,000Kbps (両端の値を含む) の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。
- ステップ 9** [Burst Real-Time Rate] テキストボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックのピークリアルタイム レートを定義します。0 ~ 60,000Kbps (両端の値を含む) の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。
- (注) バーストリアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレスクライアントとのトラフィックがブロックされることがあります。
- ステップ 10** [Apply] をクリックします。
- ステップ 11** [Save Configuration] をクリックします。
- ステップ 12** 「コントローラに対するローカルネットワーク ユーザの設定 (GUI)」の項の説明に従って、QoS ロールをゲストユーザに適用します。

## QoS ロールの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、ゲストユーザ用の QoS ロールを作成します。
- ```
config netuser guest-role create role_name
```
- (注) QoS ロールを削除する場合は、**config netuser guest-role delete role_name** コマンドを入力します。
- ステップ 2** 次のコマンドを入力して、QoS ロール用の帯域幅コントラクトを設定します。
- **config netuser guest-role qos data-rate average-data-rate role_name rate** : ユーザごとの TCP トラフィックの平均データ レートを設定します。
 - **config netuser guest-role qos data-rate burst-data-rate role_name rate** : ユーザごとの TCP トラフィックのピーク データ レートを設定します。
- (注) burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレスクライアントとのトラフィックがブロックされることがあります。
- **config netuser guest-role qos data-rate average-realtime-rate role_name rate** : ユーザごとの UDP トラフィックの平均リアルタイム レートを設定します。
 - **config netuser guest-role qos data-rate burst-realtime-rate role_name rate** : ユーザごとの UDP トラフィックのピーク リアルタイム レートを設定します。
- (注) バーストリアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレスクライアントとのトラフィックがブロックされることがあります。

- (注) このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意で識別できるように付けてください (Contractor、Vendor、など)。 *rate* パラメータには、0 ~ 60,000Kbps の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

ステップ 3 次のコマンドを入力して、ゲスト ユーザに QoS ロールを適用します。

config netuser guest-role apply username role_name

たとえば、Contractor のロールをゲスト ユーザ *jsmith* に適用するとします。

- (注) ゲスト ユーザに QoS ロールを割り当てない場合、[User Details] の [Role] テキストボックスには、ロールとして「default」と表示されます。このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されています。
- (注) ゲスト ユーザの QoS ロールの割り当てを解除する場合は、**config netuser guest-role apply username default** コマンドを入力します。今後、このユーザについては WLAN の QoS プロファイルで定義された帯域幅コントラクトが使用されます。

ステップ 4 次のコマンドを入力して、変更を保存します。

save config

ステップ 5 次のコマンドを入力して、現在の QoS ロールとそれらの帯域幅パラメータの一覧を表示します。

show netuser guest-roles

以下に類似した情報が表示されます。

```

Role Name..... Contractor
Average Data Rate..... 10
Burst Data Rate..... 10
Average Realtime Rate..... 100
Burst Realtime Rate..... 100

Role Name..... Vendor
Average Data Rate..... unconfigured
Burst Data Rate..... unconfigured
Average Realtime Rate..... unconfigured
Burst Realtime Rate..... unconfigured

```



第 16 章

Application Visibility and Control の設定

- [Application Visibility and Control](#) について, 153 ページ
- [Application Visibility and Control](#) の制限, 154 ページ
- [Application Visibility and Control](#) の設定 (GUI) , 154 ページ
- [Application Visibility and Control](#) の設定 (CLI) , 156 ページ
- [NetFlow](#) の設定, 157 ページ

Application Visibility and Control について

Application Visibility and Control (AVC) は、ネットワークベースのアプリケーション認識 (NBAR) エンジンによるディープパケットインスペクション技術を使用してアプリケーションを分類し、Wi-Fi ネットワークのアプリケーション レベルの可視性と制御を提供します。アプリケーションが認識されると、AVC 機能によってデータトラフィックをドロップまたはマークできます。

AVC を使用して、1000 以上のアプリケーションを検出できます。AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストの掛かるネットワークリンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成することができるようになります。



(注) UI の [Monitor Summary] セクションで、[Top Applications] に 30 のアプリケーションのリストを表示できます。

AVC コントローラをサポートしているプラットフォームは、Cisco 2500 シリーズワイヤレス LAN コントローラ、Cisco 5500 シリーズワイヤレス LAN コントローラ、中央スイッチングモードの Cisco Flex 7500 シリーズワイヤレス LAN コントローラ、Cisco 8500 シリーズワイヤレス LAN コントローラ、および Cisco Wireless Services Module 2 (WiSM2) です。

AVC DSCP は、コントローラ内の元のパケットの DSCP のみを両方向（アップストリームおよびダウンストリーム）でマークします。これは外部 CAPWAP DCSP には影響しません。アプリケーションが分類された場合にのみ AVC DSCP を適用できます。たとえば、AVC プロファイル設定に基づいて、アプリケーションが ftp または http に分類される場合、対応する DSCP マーキングは

WLAN QoSにかかわらず適用されます。ダウンストリームの場合、外部 CAPWAP ヘッダーの DSCP 値および内部パケットの DSCP が AVC DSCP から取得されます。WLAN QoS は CAPWAP を介した WLC から AP へのすべてのトラフィックに対してのみ適用されます。元のパケットの DSCP は変更されません。

Application Visibility and Control プロトコルパック

プロトコルパックとは、コントローラ ソフトウェアのリリース トレーニング以外のプロトコル アップデートを配布する方法です。コントローラ ソフトウェアを交換せずにコントローラにロードできます。

Application Visibility and Control プロトコルパック (AVC プロトコルパック) は、複数のプロトコル記述言語 (PDL) ファイルとマニフェスト ファイルを含む単一の圧縮ファイルです。必要なプロトコルのセットをロードすることができ、ネットワークでの分類のために追加プロトコルを認識する際に役立ちます。マニフェスト ファイルは、プロトコルパックの名前、バージョン、およびプロトコルパック内の利用可能な PDL の情報など、プロトコルパックに関する情報を提供します。

AVC プロトコルパックは、特定の AVC エンジンバージョン向けにリリースされています。コントローラ プラットフォームのエンジンバージョンがプロトコルパックに必要なバージョン以降であれば、プロトコルパックをロードできます。

Application Visibility and Control の制限

- IPv6 パケットの分類はサポートされていません。
- レイヤ 2 ローミングは、コントローラでサポートされていません。
- マルチキャスト トラフィックはサポートされていません。
- AVC プロトコルパック機能にコントローラ GUI サポートはありません。
- AVC プロトコルパックのダウンロードは Cisco 2500 シリーズ ワイヤレス LAN コントローラではサポートされていません。

Application Visibility and Control の設定 (GUI)

ステップ 1 次の手順に従って、AVC プロファイルを作成して設定します。

- a) [Wireless] > [Application Visibility and Control] > [AVC Profiles] を選択します。
- b) [New] をクリックします。
- c) AVC プロファイル名を入力します。
- d) [Apply] をクリックします。
- e) [AVC Profile Name] ページで、対応する AVC プロファイル名をクリックします。
[AVC Profile > Edit] ページが表示されます。

- f) [Add New Rule] をクリックします。
- g) 各ドロップダウンリストから、アプリケーショングループとアプリケーション名を選択します。
[Wireless] > [Application Visibility and Control] > [AVC Applications] を選択して、使用可能なデフォルト AVC アプリケーションのリストを表示します。
- h) [Action] ドロップダウンリストから、次のいずれかを選択します。
- [Drop] : 選択したアプリケーションに対応するアップストリームパケットとダウンストリームパケットをドロップします。
 - [Mark] : [DSCP (0 to 63)] ドロップダウンリストで指定した DiffServ コードポイント (DSCP) の値を使用して、選択したアプリケーションに対応するアップストリームおよびダウンストリームパケットをマークします。DSCP 値を使用して、QoS レベルに基づいて Differentiated Services を提供できます。
(注) デフォルトアクションでは、すべてのアプリケーションを許可します。
- i) [Action] ドロップダウンリストから [Mark] を選択した場合は、[DSCP (0 to 63)] ドロップダウンリストから DSCP 値を選択します。
DSCP 値はインターネットで QoS を定義するために使用される、パケットヘッダーコードです。DSCP 値は次の QoS レベルにマッピングされます。
- [Platinum (Voice)] : 無線を介して転送される音声のために、高品質のサービスを保証します。
 - [Gold (Video)] : 高品質のビデオアプリケーションをサポートします。
 - [Silver (Best Effort)] : クライアントの通常の帯域幅をサポートします。
 - [Bronze (Background)] : ゲストサービス用の最小の帯域幅を提供します。
- [Custom] を選択して、DSCP 値を指定することもできます。有効値は 0 ~ 63 です。
- j) [Apply] をクリックします。
- k) [Save Configuration] をクリックします。

ステップ 2 次の手順に従って、WLAN に AVC プロファイルを関連付けます。

- a) [WLANs] を選択して対応する WLAN ID をクリックします。
[WLANs > Edit] ページが表示されます。
- b) [QoS] タブをクリックします。
- c) [AVC Profile] ドロップダウンリストから AVC プロファイルを選択します。
- d) [Apply] をクリックします。
- e) [Save Configuration] をクリックします。

Application Visibility and Control の設定 (CLI)

- 次のコマンドを入力して、AVC プロファイルを作成または削除します。

```
config avc profile avc-profile-name {create | delete}
```

- 次のコマンドを入力して、AVC プロファイルのルールを追加します。

```
config avc profile avc-profile-name rule add application application-name {drop | mark dscp-value | ratelimit Average Ratelimit value Burst Ratelimit value}
```

- 次のコマンドを入力して、AVC プロファイルのルールを排除します。

```
config avc profile avc-profile-name rule remove application application-name
```

- 次のコマンドを入力して、WLAN に AVC プロファイルを設定します。

```
config wlan avc wlan-id profile avc-profile-name {enable | disable}
```

- 次のコマンドを入力して、WLAN に対してアプリケーション可視性を設定します。

```
config wlan avc wlan-id visibility {enable | disable}
```



(注) アプリケーションの可視性は、AVC プロファイルのサブセットです。このため、WLAN に AVC プロファイルを設定すると、可視性が自動的に有効になります。

- 次のコマンドを入力して、コントローラに AVC プロトコルパックをダウンロードします。

```
1 transfer download datatype avc-protocol-pack
```

```
2 transfer download start
```

- 次のコマンドを入力して、すべての AVC プロファイルまたは特定の AVC プロファイルに関する情報を表示します。

```
show avc profile {summary | detailed avc-profile-name}
```

- 次のコマンドを入力して、AVC アプリケーションに関する情報を表示します。

```
show avc applications [application-group]
```

- 次のコマンドを入力して、AVC の各種統計情報を表示します。

```
show avc statistics
```

- 次のコマンドを入力して、コントローラで使用するプロトコルパックを表示します。

```
show avc protocol-pack version
```

- 次のコマンドを入力して、AVC エンジンのバージョン情報を表示します。

```
show avc engine version
```

- 次のコマンドを入力して、AVC イベントのトラブルシューティングを設定します。

```
debug avc events {enable | disable}
```

- 次のコマンドを入力して、AVC エラーのトラブルシューティングを設定します。

```
debug avc error {enable | disable}
```

NetFlow の設定

NetFlow 情報

NetFlow は、ネットワーク ユーザとアプリケーション、ピーク時の使用時間、およびトラフィック ルーティングに関する情報を提供するプロトコルです。NetFlow プロトコルはネットワーク デバイスから IP トラフィック情報を収集して、トラフィックをモニタします。NetFlow アーキテクチャは、次のコンポーネントで構成されています。

- コレクタ：さまざまなネットワーク要素からすべての IP トラフィックの情報を収集するエンティティ。
- エクスポート：IP トラフィック情報とともにテンプレートをエクスポートするネットワーク エンティティ。コントローラは、エクスポートとして機能します。

NetFlow の設定 (GUI)

ステップ 1 次の手順に従って、エクスポートを設定します。

- [Wireless] > [Netflow] > [Exporter] を選択します。
- [New] をクリックします。
- エクスポート名、IP アドレス、およびポート番号を入力します。
ポート番号の有効範囲は 1~65535 です。
- [Apply] をクリックします。
- [Save Configuration] をクリックします。

ステップ 2 次の手順に従って、NetFlow モニタを設定します。

- [Wireless] > [Netflow] > [Monitor] を選択します。
- [New] をクリックして、モニタ名を入力します。
- [Monitor List] ページで、モニタ名をクリックし、[Netflow Monitor > Edit] ページを開きます。
- 各ドロップダウン リストからエクスポート名とレコード名を選択します。
- [Apply] をクリックします。
- [Save Configuration] をクリックします。

ステップ 3 次の手順に従って、WLAN に NetFlow モニタを関連付けます。

- [WLANs] を選択し、[WLAN ID] をクリックして、[WLANs > Edit] ページを開きます。
- [QoS] タブで、NetFlow モニタのドロップダウン リストから NetFlow モニタを選択します。
- [Apply] をクリックします。

- d) [Save Configuration] をクリックします。
-

NetFlow の設定 (CLI)

- 次のコマンドを入力して、エクスポートを作成します。
config flow create exporter *exporter-name ip-addr port-number*
- 次のコマンドを入力して、NetFlow モニタを作成します。
config flow create monitor *monitor-name*
- 次のコマンドを使用して、NetFlow モニタをエクスポートに関連付けるか、関連付けを解除します。
config flow {add | delete} monitor *monitor-name exporter exporter-name*
- 次のコマンドを使用して、NetFlow モニタをレコードに関連付けるか、関連付けを解除します。
config flow {add | delete} monitor *monitor-name record ipv4_client_app_flow_record*
- 次のコマンドを使用して、NetFlow モニタを WLAN に関連付けるか、関連付けを解除します。
config wlan flow *wlan-id monitor monitor-name {enable | disable}*
- 次のコマンドを入力して、NetFlow モニタの概要を表示します。
show flow monitor summary
- 次のコマンドを入力して、エクスポートに関する情報を表示します。
show flow exporter {summary | statistics}
- 次のコマンドを入力して、NetFlow のデバッグを設定します。
debug flow {detail | error | info} {enable | disable}



第 17 章

メディアおよび EDCA パラメータの設定

- [音声パラメータとビデオパラメータの設定, 159 ページ](#)
- [SIP ベースの CAC の設定, 173 ページ](#)
- [メディアパラメータの設定, 175 ページ](#)
- [優先コール番号を使用した音声優先制御の設定, 176 ページ](#)
- [EDCA パラメータの設定, 177 ページ](#)

音声パラメータとビデオパラメータの設定

音声パラメータとビデオパラメータの設定について

コントローラには、音声またはビデオ、あるいはその両方の品質に影響を及ぼす次の3つのパラメータがあります。

- Call admission control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

これらのパラメータはそれぞれ、Cisco Compatible Extensions (CCX) v4およびv5でサポートされています。



(注) 音声の品質に関する問題の監視およびレポートには、Traffic Stream Metrics (TSM) を使用します。

コールアドミッション制御

コールアドミッション制御 (CAC) を使用すると、無線 LAN で輻輳が発生したときに、アクセスポイントは制御された Quality of Service (QoS) を維持できます。CCX v3 で展開される Wi-Fi Multimedia (WMM) プロトコルにより、無線 LAN に輻輳が発生しない限り十分な QoS が保証されます。ただし、ネットワークの負荷が変化するとき QoS を維持するには、CCX v4 の CAC が必要です。帯域幅ベースの CAC と負荷ベース CAC の CAC という 2 種類の CAC が使用できます。

帯域幅ベースの CAC

帯域幅ベースまたは静的な CAC を使用すると、クライアントで新しいコールを受け入れるために必要な帯域幅または共有メディア時間を指定できます。その結果としてアクセスポイントでは、この特定のコールに対応する能力があるかどうかを決定できます。アクセスポイントでは、許容される品質でコールの最大数を維持するために、必要であればコールを拒否します。

WLAN の QoS 設定により、帯域幅ベースの CAC サポートのレベルが決定します。音声アプリケーションで帯域幅ベースの CAC を使用するには、WLAN を Platinum QoS に対して設定する必要があります。ビデオアプリケーションで帯域幅ベースの CAC を使用するには、WLAN を Gold QoS に対して設定する必要があります。さらに、WMM が WLAN に対して有効化されているのを確認します。QoS と WMM の設定の手順については、「[802.3 ブリッジの設定について](#)、(119 ページ)」の項を参照してください。



(注) WMM が有効化されている CCX v4 クライアントに対して Admission Control (ACM; アドミッションコントロール) を有効にする必要があります。そうしない場合、帯域幅ベースの CAC は適切に動作しません。

負荷ベース CAC

負荷ベース CAC では、音声アプリケーションに関して帯域幅を消費するすべてのトラフィックの種類 (クライアントからのトラフィックなど)、同じチャネルのアクセスポイントの負荷、および同じ場所に設置されたチャネルの干渉を考慮した測定方法を取り入れます。負荷ベース CAC では、PHY およびチャネル欠陥の結果発生する追加の帯域幅消費も対象となります。

負荷ベース CAC では、アクセスポイントは RF チャネルの使用状況 (つまり、消費された帯域幅の割合)、チャネル干渉、およびアクセスポイントで許可される追加コールを継続的に測定し、更新します。アクセスポイントは、コールをサポートするのに十分なだけの未使用帯域幅がチャネルにある場合に限り、新規のコールを許可します。このようにすることで、負荷ベース CAC は、チャネルのオーバーサブスクリプションを防ぎ、WLAN の負荷および干渉のあらゆる状況下で QoS を維持します。



(注) 負荷ベース CAC は Lightweight アクセスポイントでのみサポートされています。負荷ベース CAC を無効にすると、アクセスポイントが帯域幅ベースの CAC を使用するようになります。

Expedited Bandwidth Requests

Expedited Bandwidth Request 機能を使用すると、CCXv5 クライアントは WLAN への緊急の WMM Traffic Specifications (TSPEC) 要求 (e911 コールなど) を示すことができるようになります。コントローラがこの要求を受信すると、コントローラは、処理中の他の TSPEC コールの質を変えることなく、緊急のコールに対応しようとします。

Expedited Bandwidth Requests は、帯域幅ベースの CAC と load-based の CAC の両方に適用できません。Expedited Bandwidth Requests はデフォルトでは無効になっています。この機能が無効の場合、コントローラはすべての緊急の要求を無視し、TSPEC 要求は通常の TSPEC 要求として処理します。

この表に、通常の TSPEC 要求と Expedited Bandwidth Requests の TSPEC 要求処理の例を示します。

表 4: TSPEC 要求処理の例

CAC モード	音声コールに予約された帯域幅 ¹	用途 ²	通常の TSPEC 要求	緊急 TSPEC 帯域幅要求
帯域幅ベースの CAC	75% (デフォルト設定)	75% 未満	許可	許可
		75% ~ 90% (音声コール用に予約された帯域幅が消費される)	拒否	許可
		90% 以上	拒否	拒否
負荷ベース CAC		75% 未満	許可	許可
		75% ~ 85% (音声コール用に予約された帯域幅が消費される)	拒否	許可
		85% 以上	拒否	拒否

¹ 帯域幅ベースの CAC の場合、音声コールの帯域幅利用率はアクセスポイント単位となり、同じチャンネルのアクセスポイントは考慮されません。load-based の CAC の場合、音声コールの帯域幅利用率は、チャンネル全体に対して測定されます。

² 帯域幅ベースの CAC (音声およびビデオに消費された帯域幅) または load-based の CAC (チャンネル利用率 [Pb])



(注) TSPEC g711-40ms コーデック タイプのアドミッション制御がサポートされます。



(注) ビデオ ACM が有効になっている場合、TSPEC 内の非 MSDU サイズが 149 より大きい、または平均データ レートが 1 Kbps よりも大きいと、コントローラがビデオ TSPEC を拒否します。

U-APSD

Unscheduled automatic power save delivery (U-APSD) は、モバイルクライアントのバッテリー寿命を延ばす IEEE 802.11e で定義されている QoS 機能です。バッテリー寿命を延ばすだけでなく、この機能は無線メディアで配送されるトラフィック フローの遅延時間を短縮します。U-APSD は、アクセス ポイントでバッファされる個々のパケットをポーリングするようにクライアントに要求するため、単一のアップリンク トリガー パケットを送信することにより、複数のダウンリンク パケットの送信が許可されます。WMM が有効化されると、U-APSD は自動的に有効化されます。

Traffic Stream Metrics

voice-over-wireless LAN (VoWLAN) 展開では、クライアントとアクセス ポイント間のエア インターフェイスでの音声関連のメトリクスの測定には、Traffic Stream Metrics (TSM) が使用されます。TSM ではパケット遅延とパケット損失の両方がレポートされます。これらのレポートを調べることにより、劣悪な音声品質の問題を分離できます。

このメトリクスは、CCX v4 以降のリリースをサポートするアクセス ポイントとクライアント デバイス間のアップリンク (クライアント側) 統計とダウンリンク (アクセス ポイント側) 統計の集合から成ります。クライアントが CCX v4 または CCXv5 に準拠していない場合、ダウンリンク 統計のみが取得されます。クライアントとアクセス ポイントで、これらのメトリクスが測定されます。アクセス ポイントではまた、5 秒おきに測定値が収集されて、90 秒のレポートが作成された後、レポートがコントローラに送信されます。コントローラは、アップリンクの測定値はクライアント単位で保持し、ダウンリンクの測定値はアクセス ポイント単位で保持します。履歴データは 1 時間分を保持します。このデータを格納するには、アップリンク メトリクス用に 32MB、ダウンリンク メトリクス用に 4.8MB の追加のメモリがコントローラに必要です。

無線帯域別ベースで (たとえば、すべての 802.11a ラジオ)、GUI または CLI により TSM を設定できます。コントローラは、リポート後も持続するように、フラッシュメモリに設定を保存します。アクセス ポイントにより、コントローラからの設定が受信された後、指定された無線帯域で TSM が有効化されます。



(注) アクセス ポイントでは、ローカルモードと FlexConnect モードの両方で TSM エントリがサポートされます。

この表に、別のコントローラ シリーズでの TSM エントリの上限を示します。

TSM エントリ	5500	7500
最大 AP TSM エントリ数	100	100
最大クライアント TSM エントリ数	250	250

TSM エントリ	5500	7500
最大 TSM エントリ数	100*250=25000	100*250=25000



(注) 上限に到達すると、追加の TSM エントリを保存し、Cisco Prime Infrastructure に送信することができなくなります。クライアント TSM エントリが満杯で、AP TSM エントリにまだ空きがある場合、AP エントリのみが保存されます（逆もまた同様）。これにより、出力が不完全になります。TSM クリーンアップは、1 時間ごとに行われます。エントリは、対応する AP とクライアントがシステム内に存在しない場合にのみ削除されます。

音声パラメータの設定

音声パラメータの設定 (GUI)

- ステップ 1** WMM と Platinum QoS レベルに対して WLAN が設定されていることを確認してください。
- ステップ 2** WMM が有効になっている WLAN をすべて無効にして、[Apply] をクリックします。
- ステップ 3** [Wireless] を選択してから [802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオフにし、[Apply] をクリックして無線ネットワークを無効にします。
- ステップ 4** [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Media] の順に選択します。[802.11a (または 802.11b) > Media] ページが表示されます。デフォルトで [Voice] タブが表示されます。
- ステップ 5** この無線帯域で帯域幅ベースの CAC を有効にするには、[Admission Control (ACM)] チェックボックスをオンにします。デフォルト値はディセーブルです。
- ステップ 6** 次の選択肢の中から使用する [Admission Control (ACM)] を選択します。
- [Load-based] : チャネルベースの CAC を有効にします。これがデフォルトのオプションです。
 - [Static] : 無線ベースの CAC を有効にします。
- ステップ 7** [Max RF Bandwidth] テキストボックスに、この無線帯域で音声アプリケーション用にクライアントに割り当てられる最大帯域幅の割合を入力します。指定された値に達すると、アクセスポイントはこの無線帯域での新しいコールを拒否します。範囲は 5 ~ 85% です。音声とビデオが最大帯域幅に占める割合の合計が 85% を超えることはできません。デフォルトは 75% です。

- ステップ 8** [Reserved Roaming Bandwidth] テキストボックスに、ローミングする音声クライアント用に割り当てられる最大帯域幅の割合を入力します。コントローラは、割り当てられた最大帯域幅のうち、この割合の帯域幅をローミングする音声クライアント用に予約します。
範囲は 0 ~ 25% です。
デフォルトは 6% です。
- ステップ 9** Expedited Bandwidth Requests を有効にするには、[Expedited Bandwidth] チェックボックスをオンにします。デフォルトでは、このチェックボックスは無効になっています。
- ステップ 10** SIP CAC サポートを有効にするには、[SIP CAC Support] チェックボックスをオンにします。デフォルトでは、SIP CAC サポートは無効になっています。
- ステップ 11** [SIP Codec] ドロップダウンリストから、次のいずれかのオプションを選択してコーデック名を設定します。デフォルト値は [G.711] です。オプションは次のとおりです。
- User Defined
 - G.711
 - G.729
- ステップ 12** [SIP Bandwidth (kbps)] テキストボックスに、キロビット/秒の単位で帯域幅を入力します。有効な範囲は 8 ~ 64 です。
デフォルト値は 64 です。
- (注) [SIP Bandwidth (kbps)] テキストボックスは、SIP コーデックに [User-Defined] を選択した場合にのみ強調表示されます。SIP コーデックに [G.711] を選択すると、[SIP Bandwidth (kbps)] テキストボックスに 64 が設定されます。SIP コーデックに [G.729] を選択すると、[SIP Bandwidth (kbps)] テキストボックスに 8 が設定されます。
- ステップ 13** [SIP Voice Sample Interval (msecs)] テキストボックスに、サンプルインターバルの値を入力します。
- ステップ 14** [Maximum Calls] テキストボックスに、この無線で実行可能なコールの最大数を入力します。最大コール数の制限には、直接コールとローミングインコールの両方が含まれます。最大コール制限に達すると、新規またはローミングコールは失敗します。
有効な範囲は 0 ~ 25 です。
デフォルト値は 0 です。この場合、最大コール数の制限はチェックされません。
- (注) SIP CAC がサポートされていて、CAC 方式が [Static] の場合、[Maximum Possible Voice Calls] フィールドと [Maximum Possible Roaming Reserved Calls] フィールドが表示されます。

- ステップ 15** [Metrics Collection] チェックボックスをオンにして、トラフィックストリームメトリックを収集します。デフォルトでは、このボックスはオフになっています。つまり、トラフィックストリームメトリックは、デフォルトでは収集されません。
- ステップ 16** [Apply] をクリックします。
- ステップ 17** すべての WMM WLAN を有効にし、[Apply] をクリックします。
- ステップ 18** [802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオンにし、[Apply] をクリックして無線ネットワークを再度有効にします。
- ステップ 19** [Save Configuration] をクリックします。
- ステップ 20** 別の無線帯域に対して音声パラメータを設定する場合は、この手順を繰り返します。

音声パラメータの設定 (CLI)

はじめる前に

SIP ベースの CAC が設定されていることを確認します。

- ステップ 1** 次のコマンドを入力して、コントローラ上に設定されているすべての WLAN を表示します。
show wlan summary
- ステップ 2** 次のコマンドを入力して、変更を行う WLAN が WMM に対して設定されており、QoS レベルが Platinum に設定されていることを確認します。
show wlan wlan_id
- ステップ 3** 次のコマンドを入力して、音声パラメータの変更前に、WMM が有効になっている WLAN をすべて無効にします。
config wlan disable wlan_id
- ステップ 4** 次のコマンドを入力して、無線ネットワークを無効にします。
config {802.11a | 802.11b} disable network
- ステップ 5** 次のコマンドを入力して、設定を保存します。
save config
- ステップ 6** 次のコマンドを入力して、802.11a または 802.11b/g ネットワークに対する帯域幅ベースの音声 CAC を有効または無効にします。
config {802.11a | 802.11b} cac voice acm {enable | disable}
- ステップ 7** 次のコマンドを入力して、802.11a または 802.11b/g ネットワーク上で音声アプリケーション用にクライアントに割り当てられた最大帯域幅の割合を設定します。
config {802.11a | 802.11b} cac voice max-bandwidth bandwidth
- bandwidth* の範囲は 5 ~ 85 % で、デフォルト値は 75 % です。クライアントが指定値に達すると、このネットワーク上での新しいコールはアクセスポイントで拒否されます。

ステップ 8 次のコマンドを入力して、ローミングする音声クライアント用に割り当てられている最大帯域幅の割合を設定します。

```
config {802.11a | 802.11b} cac voice roam-bandwidth bandwidth
```

bandwidth の範囲は 0 ~ 25% で、デフォルト値は 6% です。コントローラは、割り当てられた最大帯域幅のうち、この割合の帯域幅をローミングする音声クライアント用に予約します。

ステップ 9 次のコマンドを入力して、コーデック名とサンプルインターバルをパラメータで設定し、コールあたりの必要な帯域幅を計算するようにします。

```
config {802.11a | 802.11b} cac voice sip codec {g711 | g729} sample-interval number_msecs
```

ステップ 10 次のコマンドを入力して、1 コールに必要な帯域幅を設定します。

```
config {802.11a | 802.11b} cac voice sip bandwidth bandwidth_kbps sample-interval number_msecs
```

ステップ 11 次のコマンドを入力して、WMM が有効になっている WLAN をすべて有効にします。

```
config wlan enable wlan_id
```

ステップ 12 次のコマンドを入力して、無線ネットワークを有効にします。

```
config {802.11a | 802.11b} enable network
```

ステップ 13 次のコマンドを入力して、TSM 音声メトリックを表示します。

```
show [802.11a | 802.11b] cu-metrics AP_Name
```

このコマンドでは、チャンネル使用率メトリックも表示されます。

ステップ 14 `save config` コマンドを入力して、設定を保存します。

ビデオパラメータの設定

ビデオパラメータの設定 (GUI)

ステップ 1 WMM と Gold QoS レベルに対して WLAN が設定されていることを確認してください。

ステップ 2 WMM が有効になっている WLAN をすべて無効にして、[Apply] をクリックします。

ステップ 3 [Wireless] を選択してから [802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオフにし、[Apply] をクリックして無線ネットワークを無効にします。

ステップ 4 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Media] を選択します。[802.11a (または 802.11b) > Media] ページが表示されます。

ステップ 5 [Video] タブで、[Admission Control (ACM)] チェックボックスをオンにして、この無線帯域のビデオ CAC を有効にします。デフォルト値はディセーブルです。

ステップ 6 [CAC Method] ドロップダウンリストで、[Static] および [Load Based] の方式から選択します。静的な CAC 方式は無線に基づいており、負荷ベースの CAC 方式はチャンネルに基づきます。

(注) ビデオ通話用の TSpec ベースおよび SIP ベースの CAC の場合は、静的な方式のみがサポートされます。

- ステップ 7** [Max RF Bandwidth] テキスト ボックスに、この無線帯域でビデオアプリケーション用にクライアントに割り当てられる最大帯域幅の割合を入力します。指定された値に達すると、アクセス ポイントはこの無線帯域での新しい要求を拒否します。
範囲は 5 ~ 85% です。音声とビデオが最大帯域幅に占める割合の合計が 85% を超えることはできません。デフォルトは 0% です。
- ステップ 8** [Reserved Roaming Bandwidth] テキスト ボックスに、ビデオのローミングクライアント用に予約される最大 RF 帯域幅の割合を入力します。
- ステップ 9** [SIP CAC Support] チェックボックスをオンまたはオフにして、SIP CAC サポートを設定します。SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。
- (注) 負荷ベースの CAC 方式を選択した場合は、SIP CAC を有効にできません。
- ステップ 10** [Apply] をクリックします。
- ステップ 11** すべての WMM WLAN を有効にし、[Apply] をクリックします。
- ステップ 12** [802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオンにし、[Apply] をクリックして無線ネットワークを再度有効にします。
- ステップ 13** [Save Configuration] をクリックします。
- ステップ 14** 別の無線帯域に対してビデオパラメータを設定する場合は、この手順を繰り返します。

ビデオパラメータの設定 (CLI)

はじめる前に

SIP ベースの CAC が設定されていることを確認します。

- ステップ 1** 次のコマンドを入力して、コントローラ上に設定されているすべての WLAN を表示します。
show wlan summary
- ステップ 2** 次のコマンドを入力して、変更を行う WLAN が WMM に対して設定されており、QoS レベルが Gold に設定されていることを確認します。
show wlan wlan_id
- ステップ 3** 次のコマンドを入力して、ビデオパラメータの変更前に、WMM が有効になっている WLAN をすべて無効にします。
config wlan disable wlan_id
- ステップ 4** 次のコマンドを入力して、無線ネットワークを無効にします。
config {802.11a | 802.11b} disable network

- ステップ 5** 次のコマンドを入力して、設定を保存します。
save config
- ステップ 6** 次のコマンドを入力して、802.11a または 802.11b/g ネットワークに対するビデオ CAC を有効または無効にします。
config {802.11a | 802.11b} cac video acm {enable | disable}
- ステップ 7** 静的または負荷ベースとして CAC 方式を設定するには、次のコマンドを入力します。
config {802.11a | 802.11b} cac video cac-method {static | load-based}
- ステップ 8** 次のコマンドを入力して、802.11a または 802.11b/g ネットワーク上でビデオアプリケーション用にクライアントに割り当てられている最大帯域幅の割合を設定します。
config {802.11a | 802.11b} cac video max-bandwidth bandwidth
- bandwidth* の範囲は 5 ~ 85 % で、デフォルト値は 5 % です。ただし、音声とビデオを加算した最大 RF 帯域幅が 85 % を超えてはなりません。クライアントが指定値に達すると、このネットワーク上での新しいコールはアクセス ポイントで拒否されます。
- (注) このパラメータがゼロ (0) に設定されている場合、コントローラは、帯域割り当てが行われなものと想定して、すべての帯域幅の要求を許可します。
- ステップ 9** ビデオのローミングクライアントに予約されている最大 RF 帯域幅の割合を設定するには、次のコマンドを入力します。
config {802.11a | 802.11b} cac video roam-bandwidth bandwidth
- ステップ 10** SIP ベースのビデオ通話用の CAC パラメータを設定するには、次のコマンドを入力します。
config {802.11a | 802.11b} cac video sip {enable | disable}
- ステップ 11** 次のコマンドを入力して、アクセス ポイントから受信した TSPEC 無活動タイムアウトを処理または無視します。
config {802.11a | 802.11b} cac video tspec-inactivity-timeout {enable | ignore}
- ステップ 12** 次のコマンドを入力して、WMM が有効になっている WLAN をすべて有効にします。
config wlan enable wlan_id
- ステップ 13** 次のコマンドを入力して、無線ネットワークを有効にします。
config {802.11a | 802.11b} enable network
- ステップ 14** **save config** コマンドを入力して、設定を保存します。

音声設定とビデオ設定の表示

音声設定とビデオ設定の表示 (GUI)

- ステップ 1** [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。
- ステップ 2** 目的のクライアントの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。

このページでは、このクライアントの U-APSD ステータス（有効になっている場合）が [Quality of Service Properties] の下に表示されます。

ステップ 3 [Clients] ページに戻るには、[Back] をクリックします。

ステップ 4 次の手順に従って、特定のクライアントと、この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に対する TSM 統計を表示します。

a) カーソルを目的のクライアントの青のドロップダウン矢印の上に置いて、[802.11aTSM] または [802.11b/g TSM] を選択します。[Clients > AP] ページが表示されます。

b) 目的のアクセスポイントの [Detail] リンクをクリックして [Clients > AP > Traffic Stream Metrics] ページを開きます。

このページには、このクライアントと、この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の TSM 統計が表示されます。統計は、90 秒間隔で表示されます。[timestamp] テキストボックスには、統計が収集された期間が表示されます。

ステップ 5 次の手順に従って、特定のアクセスポイントと、このアクセスポイントにアソシエートされている特定のクライアントに対する TSM 統計を表示します。

a) [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] を選択します。[802.11a/n/ac Radios] ページまたは [802.11b/g/n Radios] ページが表示されます。

b) カーソルを目的のアクセスポイントの青のドロップダウン矢印の上に置いて、[802.11aTSM] または [802.11b/g TSM] を選択します。[AP > Clients] ページが表示されます。

c) 目的のクライアントの [Detail] リンクをクリックして [AP > Clients > Traffic Stream Metrics] ページを開きます。

このページには、このアクセスポイントと、この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の TSM 統計が表示されます。統計は、90 秒間隔で表示されます。[timestamp] テキストボックスには、統計が収集された期間が表示されます。

音声設定とビデオ設定の表示 (CLI)

ステップ 1 次のコマンドを入力して、802.11 ネットワークの CAC 設定を表示します。
show ap stats {802.11a | 802.11b}

ステップ 2 次のコマンドを入力して、特定のアクセスポイントの CAC 統計を表示します。
show ap stats {802.11a | 802.11b} ap_name

以下に類似した情報が表示されます。

```
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)..... 0
Total channel MT free..... 0
Total voice MT free..... 0
Na Direct..... 0
```

```

Na Roam..... 0
  Video Bandwidth in use(% of config bw)..... 0
  Total num of voice calls in progress..... 0
  Num of roaming voice calls in progress..... 0
  Total Num of voice calls since AP joined..... 0
  Total Num of roaming calls since AP joined..... 0
Total Num of exp bw requests received..... 5
  Total Num of exp bw requests admitted..... 2

Num of voice calls rejected since AP joined..... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficient bw....0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate..... 0
  Num of calls rejected due to QoS policy..... 0

```

この例では、「MT」はメディア時間、「Na」は追加コールの数、「exp bw」は緊急用帯域幅です。

(注) 音声クライアントがアクティブコールのときに、そのアソシエート先の AP でリポートが必要になったとします。AP がリポートされた後も、そのコールはクライアントで維持され続けます。また、その AP がダウンしている間、コントローラによってデータベースが更新されることはありません。そのため、AP がダウン状態になる前に、すべてのアクティブコールを終了させることをお勧めします。

ステップ 3 次のコマンドを入力して、特定のクライアントの U-APSD ステータスを表示します。

```
show client detail client_mac
```

ステップ 4 次のコマンドを入力して、特定のクライアントと、この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に対する TSM 統計を表示します。

```
show client tsm {802.11a | 802.11b} client_mac {ap_mac | all}
```

オプションの **all** コマンドは、このクライアントがアソシエートされているすべてのアクセスポイントを表示します。以下に類似した情報が表示されます。

```

Client Interface Mac:          00:01:02:03:04:05
Measurement Duration:         90 seconds

Timestamp                      1st Jan 2006, 06:35:80
UpLink Stats
=====
  Average Delay (5sec intervals).....35
  Delay less than 10 ms.....20
  Delay bet 10 - 20 ms.....20
  Delay bet 20 - 40 ms.....20
  Delay greater than 40 ms.....20
Total packet Count.....80
Total packet lost count (5sec).....10
Maximum Lost Packet count(5sec).....5
Average Lost Packet count(5secs).....2
DownLink Stats
=====
  Average Delay (5sec intervals).....35

```



```

Delay less than 10 ms.....20
Delay bet 10 - 20 ms.....20
Delay bet 20 - 40 ms.....20
Delay greater than 40 ms.....20
Total packet Count.....80
Total packet lost count (5sec).....10
Maximum Lost Packet count(5sec).....5
Average Lost Packet count(5secs).....2

```

(注) 統計は、90秒間隔で表示されます。[timestamp]テキストボックスには、統計が収集された期間が表示されます。

(注) **clear client tsm {802.11a | 802.11b} client_mac {ap_mac | all}** コマンドを入力して、特定のアクセスポイント、またはクライアントがアソシエートされているすべてのアクセスポイントのTSM統計情報をクリアします。

ステップ5 次のコマンドを入力して、特定のアクセスポイントと、このアクセスポイントにアソシエートされている特定のクライアントに対するTSM統計を表示します。

show ap stats {802.11a | 802.11b} ap_name tsm {client_mac | all}

オプションの **all** コマンドは、このアクセスポイントにアソシエートされているすべてのクライアントを表示します。以下に類似した情報が表示されます。

```

AP Interface Mac:          00:0b:85:01:02:03
Client Interface Mac:     00:01:02:03:04:05
Measurement Duration:     90 seconds

```

```

Timestamp                  1st Jan 2006, 06:35:80
UpLink Stats
=====
Average Delay (5sec intervals).....35
Delay less than 10 ms.....20
Delay bet 10 - 20 ms.....20
Delay bet 20 - 40 ms.....20
Delay greater than 40 ms.....20
Total packet Count.....80
Total packet lost count (5sec).....10
Maximum Lost Packet count(5sec).....5
Average Lost Packet count(5secs).....2
DownLink Stats
=====
Average Delay (5sec intervals).....35
Delay less than 10 ms.....20
Delay bet 10 - 20 ms.....20
Delay bet 20 - 40 ms.....20
Delay greater than 40 ms.....20
Total packet Count.....80
Total packet lost count (5sec).....10
Maximum Lost Packet count(5sec).....5
Average Lost Packet count(5secs).....2

```

(注) 統計は、90秒間隔で表示されます。[timestamp]テキストボックスには、統計が収集された期間が表示されます。

ステップ 6 次のコマンドを入力して、コールアドミッション制御（CAC）のメッセージ、イベント、またはパケットのデバッグを有効または無効にします。

```
debug cac {all | event | packet} {enable | disable}
```

all はすべての CAC メッセージのデバッグ、**event** はすべての CAC イベントのデバッグ、**packet** はすべての CAC パケットのデバッグを行うことを示します。

ステップ 7 次のコマンドを使用して、最大 2 台の 802.11 クライアント間の音声診断を実行し、デバッグメッセージを表示します。

```
debug voice-diag {enable | disable} mac-id mac-id2 [verbose]
```

verbose モードはオプションの引数です。verbose オプションを使用すると、すべてのデバッグメッセージがコンソールに表示されます。このコマンドを使用して、最大 2 台の 802.11 クライアントを監視できます。一方のクライアントが非 WiFi クライアントの場合、802.11 クライアントのみがデバッグメッセージについて監視されます。

(注) 監視対象のクライアントがコール中であることを前提にしていま
す。

(注) このデバッグ コマンドは、60 分後に自動停止しま
す。

ステップ 8 次のコマンドを使用して、音声関連の各種パラメータを表示します。

- **show client voice-diag status**

音声診断が有効になっているか無効になっているかについて表示されます。有効になっている場合は、ウォッチリスト内のクライアントに関する情報と音声コール診断の残り時間も表示されます。

音声診断が無効になっている場合、次のコマンドが実行されると、音声診断が無効になっていることを示すメッセージが表示されます。

- **show client voice-diag tspec**

音声診断が有効になっているクライアントから送信された TSPEC 情報が表示されます。

- **show client voice-diag qos-map**

QoS/DSCP マッピングに関する情報と 4 つのキュー（VO、VI、BE、BK）それぞれのパケット統計が表示されます。各種 DSCP 値も表示されます。

- **show client voice-diag avrg_rssi**

音声診断が有効になっている場合、クライアントの過去 5 秒間の RSSI 値が表示されます。

- **show client voice-diag roam-history**

過去 3 回のローミング コールに関する情報が表示されます。出力には、タイムスタンプ、ローミングに関連したアクセスポイント、およびローミングの理由が含まれ、ローミングに失敗した場合にはその理由も含まれます。

- **show client calls {active | rejected} {802.11a | 802.11bg | all}**

このコマンドにより、コントローラ上のアクティブな TSPEC および SIP コールの詳細が一覧表示されます。

ステップ 9 次のコマンドを使用して、ビデオ デバッグ メッセージと統計をトラブルシューティングします。

- **debug ap show stats {802.11b | 802.11a} ap-name multicast** : アクセス ポイントのサポート マルチキャスト レートが表示されます。
- **debug ap show stats {802.11b | 802.11a} ap-name load** : アクセス ポイントの QBSS およびその他の統計が表示されます。
- **debug ap show stats {802.11b | 802.11a} ap-name tx-queue** : アクセス ポイントの送信キュー トラフィック 統計が表示されます。
- **debug ap show stats {802.11b | 802.11a} ap-name client {all | video | client-mac}** : アクセス ポイントのクライアント メトリックが表示されます。
- **debug ap show stats {802.11b | 802.11a} ap-name packet** : アクセス ポイントのパケット 統計が表示されます。
- **debug ap show stats {802.11b | 802.11a} ap-name video metrics** : アクセス ポイントのビデオ メトリックが表示されます。
- **debug ap show stats video ap-name multicast mgid number** : アクセス ポイントのレイヤ 2 MGID データベース番号が表示されます。
- **debug ap show stats video ap-name admission** : アクセス ポイントのアドミッション制御統計が表示されます。
- **debug ap show stats video ap-name bandwidth** : アクセス ポイントのビデオ帯域幅が表示されます。

SIP ベースの CAC の設定

SIP ベースの CAC の制限

- SIP は、Cisco 5500 シリーズコントローラ、Cisco 8500 シリーズコントローラ、1240、1130、および 11n アクセス ポイント上でのみ使用できます。
- SIP CAC は、ステータス コード 17 をサポートし、TSPEC ベースのアドミッション制御をサポートしない電話に対してのみ使用してください。
- SIP CAC は、SIP スヌーピングが有効になっている場合にのみサポートされます。

SIP ベースの CAC の設定 (GUI)

はじめる前に

- 音声 が Platinum QoS レベルに設定されていることを確認します。

- WLAN のコール スヌーピングが有効になっていることを確認します。
- この無線のアドミッション制御 (ACM) が有効になっていることを確認します。

-
- ステップ 1 [Wireless] > [Advanced] > [SIP Snooping] を選択して、[SIP Snooping] ページを開きます。
- ステップ 2 開始ポートおよび終了ポートを入力して、コール スヌーピング ポートを指定します。
- ステップ 3 [Apply] をクリックし、[Save Configuration] をクリックします。
-

SIP ベースの CAC の設定 (CLI)

- ステップ 1 次のコマンドを入力して、音声を Platinum QoS レベルに設定します。
config wlan qos wlan-id Platinum
- ステップ 2 次のコマンドを入力して、特定の WLAN に対してコール スヌーピングの機能を有効にします。
config wlan call-snoop enable wlan-id
- ステップ 3 次のコマンドを入力して、この無線に対する ACM を有効にします。
config {802.11a | 802.11b} cac {voice | video} acm enable
- ステップ 4 コール スヌーピング ポートを設定するには、次のコマンドを入力します。
config advanced sip-snooping-ports starting-port ending-port
- ステップ 5 SIP ベースの CAC イベントをトラブルシューティングするには、次のコマンドを入力します。
debug sip event {enable | disable}
-

メディアパラメータの設定

メディアパラメータの設定 (GUI)

-
- ステップ 1 WMM と Gold QoS レベルに対して WLAN が設定されていることを確認してください。
- ステップ 2 WMM が有効になっている WLAN をすべて無効にして、[Apply] をクリックします。
- ステップ 3 [Wireless] を選択してから [802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオフにし、[Apply] をクリックして無線ネットワークを無効にします。
- ステップ 4 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Media] の順に選択します。[802.11a (または 802.11b) > Media > Parameters] ページが表示されます。
- ステップ 5 [Media] タブを選択して、[Media] ページを開きます。
- ステップ 6 [Unicast Video Redirect] チェックボックスをオンにして、ユニキャストビデオリダイレクトを有効にします。デフォルト値はディセーブルです。
- ステップ 7 [Maximum Media Bandwidth (0-85%)] テキストボックスに、この無線帯域でメディアアプリケーション用に割り当てられる最大帯域幅の割合を入力します。クライアントが指定値に達すると、アクセスポイントはこの無線帯域での新しいコールを拒否します。デフォルト値は 85 % です。有効な値は 0 ~ 85 % です。
- ステップ 8 [Client Phy Rate] テキストボックスに、クライアントの動作レートをキロビット/秒の値で入力します。
- ステップ 9 [Maximum Retry Percent (0-100%)] テキストボックスに、最大再試行の割合を入力します。デフォルト値は 80 です。
- ステップ 10 [Multicast Direct Enable] チェックボックスをオンにして、[Multicast Direct Enable] テキストボックスを有効にします。デフォルト値はイネーブルです。
- ステップ 11 [Max Streams per Radio] ドロップダウンリストから、無線あたりのマルチキャストダイレクトストリームの最大許可数を選択します。1 ~ 20 の値または [No Limit] を選択します。デフォルト値は [No Limit] に設定されています。
- ステップ 12 [Max Streams per Client] ドロップダウンリストから、無線あたりのクライアントの最大許可数を選択します。1 ~ 20 の値または [No Limit] を選択します。デフォルト値は [No Limit] に設定されています。
- ステップ 13 この無線に対して最良の無線キューを有効にする場合は、[Best Effort QoS Admission] チェックボックスをオンにします。デフォルト値はディセーブルです。
-

優先コール番号を使用した音声優先制御の設定

優先コール番号を使用した音声優先制御の設定について

TSPEC ベースのコールをサポートしないクライアントからのコールをサポートするようにコントローラを設定できます。この機能は、音声優先制御と呼ばれています。これらのコールは、音声プールを利用している他のクライアントよりも優先されます。音声優先制御は、SIP ベースのコールに対してのみ使用可能であり、TSPEC ベースのコールには使用できません。帯域幅が利用可能な場合は、通常のフローが使用され、それらのコールに帯域幅が割り当てられます。

最大 6 個の優先コール番号を設定できます。設定されている優先番号のうちの 1 つにコールが着信した場合、コントローラは、最大コール数の制限をチェックしません。優先コール用の帯域幅を割り当てるように、CAC が実行されます。帯域割り当ては、帯域幅プール全体（設定された最大音声プールからだけではない）の 85 % になります。帯域割り当ては、ローミング コールの場合であっても同じです。

優先コール番号を使用した音声優先制御の設定の前提条件

音声優先制御を設定する前に、次の設定を実行しておく必要があります。

- WLAN QoS を Platinum に設定します。
- 無線の ACM を有効にします。
- WLAN 上で SIP コール スヌーピングを有効にします。

優先コール番号の設定（GUI）

ステップ 1 WLAN QoS プロファイルを Platinum に設定します。

ステップ 2 WLAN 無線の ACM を有効にします。

ステップ 3 WLAN の SIP コール スヌーピングを有効にします。

ステップ 4 [Wireless] > [Advanced] > [Preferred Call] の順に選択して、[Preferred Call] ページを開きます。コントローラ上に設定されているすべてのコールが表示されます。

(注) 優先コールを削除するには、青いドロップダウン矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 5 [Add Number] をクリックして、新しい優先コールを追加します。

ステップ 6 [Call Index] テキストボックスに、コールに割り当てるインデックスを入力します。有効な値は 1 ~ 6 です。

ステップ 7 [Call Number] テキストボックスに、番号を入力します。

ステップ 8 [Apply] をクリックして、新しい番号を追加します。

優先コール番号の設定 (CLI)

-
- ステップ 1 次のコマンドを入力して、音声を Platinum QoS レベルに設定します。
config wlan qos wlan-id Platinum
- ステップ 2 次のコマンドを入力して、この無線に対する ACM を有効にします。
config {802.11a | 802.11b} cac {voice | video} acm enable
- ステップ 3 次のコマンドを入力して、特定の WLAN に対してコール スヌーピングの機能を有効にします。
config wlan call-snoop enable wlan-id
- ステップ 4 次のコマンドを入力して、新しい優先コールを追加します。
config advanced sip-preferred-call-no call_index {call_number | none}
- ステップ 5 次のコマンドを入力して、優先コールを削除します。
config advanced sip-preferred-call-no call_index none
- ステップ 6 次のコマンドを入力して、優先コールの統計を表示します。
show ap stats {802.11{a | b} | wlan} ap_name
- ステップ 7 次のコマンドを入力して、優先コール番号の一覧を表示します。
show advanced sip-preferred-call-no
-

EDCA パラメータの設定

EDCA パラメータについて

Enhanced Distributed Channel Access (EDCA; 拡張型分散チャネルアクセス) パラメータは、音声、ビデオ、およびその他の Quality of Service (QoS) トラフィックに優先的な無線チャネルアクセスを提供するように設計されています。

EDCA パラメータの設定 (GUI)

ステップ 1 [Wireless] を選択してから [802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオフにし、[Apply] をクリックして無線ネットワークを無効にします。

ステップ 2 [802.11a/n/ac] または [802.11b/g/n] の下の [EDCA Parameters] を選択します。[802.11a (または 802.11b/g) > EDCA Parameters] ページが表示されます。

ステップ 3 [EDCA Profile] ドロップダウン リストで、次のいずれかのオプションを選択します。

- [WMM] : Wi-Fi Multimedia (WMM) のデフォルトパラメータを有効にします。これは、デフォルト値です。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
- [Spectralink Voice Priority] : SpectraLink 音声優先パラメータを有効にします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。
- [Voice Optimized] : 音声用に最適化された EDCA プロファイルパラメータを有効にします。ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。
- [Voice & Video Optimized] : 音声とビデオ用に最適化された EDCA プロファイルパラメータを有効にします。ネットワーク上で音声サービスとビデオサービスを両方とも展開する場合に、このオプションを選択します。
- [Custom Voice] : 802.11a 用のカスタム音声 EDCA パラメータを有効にします。このオプションの EDCA パラメータは、このプロファイルが適用された場合、6.0 WMM EDCA パラメータとも一致します。

(注) ビデオサービスを展開する場合は、アドミッション制御 (Admission Control Management (ACM)) を無効にする必要があります。

ステップ 4 音声用の MAC の最適化を有効にする場合は、[Enable Low Latency MAC] チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします (デフォルト値)。この機能は、音声性能を向上させるために、パケットの再送信を制御するとともに、Lightweight アクセス ポイント上の音声パケットを適切にエージングアウトさせるというものです。その結果、アクセス ポイントあたりの処理可能な音声コール数が増加します。

(注) 低遅延 MAC を有効にすることはお勧めしません。WLAN で WMM クライアントが許可されている場合のみ、低遅延 MAC を有効にする必要があります。WMM が有効になっている場合は、低遅延 MAC を任意の EDCA プロファイルと共に使用できます。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 無線ネットワークを再度有効にするには、[802.11a/n/ac] または [802.11b/g/n] の下の [Network] を選択し、[802.11a (または 802.11b/g) Network Status] チェックボックスをオンにして、[Apply] をクリックします。

ステップ 7 [Save Configuration] をクリックします。

EDCA パラメータの設定 (CLI)

ステップ 1 次のコマンドを入力して、無線ネットワークを無効にします。

config {802.11a | 802.11b} disable network

ステップ 2 次のコマンドを入力して、設定を保存します。

save config

ステップ 3 次のコマンドを入力して、特定の EDCA プロファイルを有効にします。

config advanced {802.11a | 802.11b} edca-parameters {wmm-default | svp-voice| optimized-voice| optimized-voice-video| custom-voice}

- **wmm-default** : Wi-Fi Multimedia (WMM) のデフォルトパラメータを有効にします。これは、デフォルト値です。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
- **svp-voice** : SpectraLink 音声優先パラメータを有効にします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。
- **optimized-voice** : 音声用に最適化された EDCA プロファイルパラメータを有効にします。ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。
- **optimized-video-voice** : 音声とビデオ用に最適化された EDCA プロファイルパラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。
- **custom-voice** : 802.11a 用のカスタム音声 EDCA パラメータを有効にします。このオプションの EDCA パラメータは、このプロファイルが適用された場合、6.0 WMM EDCA パラメータとも一致します。

(注) ビデオ サービスを展開する場合は、アドミッション制御 (Admission Control Management (ACM)) を無効にする必要があります。

ステップ 4 次のコマンドを入力して、音声用の MAC 最適化の現在のステータスを表示します。

show {802.11a | 802.11b}

以下に類似した情報が表示されます。

```
Voice-mac-optimization.....Disabled
```

ステップ 5 次のコマンドを入力して、音声用の MAC 最適化を有効または無効にします。

config advanced {802.11a | 802.11b} voice-mac-optimization {enable | disable}

この機能は、音声性能を向上させるために、パケットの再送信を制御するとともに、Lightweight アクセスポイント上の音声パケットを適切にエージングアウトさせるというものです。その結果、アクセスポイントあたりの処理可能な音声コール数が増加します。デフォルト値はディセーブルです。

ステップ 6 次のコマンドを入力して、無線ネットワークを有効にします。

config {802.11a | 802.11b} enable network

ステップ 7 `save config` コマンドを入力して、設定を保存します。



第 18 章

Cisco Discovery Protocol の設定

- [Cisco Discovery Protocol の設定について, 181 ページ](#)
- [Cisco Discovery Protocol の設定に関する制限, 181 ページ](#)
- [Cisco Discovery Protocol の設定, 183 ページ](#)
- [Cisco Discovery Protocol 情報の表示, 186 ページ](#)
- [CDP デバッグ情報の取得, 189 ページ](#)

Cisco Discovery Protocol の設定について

Cisco Discovery Protocol (CDP) は、すべてのシスコ製の機器で実行されるデバイスディスカバリプロトコルです。CDP を使用して有効化されたデバイスは、近隣のデバイスにその存在を認識させるためにインターフェイスの更新をマルチキャストアドレスに周期的に送信します。

周期的な送信の間隔のデフォルト値は 60 秒で、アドバタイズされた有効期間のデフォルト値は 180 秒です。最新の 2 番目のバージョンのプロトコルである CDPv2 は、新しい Time Length Value (TLV) が導入されるとともに、従来よりも迅速なエラー追跡を可能にするレポートメカニズムを備えており、ダウンタイムが短縮されます。



(注) CDP はシスコ以外のスイッチとネットワーク要素でサポートされていないため、シスコ以外のスイッチに接続するときは、コントローラとアクセスポイント上で Cisco Discovery Protocol を無効にすることをお勧めします。

Cisco Discovery Protocol の設定に関する制限

- CDPv1 および CDPv2 は次のデバイスでサポートされています。
 - Cisco 5500 および 2500 シリーズ コントローラ

- CAPWAP が有効化されているアクセス ポイント
- Cisco 5500 シリーズ コントローラに直接接続されたアクセス ポイント



(注) Intelligent Power Management 機能を使用するには、Cisco 2500 シリーズ コントローラ上で CDPv2 を有効にしておく必要があります。CDP v2 は、デフォルトで有効になっています。

- Cisco 600 シリーズ OEAP アクセス ポイントは CDP をサポートしません。
- CDPv1 と CDPv2 のサポートにより、ネットワーク管理アプリケーションは、シスコ デバイスを検出できるようになります。
- 次の TLV は、コントローラとアクセス ポイントの両方でサポートされています。
 - Device-ID TLV (0x0001) : コントローラ、アクセス ポイント、または CDP ネイバーのホスト名。
 - Address TLV (0x0002) : コントローラ、アクセス ポイント、または CDP ネイバーの IP アドレス。
 - Port-ID TLV (0x0003) : CDP パケットが送信されるインターフェイス名。
 - Capabilities TLV (0x0004) : デバイスの機能。コントローラから送信されるこの TLV の値は Host: 0x10、アクセス ポイントから送信されるこの TLV の値は Transparent Bridge: 0x02 です。
 - Version TLV (0x0005) : コントローラ、アクセス ポイント、または CDP ネイバーのソフトウェア バージョン。
 - Platform TLV (0x0006) : コントローラ、アクセス ポイント、または CDP ネイバーのハードウェア プラットフォーム。
 - Power Available TLV (0x001a) : 使用可能な電力量。デバイスが適切な電力設定をネゴシエートし、選択するために、給電側機器から送信されます。
 - Full/Half Duplex TLV (0x000b) : CDP パケットが送信されるイーサネット リンクの全二重または半二重モード。
- 次の TLV は、アクセス ポイントでのみサポートされます。
 - Power Consumption TLV (0x0010) : アクセス ポイントが消費する電力の最大量。
 - Power Request TLV (0x0019) : ネットワーク電力の供給側と適切な電力レベルをネゴシエートするために給電可能デバイスから送信される電力量。
- CDP 設定をコントローラで変更しても、コントローラに接続されているアクセス ポイントの CDP 設定は変更されません。各アクセス ポイントに対して個別に CDP を有効または無効にする必要があります。

- すべてまたは特定のインターフェイスおよび無線に対して CDP の状態を有効または無効にできます。この設定は、すべてのアクセス ポイントまたは特定のアクセス ポイントに適用できます。
- 各種インターフェイスおよびアクセス ポイントに対して想定される動作は次のとおりです。
 - 屋内（非屋内メッシュ）アクセス ポイント上の無線インターフェイスでは、CDP は無効になります。
 - 非メッシュ アクセス ポイントでは、それらがコントローラに join している場合、無線インターフェイス上で CDP は無効になります。前のイメージで CDP がサポートされていた AP には、永続的な CDP 設定が使用されます。
 - 屋内メッシュ アクセス ポイント上とメッシュ アクセス ポイント上の無線インターフェイスでは、CDP は有効になります。
 - メッシュ アクセス ポイントでは、それらがコントローラに join している場合、無線インターフェイス上で CDP が有効になります。前のイメージで CDP がサポートされていたアクセス ポイントには、永続的な CDP 設定が使用されます。無線インターフェイスの CDP 設定は、メッシュ AP に対してだけ適用されます。

Cisco Discovery Protocol の設定

Cisco Discovery Protocol の設定（GUI）

-
- ステップ 1** [Controller]>[CDP]>[Global Configuration] の順に選択して [CDP>Global Configuration] ページを開きます。
- ステップ 2** コントローラ上で CDP を有効にする場合は [CDP Protocol Status] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はオンです。
 (注) この機能の有効化と無効化は、すべてのコントローラ ポートに適用されません。
- ステップ 3** [CDP Advertisement Version] ドロップダウン リストから、コントローラでサポートされている CDP の最新バージョン ([v1] または [v2]) を選択します。デフォルト値は [v1] です。
- ステップ 4** [Refresh-time Interval] テキスト ボックスに、CDP メッセージが生成される間隔を入力します。範囲は 5 ~ 254 秒で、デフォルト値は 60 秒です。
- ステップ 5** [Holdtime] テキスト ボックスに、生成された CDP パケットの中の存続可能時間値としてアドバタイズされる時間の長さを入力します。範囲は 10 ~ 255 秒で、デフォルト値は 180 秒です。
- ステップ 6** [Apply] をクリックして、変更を確定します。
- ステップ 7** [Save Configuration] をクリックして、変更を保存します。
- ステップ 8** 次のいずれかの操作を行います。

- 特定のアクセス ポイントで CDP を有効または無効にする手順は、次のとおりです。

[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

目的のアクセス ポイントのリンクをクリックします。

[Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。

このアクセス ポイントで CDP を有効にする場合は [Cisco Discovery Protocol] チェックボックスをオンにします。この機能が無効にする場合は、オフにします。デフォルト値はイネーブルです。

(注) ステップ 2 で CDP を無効していた場合、コントローラ CDP が無効になっていることを示すメッセージが表示されます。

- 次の手順に従って、特定のイーサネット インターフェイス、無線、またはスロットに対して CDP を有効にします。

[Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

目的のアクセス ポイントのリンクをクリックします。

[Interfaces] タブを選択し、[CDP Configuration] セクションで無線またはスロットの対応するチェックボックスをオンにします。

(注) 無線に対する設定は、メッシュ アクセス ポイントにだけ適用されません。

[Apply] をクリックして、変更を確定します。

- このコントローラに現在アソシエートされているすべてのアクセス ポイントで CDP を有効または無効にする手順は、次のとおりです。

[Wireless] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。

コントローラにアソシエートされているすべてのアクセス ポイントで CDP を有効にするには、[CDP State] チェックボックスをオンにします。すべてのアクセス ポイントで CDP を無効にするには、オフにします。デフォルト値はオンです。特定のイーサネット インターフェイス、無線、またはスロットのチェックボックスをオンにすることで、それらに対する CDP を有効にできます。この設定は、コントローラにアソシエートされているすべてのアクセス ポイントに適用されます。

[Apply] をクリックして、変更を確定します。

ステップ 9 [Save Configuration] をクリックして、変更を保存します。

Cisco Discovery Protocol の設定 (CLI)

ステップ 1 次のコマンドを入力して、コントローラ上で CDP を有効または無効にします。

```
config cdp {enable | disable}
```

CDP はデフォルトで有効になっています。

- ステップ 2** 次のコマンドを入力して、CDP メッセージが生成される間隔を指定します。
config cdp timer seconds
範囲は 5 ~ 254 秒で、デフォルト値は 60 秒です。
- ステップ 3** 次のコマンドを入力して、生成された CDP パケットの中の存続可能時間値としてアドバタイズされる時間の長さを指定します。
config cdp holdtime seconds
範囲は 10 ~ 255 秒で、デフォルト値は 180 秒です。
- ステップ 4** 次のコマンドを入力して、コントローラでサポートされる最高の CDP バージョンを指定します。
config cdp advertise {v1 | v2}
デフォルト値は [v1] です。
- ステップ 5** **config ap cdp {enable | disable} all** コマンドを入力して、コントローラに join しているすべてのアクセス ポイント上で CDP を有効または無効にします。
config ap cdp disable all コマンドは、コントローラに join しているすべてのアクセス ポイントおよび今後 join するすべてのアクセス ポイントの CDP を無効化します。CDP は、コントローラまたはアクセス ポイントのリブート後も現在と将来のアクセス ポイントで無効のままになります。CDP を有効にするには、**config ap cdp enable all** コマンドを入力します。
(注) コントローラに join しているすべてのアクセス ポイントで CDP を有効にした後、ステップ 6 のコマンドを使用して個々のアクセス ポイントで CDP を無効にした後再び有効にできます。コントローラに join されたすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、無効にすることはできません。
- ステップ 6** 次のコマンドを入力して、特定のアクセス ポイントで CDP を有効または無効にします。
config ap cdp {enable | disable} Cisco_AP
- ステップ 7** 次のコマンドを入力して、特定またはすべてのアクセス ポイントで特定のインターフェイスに CDP を設定します。
config ap cdp {ethernet | radio} interface_number slot_id {enable | disable} {all | Cisco_AP}
(注) **config ap cdp** コマンドを使用して無線インターフェイスに CDP を設定した場合、その設定はメッシュ アクセス ポイントにしか適用されないことを示す警告メッセージが表示されます。
- ステップ 8** 次のコマンドを入力して、変更を保存します。
save config
-

Cisco Discovery Protocol 情報の表示

Cisco Discovery Protocol 情報の表示 (GUI)

ステップ 1 [Monitor] > [CDP] > [Interface Neighbors] の順に選択して、[CDP > Interface Neighbors] ページを開きます。このページには、次の情報が表示されます。

- CDP パケットが受信されたコントローラ ポート
- 各 CDP ネイバーの名前
- 各 CDP ネイバーの IP アドレス
- CDP パケットの送信に各 CDP ネイバーが使用するポート
- 各 CDP ネイバー エントリの有効期限までの残り時間 (秒)
- 各 CDP ネイバーの機能は、R : ルータ、T : 転送ブリッジ、B : ソースルートブリッジ、S : スイッチ、H : ホスト、I : IGMP、r : リピータ、M : リモート管理デバイスとして表示されます。
- 各 CDP ネイバー デバイスのハードウェア プラットフォーム

ステップ 2 目的のインターフェイス ネイバーの名前をクリックして、各インターフェイスの CDP ネイバーの詳細情報を表示します。[CDP > Interface Neighbors > Detail] ページが表示されます。このページには、次の情報が表示されます。

- CDP パケットが受信されたコントローラ ポート
- CDP ネイバーの名前
- CDP ネイバーの IP アドレス
- CDP パケットの送信に CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン (v1 または v2)
- CDP ネイバー エントリの有効期限までの残り時間 (秒)
- CDP ネイバーの機能 ([Router]、[Trans Bridge]、[Source Route Bridge]、[Switch, Host]、[IGMP]、[Repeater]、または [Remotely Managed Device])
- CDP ネイバー デバイスのハードウェア プラットフォーム
- CDP ネイバーで実行されているソフトウェア

ステップ 3 [AP Neighbors] を選択して、コントローラに接続されているすべてのアクセス ポイントの CDP ネイバーのリストを表示します。[CDP AP Neighbors] ページが表示されます。

ステップ 4 目的のアクセス ポイントの [CDP Neighbors] リンクをクリックして、特定のアクセス ポイントの CDP ネイバーのリストを表示します。[CDP > AP Neighbors] ページが表示されます。

このページには、次の情報が表示されます。

- 各アクセス ポイントの名前
- 各アクセス ポイントの IP アドレス
- 各 CDP ネイバーの名前
- 各 CDP ネイバーの IP アドレス
- 各 CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン (v1 または v2)

ステップ 5 目的のアクセス ポイントの名前をクリックして、アクセス ポイントの CDP ネイバーの詳細情報を表示します。 [CDP > AP Neighbors > Detail] ページが表示されます。このページには、次の情報が表示されます。

- アクセス ポイントの名前
- アクセス ポイントの無線の MAC アドレス
- アクセス ポイントの IP アドレス
- CDP パケットが受信されたインターフェイス
- CDP ネイバーの名前
- CDP ネイバーの IP アドレス
- CDP ネイバーが使用するポート
- アドバタイズされている CDP バージョン (v1 または v2)
- CDP ネイバー エントリの有効期限までの残り時間 (秒)
- CDP ネイバーの機能 (R : ルータ、T : 転送ブリッジ、B : ソース ルート ブリッジ、S : スイッチ、H : ホスト、I : IGMP、r : リピータ、M : リモート管理デバイス)
- CDP ネイバー デバイスのハードウェア プラットフォーム
- CDP ネイバーで実行されているソフトウェア

ステップ 6 [Traffic Metrics] を選択して、CDP トラフィック情報を表示します。 [CDP > Traffic Metrics] ページが表示されます。このページには、次の情報が表示されます。

- コントローラで受信した CDP パケット数
- コントローラから送信した CDP パケット数
- チェックサム エラーが発生したパケット数
- メモリ不足のためにドロップされたパケット数
- 無効なパケット数

Cisco Discovery Protocol 情報の表示 (CLI)

- ステップ 1** 次のコマンドを入力して、CDP のステータスを確認し、CDP プロトコル情報を表示します。
show cdp
- ステップ 2** 次のコマンドを入力して、すべてのインターフェイスのすべての CDP ネイバーのリストを確認します。
show cdp neighbors [detail]
オプションの detail コマンドを指定すると、コントローラの CDP ネイバーの詳細な情報が表示されます。
(注) このコマンドは、コントローラの CDP ネイバーのみを表示します。コントローラにアソシエートしているアクセス ポイントの CDP ネイバーは表示されません。アクセス ポイントごとの CDP ネイバーのリストを表示するコマンドは、この後で説明します。
- ステップ 3** 次のコマンドを入力して、データベース内のすべての CDP エントリを表示します。
show cdp entry all
- ステップ 4** 次のコマンドを入力して、指定されたポートの CDP トラフィック情報（送受信されるパケット、CRC エラーなど）を表示します。
show cdp traffic
- ステップ 5** 次のコマンドを入力して、特定のアクセス ポイントの CDP ステータスを表示します。
show ap cdp ap-name Cisco_AP
- ステップ 6** 次のコマンドを入力して、このコントローラに接続されたすべてのアクセス ポイントの CDP ステータスを表示します。
show ap cdp all
- ステップ 7** 次のコマンドを入力して、特定のアクセス ポイントのすべての CDP ネイバーのリストを表示します。
- **show ap cdp neighbors ap-name Cisco_AP**
 - **show ap cdp neighbors detail Cisco_AP**
- (注) アクセス ポイントからコントローラに CDP ネイバー情報が送信されるのは、情報が変更されたときだけです。
- ステップ 8** 次のコマンドを入力して、コントローラに接続されているすべてのアクセス ポイントのすべての CDP ネイバーのリストを表示します。
- **show ap cdp neighbors all**
 - **show ap cdp neighbors detail all**
- (注) アクセス ポイントからコントローラに CDP ネイバー情報が送信されるのは、情報が変更されたときだけです。
-

CDP デバッグ情報の取得

- 次のコマンドを入力して、CDP パケットに関連したデバッグ情報を取得します。

debug cdp packets

- 次のコマンドを入力して、CDP イベントに関連したデバッグ情報を取得します。

debug cdp events



第 19 章

コントローラと NTP サーバの認証の設定

- [コントローラと NTP サーバの認証の設定について](#)、191 ページ
- [NTP サーバの認証の設定 \(GUI\)](#)、191 ページ
- [NTP サーバの認証の設定 \(CLI\)](#)、192 ページ

コントローラと NTP サーバの認証の設定について

リリース 7.0.116.0 から、コントローラ ソフトウェアは RFC 1305 に準拠するようになりました。この要件に従い、コントローラは、認証によって NTP サーバと時刻を同期させる必要があります。デフォルトでは、MD5 チェックサムが使用されます。

NTP サーバの認証の設定 (GUI)

- ステップ 1** [Controller] > [NTP] > [Server] を選択して、[NTP Servers] ページを開きます。
 - ステップ 2** [New] をクリックして、新しい NTP サーバを追加します。
 - ステップ 3** [Server Index (Priority)] テキスト ボックスに、NTP サーバ インデックスを入力します。コントローラは、インデックス 1 を最初に試し、その後はインデックス 2 から 3 へと優先順位の高い順に試します。ネットワークで NTP サーバが 1 台しか使用されていない場合は、1 に設定します。
 - ステップ 4** サーバの IP アドレスを入力します。
 - ステップ 5** NTP 認証を有効または無効にします。
 - ステップ 6** NTP 認証を有効にした場合、キー インデックスを入力します。
 - ステップ 7** [Apply] をクリックします。
-

NTP サーバの認証の設定 (CLI)

はじめる前に

- **config time ntp auth enable** *server-index key-index* : 指定された NTP サーバに対して NTP 認証を有効にします。
- **config time ntp key-auth add** *key-index md5 key-format key* : 認証キーを追加します。デフォルトでは MD5 が使用されます。キー形式には、「ascii」または「hex」を使用できます。
- **config time ntp key-auth delete** *key-index* : 認証キーを削除します。
- **config time ntp auth disable** *server-index* : NTP 認証を無効にします。
- **show ntp-keys** : NTP 認証関連のパラメータを表示します。



第 20 章

RFID タグ追跡の設定

- RFID タグ追跡の設定について, 193 ページ
- RFID タグ追跡の設定 (CLI), 195 ページ
- RFID タグ追跡情報の表示 (CLI), 195 ページ
- RFID タグ追跡問題のデバッグ (CLI), 196 ページ

RFID タグ追跡の設定について

コントローラでは、Radio-Frequency Identification (RFID) タグ追跡を設定できます。RFID タグは、資産の位置をリアルタイムで追跡するために取り付けられる、小型の無線装置です。タグは、その位置を専用の 802.11 パケットを使用してアドバタイズします。このパケットは、アクセスポイント、コントローラ、および Mobility Services Engine で処理されます。

コントローラでサポートされるタグの詳細情報は、http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html に示されています。Mobility Services Engine は、この CCX 仕様に準拠したタグからテレメトリ情報とチョークポイント情報を受け取ります。

表 5: RFID タグ用 *Cisco Compatible Extensions* の概要

パートナー	AeroScout		WhereNet	Pango (InnerWireless)
製品名	T2	T3	Wheretag IV	V3
テレメトリ				
温度	○	○	—	○
圧力	—	—	—	—
湿度	—	—	—	—

パートナー	AeroScout		WhereNet	Pango (InnerWireless)
ステータス	—	—	—	—
燃料	—	—	—	—
数量	—	—	—	—
距離	—	—	—	—
動作検出	○	○	—	○
パニック ボタンの数	1	2	0	1
改ざん		○	○	○
バッテリー情報	○	○	○	○
複数周波数タグ ³	○	○	○	

³ チョークポイント システムでは、このタグは同じベンダー製のチョークポイント以外で機能しないことに注意してください。



(注)

ネットワーク モビリティ サービス プロトコル (NMSP) は、Mobility Services Engine 上で動作します。NMSP が機能するためには、コントローラおよび Mobility Services Engine が通信を行う TCP ポート (16113) が、これらの 2 つのデバイス間にあるファイアウォールで開いた (ブロックされていない) 状態である必要があります。

シスコ認定タグでは、次の機能がサポートされています。

- **情報通知** : ベンダー固有の情報および緊急情報を表示できます。
- **情報のポーリング** : バッテリーのステータスおよびテレメトリ データを監視できます。さまざまな種類のテレメトリ データにより、知覚ネットワークおよび RFID タグの各種アプリケーションに対するサポートを提供します。
- **測定の通知** : 建物やキャンパス内の重要ポイントにチョークポイントを展開できます。決められたチョークポイントの近くに RFID タグが移動すると、タグはそのチョークポイントに対する自分の位置をアダプタイズするパケットの送信を開始します。

RFID タグ追跡情報は、コントローラ CLI を使用して設定および表示できます。

RFID タグ追跡の設定 (CLI)

ステップ 1 次のコマンドを入力して、RFID タグ追跡を有効または無効にします。

```
config rfid status {enable | disable}
```

デフォルト値はイネーブルです。

ステップ 2 次のコマンドを入力して、静的なタイムアウト値 (60 ~ 7200 秒) を指定します。

```
config rfid timeout seconds
```

静的なタイムアウト値は、タグを失効させずにコントローラが保持する期間です。たとえば、タグが 30 秒ごとにビーコンするよう設定されている場合は、タイムアウト値を 90 秒 (ビーコン値の約 3 倍) に設定することをお勧めします。デフォルト値は 1200 秒です。

ステップ 3 次のコマンドを入力して、特定のタグに対する RFID タグのモビリティを有効または無効にします。

- **config rfid mobility vendor_name enable** : 特定のベンダーのタグに対するクライアント モビリティを有効にします。このコマンドを入力すると、タグが設定を選択またはダウンロードしようとするとき、クライアントモードの DHCP アドレスを取得できなくなります。
- **config rfid mobility vendor_name disable** : 特定のベンダーのタグに対するクライアント モビリティを無効にします。このコマンドを入力した場合、タグは DHCP アドレスを取得できます。タグがあるサブネットから別のサブネットへ移動すると、タグは、アンカー状態を維持するのではなく、新しいアドレスを取得します。

(注) これらのコマンドは Pango タグに対してのみ使用できます。したがって、*vendor_name* に指定できる値は、すべて小文字の「pango」のみとなります。

RFID タグ追跡情報の表示 (CLI)

ステップ 1 次のコマンドを入力して、RFID タグ追跡の現在の設定を確認します。

```
show rfid config
```

ステップ 2 次のコマンドを入力して、特定の RFID タグの詳細情報を表示します。

```
show rfid detail mac_address
```

mac_address は、タグの MAC アドレスです。

ステップ 3 次のコマンドを入力して、コントローラに現在接続されているすべての RFID タグのリストを表示します。

```
show rfid summary
```

ステップ 4 次のコマンドを入力して、コントローラにアソシエートされている RFID タグのリストを表示します。

```
show rfid client
```

RFID タグ追跡問題のデバッグ (CLI)

RFID タグ追跡に関する問題が発生した場合は、次のデバッグ コマンドを使用します。

- 次のコマンドを入力して、MAC アドレスのデバッグを設定します。

```
debug mac addr mac_address
```



(注) タグごとにデバッグを実行することをお勧めします。すべてのタグに対してデバッグを有効にすると、コンソールまたは Telnet 画面に非常にたくさんのメッセージが表示されることになります。

- 次のコマンドを入力して、802.11 RFID タグ モジュールのデバッグを有効または無効にします。

```
debug dot11 rfid {enable | disable}
```

- 次のコマンドを入力して、RFID デバッグ オプションを有効または無効にします。

```
debug rfid {all | detail | error | nmsp | receive} {enable | disable}
```

値は次のとおりです。

- **all** : すべての RFID メッセージのデバッグを行います。
- **detail** : RFID 詳細メッセージのデバッグを行います。
- **error** : RFID エラー メッセージのデバッグを行います。
- **nmsp** : RFID NMSP メッセージのデバッグを行います。
- **receive** : 受信した RFID タグ メッセージのデバッグを行います。



第 **21** 章

コントローラのデフォルト設定へのリセット

- [コントローラのデフォルト設定へのリセットについて](#), 197 ページ
- [コントローラのデフォルト設定へのリセット \(GUI\)](#), 198 ページ
- [コントローラのデフォルト設定へのリセット \(CLI\)](#), 198 ページ

コントローラのデフォルト設定へのリセットについて

コントローラを初期の設定に戻すには、コントローラを工場出荷時のデフォルト設定にリセットします。

コントローラのデフォルト設定へのリセット (GUI)

-
- ステップ1 インターネット ブラウザを起動します。
 - ステップ2 ブラウザのアドレス行にコントローラの IP アドレスを入力して Enter キーを押します。 [Enter Network Password] ダイアログボックスが表示されます。
 - ステップ3 [User Name] テキスト ボックスにユーザ名を入力します。 デフォルトのユーザ名は *admin* です。
 - ステップ4 [Password] テキスト ボックスに無線デバイスのパスワードを入力して Enter を押します。 デフォルトのパスワードは *admin* です。
 - ステップ5 [Commands] > [Reset to Factory Default] の順に選択します。
 - ステップ6 [Reset] をクリックします。
 - ステップ7 確認の画面が表示されたら、リセットを選択します。
 - ステップ8 設定を保存せずにコントローラをリブートします。
 - ステップ9 設定ウィザードを使用して、設定を入力します。 詳細については、「[コントローラの設定 : CLI設定ウィザードの使用](#)」の項を参照してください。
-

コントローラのデフォルト設定へのリセット (CLI)

-
- ステップ1 **reset system** コマンドを入力します。 変更内容を設定に保存するかどうかを尋ねるプロンプトが表示されたら、**N** を入力します。 ユニットがリブートします。
 - ステップ2 ユーザ名の入力を求められたら、**recover-config** コマンドを入力して、工場出荷時のデフォルト設定を復元します。 コントローラがリブートし、次のメッセージが表示されます。

Welcome to the Cisco WLAN Solution Wizard Configuration Tool
 - ステップ3 設定ウィザードを使用して、設定を入力します。 詳細については、「[コントローラの設定 : CLI設定ウィザードの使用](#)」の項を参照してください。
-



第 22 章

コントローラ ソフトウェアと設定の管理

- [コントローラ ソフトウェアのアップグレード, 199 ページ](#)
- [コントローラとのファイルのやり取り, 217 ページ](#)
- [設定の保存, 233 ページ](#)
- [設定ファイルの編集, 234 ページ](#)
- [コントローラの設定のクリア, 235 ページ](#)
- [コントローラ設定の消去, 235 ページ](#)
- [コントローラのリセット, 236 ページ](#)

コントローラ ソフトウェアのアップグレード

コントローラ ソフトウェアをアップグレードすると、コントローラにアソシエートされているアクセス ポイントのソフトウェアも自動的にアップグレードされます。アクセス ポイントがソフトウェアをロードしている場合、アクセス ポイントの各 LED は連続して点滅します。最大 10 台のアクセス ポイントをコントローラから同時にアップグレードできます。



注意

このプロセスの実行時に、コントローラまたは任意のアクセス ポイントの電源を切らないでください。電源を切ると、ソフトウェア イメージが破損する場合があります。多数のアクセス ポイントを含むコントローラをアップグレードするには、ネットワークのサイズにもよりますが、最大で 30 分かかる場合があります。ただし、コントローラ ソフトウェア リリースでサポートされているアクセス ポイントの同時アップグレード数の増加によって、アップグレードにかかる時間が大幅に短縮されました。アクセス ポイントの電源は入れたままにしておく必要があります。また、アップグレード時にコントローラをリセットしてはなりません。

コントローラソフトウェアのアップグレードに関する制限

- あるリリースから別のリリースへダウングレードするときには、現在のリリースの設定が失われるおそれがあります。回避策として、バックアップサーバに保存されている以前のコントローラ設定ファイルをリロードするか、コントローラを再設定する方法があります。
- 6.0.182.0 より古いリリースからこのリリースに直接アップグレードすることはできません。
- 特定のリリース間のみでコントローラソフトウェアをアップグレードしたり、ダウングレードしたりすることができます。一部のインスタンスでは、コントローラを中間リリースにアップグレードしてから最新のソフトウェアリリースにアップグレードする必要があります。
- 中間のソフトウェアリリースにコントローラをアップグレードする場合は、コントローラにアソシエートされているすべてのアクセスポイントを中間リリースにアップグレードしてから最新のコントローラソフトウェアをインストールしてください。大規模なネットワークでは、各アクセスポイントでソフトウェアをダウンロードするのに多少時間がかかる場合があります。
- 最新のソフトウェアリリースにアップグレードすると、コントローラにアソシエートされているアクセスポイントのソフトウェアも自動的にアップグレードされます。アクセスポイントがソフトウェアをロードしている場合、アクセスポイントの各 LED は連続して点滅します。
- コントローラの GUI を使用するには、Microsoft Internet Explorer 6.0 SP1（またはそれ以降のリリース）または Mozilla Firefox 2.0.0.11（またはそれ以降のリリース）を使用することを推奨します。
- Cisco のコントローラでは、標準の SNMP 管理情報ベース（MIB）ファイルをサポートしています。MIB は Cisco.com の Software Center からダウンロードできます。
- コントローラソフトウェアは、工場でコントローラにインストールされており、リリースのアップグレード後や、アクセスポイントがコントローラに join したときには、アクセスポイントに自動的にダウンロードされます。運用上の利点を最大限活用するために、利用可能な最新のソフトウェアバージョンをインストールすることを推奨します。
- Wireless LAN Controller Field Upgrade Software for Release 1.7.0.0-FUS をインストールすることを推奨します。これは特別な AES パッケージであり、システムに関連するコンポーネントのアップグレードが複数含まれています。これには、ブートローダ、フィールドリカバリイメージ、および FPGA/MCU ファームウェアが含まれています。FUS イメージのインストールでは重要なファームウェアがいくつかインストールされるため、特に注意が必要です。FUS イメージはランタイムイメージとは無関係です。詳細については、http://www.cisco.com/en/US/docs/wireless/controller/release/notes/fus_rm_1_7_0_0.html を参照してください。
- ソフトウェアのアップグレードに TFTP または FTP サーバが使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。
 - TFTP サーバで、コントローラソフトウェアリリースよりも大きなサイズのファイルがサポートされていることを確認します。このサイズのファイルをサポートする TFTP サーバには、tftpd32 や Cisco Prime Infrastructure 内の TFTP サーバがあります。コント

ローラ ソフトウェアをダウンロードするときに TFTP サーバでこのサイズのファイルがサポートされていないと、「TFTP failure while storing in flash」というエラーメッセージが表示されます。

- ディストリビューション システム ネットワーク ポートを経由してアップグレードする場合、ディストリビューション システム ポートはルーティング可能なため、TFTP または FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- コントローラを AC 電源に接続すると、起動スクリプトおよび電源投入時自己診断テストが実行されて、システムが初期化されます。この間に Esc キーを押すと、ブートローダの [Boot Options] メニューが表示されます。5500 および Flex 7500 シリーズのコントローラのメニュー オプションは、他のコントローラ プラットフォームとは異なります。

5500 シリーズ コントローラのブートローダ メニューは次のとおりです。

```
Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Change active boot image
 4. Clear Configuration
 5. Format FLASH Drive
 6. Manually update images
Please enter your choice:
```

他のコントローラ プラットフォームのブートローダ メニューは次のとおりです。

```
Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Manually update images
 4. Change active boot image
 5. Clear Configuration
Please enter your choice:
```

現在のソフトウェアを実行するには **1** を、以前のソフトウェアを実行するには **2** を、現在のソフトウェアを実行して、コントローラの設定を出荷時の初期状態に設定するには **4** (5500 シリーズコントローラの場合)、または **5** (他のコントローラ プラットフォームの場合) を入力します。その他のオプションは、特に指示がない限り選択しないでください。



(注) 起動スクリプトおよび電源投入時自己診断テストの実行の詳細については、コントローラのインストールガイドまたはクイック スタートガイドを参照してください。

- 管理インターフェイスで NAT が有効になっている場合に、CAPWAP ディスカバリ応答で送信されるアドレスを制御するには、次のコマンドを使用します。

```
config network ap-discovery nat-ip-only {enable | disable}
```

値は次のとおりです。

- **enable** : NAT IP の使用をディスカバリ応答でのみ有効にします。これはデフォルトです。このコマンドは、すべての AP が NAT ゲートウェイの外にある場合に使用します。

- **disable** : ディスカバリ応答での NAT IP および非 NAT IP の両方の使用を有効にします。このコマンドは、AP が NAT ゲートウェイの内部および外部にある場合に使用します。たとえば、ローカルモードの AP と OfficeExtend AP が同じコントローラにある場合です。



(注) AP が孤立するのを防ぐには、**config network ap-discovery nat-ip-only** コマンドに **disable** オプションを使用する前に、AP のリンク遅延を無効にする必要があります (有効にされている場合)。AP のリンク遅延を無効にするには、**config ap link-latency disable all** コマンドを使用します。

- 802.1p タギングを設定するには、**config qos dot1p-tag {bronze | silver | gold | platinum}** タグを使用します。7.2.103.0 以降のリリースでは、802.1p パケットをタグ付けすると、タギングは有線のパケットに対してのみ影響します。ワイヤレス パケットは、QoS に設定された最大優先レベルによってのみ影響を受けます。
- 次の操作によってネットワークのダウンタイムを減らすことができます。
 - AP イメージを事前にダウンロードできます。
 - FlexConnect アクセス ポイントの場合は、FlexConnect Efficient AP Upgrade 機能を使用して、コントローラと AP (メイン サイトとブランチ) 間のトラフィックを削減することができます。
- アップグレードの実行時に、コントローラまたはアクセスポイントの電源を切らないでください。電源を切ると、ソフトウェア イメージが破損する場合があります。多数のアクセスポイントを含むコントローラをアップグレードするには、ネットワークのサイズにもよりますが、最大で 30 分かかる場合があります。ただし、同時にアップグレードされるアクセスポイント数が増加したため、アップグレードの時間が大幅に短縮されました。アクセスポイントの電源は入れたままにしておく必要があります。また、アップグレード時にコントローラをリセットしてはなりません。
- 以前のリリースにダウングレードする場合は、次のいずれかを実行します。
 - インターフェイス グループにマッピングされている WLAN をすべて削除し、新しいポリシーを作成します。
 - すべての WLAN がインターフェイス グループではなくインターフェイスにマッピングされるようにします。
- 次の操作をコントローラで実行した後は、変更を有効にするためにコントローラをリブートする必要があります。
 - リンク集約 (LAG) の有効化または無効化
 - 証明書に関する機能の有効化 (HTTPS や Web 認証など)
 - 新しい SNMP v3 ユーザの追加、あるいは既存のユーザの変更

- 既存の SNMPv3 エンジン ID の変更
 - 新しいライセンスの追加、あるいは既存のライセンスの変更
 - ライセンスの優先度を上げる
- コントローラのブートローダには、アクティブなプライマリイメージとバックアップイメージのコピーが保存されています。プライマリイメージが破損した場合は、バックアップイメージを使用してブートローダを起動させることができます。
バックアップイメージが保存されている状態で、リブートの前にブートメニューで [Option 2: Run Backup Image] を選択し、バックアップイメージから起動されるようにします。次に、動作することが判明しているイメージでアップグレードを行い、コントローラをリブートします。
 - リカバリイメージによって、イメージのアップグレード時にアクセスポイントのパワーサイクリングを行っても使用できる、バックアップイメージが提供されます。アクセスポイントでリカバリの必要を避ける最善の方法は、システムのアップグレード時にアクセスポイントのパワーサイクリングを避けることです。サイズの大きなアクセスポイントイメージへのアップグレードの際にパワーサイクリングが発生した場合、TFTP リカバリの手順を使用してアクセスポイントを回復できます。
TFTP リカバリの手順を使用してアクセスポイントを回復させるには、次の手順を実行します。
 - 1 必要なリカバリイメージを Cisco.com (c1100-rcvk9w8-mx、c1200-rcvk9w8-mx、または c1310-rcvk9w8-mx) からダウンロードし、お使いの TFTP サーバのルートディレクトリにインストールします。
 - 2 TFTP サーバをターゲットのアクセスポイントと同じサブネットに接続して、アクセスポイントをパワーサイクリングします。アクセスポイントは TFTP イメージから起動し、次にコントローラに join してサイズの大きなアクセスポイントのイメージをダウンロードし、アップグレード手順を完了します。
 - 3 アクセスポイントが回復したら、TFTP サーバを削除できます。
 - 連邦情報処理標準 (FIPS) が有効な場合でも、コントローラソフトウェアの新しいリリースへのアップグレードや、旧リリースへのダウングレードは実行できます。

コントローラ ソフトウェアのアップグレード (GUI)

- ステップ 1** コントローラ設定ファイルをサーバにアップロードしてバックアップします。
(注) コントローラ ソフトウェアをアップグレードする前に、コントローラの設定ファイルをバックアップしておくことを強く推奨します。バックアップを行わなかった場合は、コントローラを手動で再設定する必要があります。
- ステップ 2** 次の手順に従って、コントローラ ソフトウェアのイメージを入手します。

- a) Cisco Software Center (<http://www.cisco.com/cisco/software/navigator.html>) を参照してください。
- b) [Wireless] > [Wireless LAN Controller] を選択します。
[Integrated Controllers]、[Controller Modules]、および [Standalone Controllers] の各オプションがあります。
- c) 使用しているコントローラのプラットフォームに応じて、これらのオプションのいずれかをクリックします。
- d) コントローラのモデル番号または名前をクリックします。[Download Software] ページが表示されます。
- e) コントローラ ソフトウェア リリースをクリックします。ソフトウェア リリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。
[Early Deployment (ED)] : これらのソフトウェア リリースには、新機能、新しいハードウェア プラットフォーム サポート、およびバグ修正ファイルが付属しています。
[Maintenance Deployment (MD)] : これらのソフトウェア リリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。
[Deferred (DF)] : これらは延期されたソフトウェア リリースです。アップグレードしたリリースに移行することを推奨します。
- f) ソフトウェア リリース番号を選択します。
- g) ファイル名 (*filename.aes*) をクリックします。
- h) [Download] をクリックします。
- i) シスコのエンド ユーザ ソフトウェアのライセンス契約を読み、[Agree] をクリックします。
- j) お使いのハード ドライブにファイルを保存します。
- k) ステップ a から k を繰り返して、他のファイルをダウンロードします。

ステップ 3 コントローラソフトウェアのイメージ (*filename.aes*) を TFTP サーバまたは FTP サーバのデフォルトディレクトリにコピーします。

ステップ 4 (任意) 802.11 ネットワークを無効にします。
(注) 使用率の高いネットワークやコントローラ、または小規模なコントローラ プラットフォームでは、予防措置として 802.11 ネットワークを無効にすることをお勧めします。

ステップ 5 コントローラ上のすべての WLAN を無効にします。

ステップ 6 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

ステップ 7 [File Type] ドロップダウン リストから、[Code] を選択します。

ステップ 8 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- TFTP
- FTP
- SFTP (7.4 以降のリリースで利用可能)

ステップ 9 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
TFTP サーバを使用している場合は、[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。

- ステップ 10** TFTP サーバを使用している場合は、[Maximum Retries] テキスト フィールドの 10 回の再試行、および [Timeout] テキスト フィールドの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は必要に応じて変更できます。変更する場合は、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバがソフトウェアのダウンロードを試行する時間（秒単位）を [Timeout] テキスト ボックスに入力します。
- ステップ 11** [File Path] テキスト ボックスに、ソフトウェアのディレクトリ パスを入力します。
- ステップ 12** [File Name] テキスト ボックスに、コントローラ ソフトウェア ファイルの名前 (*filename.aes*) を入力します。
- ステップ 13** FTP サーバを使用している場合は、次の手順に従います。
- [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 14** [Download] をクリックして、ソフトウェアをコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。
- ステップ 15** ダウンロードの完了後、[Reboot] をクリックします。
- ステップ 16** 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。
- ステップ 17** [OK] をクリックして確定します。
- ステップ 18** コントローラがリポートしたら、ステップ 6 から 17 を繰り返して、他のファイルをインストールします。
- ステップ 19** WLAN を再度有効にします。
- ステップ 20** Cisco WiSM2 の場合は、Catalyst スイッチのコントローラ ポート チャネルを再度有効にします。
- ステップ 21** ステップ 4 ので 802.11 ネットワークを無効にした場合は、再度有効にします。
- ステップ 22** コントローラ ソフトウェアのバージョンを確認するには、コントローラ GUI の [Monitor] を選択して、[Controller Summary] 領域の [Software Version] を参照してください。

コントローラ ソフトウェアのアップグレード (CLI)

- ステップ 1** コントローラ設定ファイルをサーバにアップロードしてバックアップします。
- (注) コントローラ ソフトウェアをアップグレードする前に、コントローラの設定ファイルをバックアップしておくことを強く推奨します。バックアップを行わなかった場合は、コントローラを手動で再設定する必要があります。
- ステップ 2** 次の手順に従って、コントローラ ソフトウェアのイメージを入手します。
- Cisco Software Center (<http://www.cisco.com/cisco/software/navigator.html>) を参照してください。
 - [Wireless] > [Wireless LAN Controller] を選択します。

[Integrated Controllers]、[Controller Modules]、および [Standalone Controllers] の各オプションがあります。

- c) 使用しているコントローラのプラットフォームに応じて、これらのオプションのいずれかをクリックします。
- d) コントローラのモデル番号または名前をクリックします。 [Download Software] ページが表示されます。
- e) コントローラソフトウェアリリースをクリックします。ソフトウェアリリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。
 - [Early Deployment (ED)] : これらのソフトウェアリリースには、新機能、新しいハードウェアプラットフォームサポート、およびバグ修正ファイルが付属しています。
 - [Maintenance Deployment (MD)] : これらのソフトウェアリリースには、バグ修正ファイルおよび現時点のソフトウェアメンテナンスが付属しています。
 - [Deferred (DF)] : これらは延期されたソフトウェアリリースです。アップグレードしたリリースに移行することを推奨します。
- f) ソフトウェアリリース番号を選択します。
- g) ファイル名 (*filename.aes*) をクリックします。
- h) [Download] をクリックします。
- i) シスコのエンドユーザソフトウェアのライセンス契約を読み、[Agree] をクリックします。
- j) お使いのハードドライブにファイルを保存します。
- k) ステップ a から k を繰り返して、他のファイルをダウンロードします。

ステップ 3 コントローラソフトウェアのイメージ (*filename.aes*) を TFTP サーバまたは FTP サーバのデフォルトディレクトリにコピーします。

ステップ 4 (任意) 802.11 ネットワークを無効にします。
 (注) 使用率の高いネットワークやコントローラ、または小規模なコントローラプラットフォームでは、予防措置として 802.11 ネットワークを無効にすることをお勧めします。

ステップ 5 コントローラ上のすべての WLAN を無効にします (`config wlan disable wlan_id` コマンドを使用)。

ステップ 6 コントローラの CLI にログインします。

ステップ 7 `ping server-ip-address` コマンドを入力して、コントローラが TFTP または FTP サーバと通信できることを確認します。

ステップ 8 `transfer download start` コマンドを入力して、現在のダウンロードの設定を表示します。プロンプトに `n` と応答して現在のダウンロード設定を表示します。

ステップ 9 必要に応じて、次のコマンドを入力して、ダウンロードの設定を変更します。

- `transfer download mode {tftp | ftp | sftp}`
- `transfer download datatype code`
- `transfer download serverip server-ip-address`
- `transfer download filename filename`
- `transfer download path server-path-to-file`

(注) TFTP または FTP サーバのパス名は、サーバのデフォルトまたはルートディレクトリからの相対パスです。たとえば、Solaris TFTP サーバの場合、パスは「/」となります。

TFTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download tftpMaxRetries retries**

- **transfer download tftpPktTimeout timeout**

(注) 10回の再試行および6秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を *retries* パラメータ、ソフトウェアのダウンロードを試行する時間の合計（秒単位）を *timeout* パラメータに入力します。

FTP サーバを使用している場合は、次のコマンドも入力します。

- **transfer download username username**

- **transfer download password password**

- **transfer download port port**

(注) port パラメータのデフォルト値は 21 です。

ステップ 10 `transfer download start` コマンドを入力して、現在の更新された設定を表示します。プロンプトに *y* と応答して、現在のダウンロード設定を確認し、ソフトウェアのダウンロードを開始します。

ステップ 11 次のコマンドを入力して、コードのアップデートを不揮発性RAM (NVRAM) に保存し、コントローラをリブートします。

reset system

コントローラのブートアッププロセスが完了します。

ステップ 12 コントローラがリブートしたら、ステップ6から11を繰り返して、他のファイルをインストールします。

ステップ 13 次のコマンドを入力して、WLAN を再び有効にします。

config wlan enable wlan_id

ステップ 14 Cisco WiSM の場合、Catalyst スイッチのコントローラ ポート チャネルを再度有効にします。

ステップ 15 ステップ 4 で 802.11 ネットワークを無効にした場合は、再度有効にします。

ステップ 16 インストールされているコントローラ ソフトウェアを確認するには、**show sysinfo** コマンドを入力して、製品バージョンを確認してください。

ステップ 17 コントローラにインストールされている Cisco Unified Wireless Network Controller Boot Software ファイルを確認するには、コントローラの CLI に **show sysinfo** コマンドを入力して、Field Recovery Image Version または Emergency Image Version を確認します。

(注) Cisco Unified Wireless Network Controller Boot Software ER.aes ファイルがインストールされていない場合は、Recovery Image Version または Emergency Image Version には「N/A」と表示されます。

アクセス ポイントへのイメージのプレダウンロード

ネットワークの停止を最小限に抑えるため、アクセス ポイントをリセットしたり、ネットワーク接続を切断したりせずに、アップグレードイメージをコントローラのアクセスポイントにダウン

ロードできるようになりました。以前は、アップグレードイメージをコントローラにダウンロードし、コントローラをリセットすると、アクセスポイントがディスカバリモードに移行してしまいました。アクセスポイントで新しいイメージを含むコントローラが検出されると、新しいイメージがダウンロードされ、アクセスポイントがリセットされ、ディスカバリモードに移行し、コントローラに再 join されます。

アップグレードイメージをコントローラにダウンロードしてから、ネットワークを稼働したままで、イメージをアクセスポイントにダウンロードできるようになりました。さらに、指定の期間のあと、または特定の日時に、コントローラおよびアクセスポイントのリポートをスケジュールすることができます。両方のデバイスが稼働している場合は、アクセスポイントによってコントローラが検出され、再 join されます。

アクセスポイントのプレダウンロードのプロセス

アクセスポイントのプレダウンロード機能は、次のように動作します。

- コントローラのイメージがダウンロードされます。
 - プライマリ イメージは、コントローラのバックアップ イメージになり、ダウンロードされたイメージが新しいプライマリ イメージになります。システム障害が発生した場合にコントローラがその最新の動作イメージでブートするように、**config boot backup** コマンドを使用してバックアップイメージとして現在のブートイメージを変更します。
 - 新しくダウンロードされたイメージに切り替えるには、**config ap image predownload primary all** コマンドを使用してアップグレードしたイメージのプレダウンロードを開始します。
 - アップグレードイメージがアクセスポイントにバックアップイメージとしてダウンロードされます。**show ap image all** コマンドを使用して、これを確認できます。
 - **config boot primary** コマンドを使用してブートイメージをプライマリ イメージに手動で変更し、アップグレードイメージをアクティブ化するためにコントローラをリポートします。
- または
 - **swap** キーワードによってスケジュールされたリポートを実行します。**swap** キーワードには重要な点があります。切り替えはアクセスポイント上のプライマリおよびバックアップイメージと、コントローラ上の現在アクティブなイメージおよびバックアップイメージに起こります。
 - コントローラをリポートすると、アクセスポイントのアソシエーションが解除され、最終的にアップグレードイメージで起動します。コントローラがアクセスポイントから送信されたディスカバリ要求に自身のディスカバリ応答パケットで応答すると、アクセスポイントから join 要求が送信されます。
- イメージの実際のアップグレードが実行されます。次の順序で処理が実行されます。
 - 起動時に、アクセスポイントは **join request** を送信します。
 - コントローラは、実行しているイメージバージョンと共に **join** 応答を返します。

- アクセスポイントは、自身が実行しているイメージとコントローラで実行されているイメージを比較します。バージョンが一致する場合は、アクセスポイントはコントローラに join します。
- バージョンが一致しない場合は、アクセスポイントはバックアップイメージのバージョンと比較します。これが一致した場合は、アクセスポイントではプライマリイメージとバックアップイメージを入れ替え、リロードした後、コントローラに join します。
- アクセスポイントのプライマリイメージがコントローラのイメージと同じである場合、アクセスポイントはリロードし、コントローラに join します。
- 上記の条件のいずれにも当てはまらない場合は、アクセスポイントはコントローラにイメージデータ要求を送信し、最新のイメージをダウンロードしてリロードし、コントローラに join します。

アクセスポイントへのイメージのプレダウロードの制限

- 同時にプレダウロードできる最大数は、通常のイメージを同時にダウンロードする数の半分に制限されます。この制限により、イメージのダウンロード中に、新しいアクセスポイントのコントローラに join が可能になります。
プレダウロードの制限に達すると、イメージを取得できなかったアクセスポイントは 180 ~ 600 秒間スリープ状態になり、その後、再度プレダウロードが試行されます。
- プレダウロードの前に、コントローラが何らかの理由でリブートした場合に、部分的にダウンロードしたアップグレードイメージではなく以前の実行イメージでバックアップされるように、アクティブなコントローラ ブート イメージをバックアップ イメージに変更する必要があります。
- アクセスポイントの使用可能なメモリの全容量が 16MB の場合（1130 および 1240 アクセスポイント）は、アップグレードイメージをダウンロードすると空き容量が不足するおそれがあるため、**crash info** ファイル、**radio** ファイル、およびすべてのバックアップイメージが自動的に削除され、空き容量が確保されます。ただし、プレダウロードイメージはアクセスポイントのバックアップイメージに置き換えられるため、この制限はプレダウロードプロセスには影響しません。
- **config time** コマンドを使用してシステム時刻を変更すると、スケジュールリセットに設定された時刻が有効ではなくなり、スケジュールされたシステムリセットはキャンセルされません。時刻を設定する前にスケジュールリセットをキャンセルするか、スケジュールリセットを保持して時刻を設定しないかを選択できます。
- すべてのプライマリ、セカンダリ、ターシャリコントローラで、同じイメージをプライマリイメージとバックアップイメージとして実行する必要があります。つまり、3つのコントローラすべてのプライマリイメージが X で、3つのコントローラすべてのセカンダリイメージが Y である必要があります。そうでない場合、機能は有効になりません。

- リセット時に、いずれかの AP がコントローラ イメージをダウンロードしている場合、スケジュール リセットはキャンセルされます。次のメッセージが表示され、スケジュールされたリセットがキャンセルされた理由が示されます。

```
%OSAPI-3-RESETSYSTEM_FAILED: osapi_task.c:4458 System will not reset as software is being upgraded.
```

- 7.2 以降のバージョンのイメージを Cisco Aironet 1240 のアクセス ポイントにプレダウンロードすることは、コントローラの以前のリリースからアップグレードする場合、サポートされません。Cisco Aironet 1240 のアクセス ポイントへのプレダウンロードが実行されると、AP は切断されます。

アクセス ポイントへのイメージのプレダウンロード：グローバル コンフィギュレーション (GUI)

ステップ 1 コントローラ設定ファイルをサーバにアップロードしてバックアップします。

- (注) コントローラ ソフトウェアをアップグレードする前に、コントローラの設定ファイルをバックアップしておくことを強く推奨します。バックアップを行わなかった場合は、コントローラを手動で再設定する必要があります。

ステップ 2 次の手順に従って、コントローラ ソフトウェアを入手します。

- Cisco Software Center (<http://www.cisco.com/cisco/software/navigator.html>) を参照します。
- 中央の選択ウィンドウから [Wireless] を選択します。
- [Wireless LAN Controllers] をクリックします。
[Integrated Controllers]、[Controller Modules]、および [Standalone Controllers] の各オプションがあります。
- 使用しているコントローラのプラットフォームに応じて、これらのオプションのいずれかをクリックします。
- コントローラのモデル番号または名前をクリックします。[Download Software] ページが表示されます。
- コントローラ ソフトウェア リリースをクリックします。ソフトウェア リリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。
[Early Deployment (ED)]：これらのソフトウェア リリースには、新機能、新しいハードウェアプラットフォーム サポート、およびバグ修正ファイルが付属しています。
[Maintenance Deployment (MD)]：これらのソフトウェア リリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。
[Deferred (DF)]：これらは延期されたソフトウェア リリースです。アップグレードしたリリースに移行することを推奨します。
- ソフトウェア リリース番号を選択します。
- ファイル名 (*filename.aes*) をクリックします。
- [Download] をクリックします。
- シスコのエンド ユーザ ソフトウェアのライセンス契約を読み、[Agree] をクリックします。
- お使いのハード ドライブにファイルを保存します。

l) ステップ a から k を繰り返して、他のファイルをダウンロードします。

- ステップ 3** コントローラソフトウェアのファイル (*filename.aes*) を TFTP サーバまたは FTP サーバのデフォルトディレクトリにコピーします。
- ステップ 4** (任意) コントローラ 802.11X ネットワークを無効にします。
(注) 使用率の高いネットワークやコントローラ、または小規模なコントローラ プラットフォームでは、予防措置として 802.11X ネットワークを無効にすることをお勧めします。
- ステップ 5** Cisco WiSM2 の場合、アクセスポイントでソフトウェアのダウンロードが開始される前にコントローラでリブートできるように、Catalyst スイッチのコントローラ ポート チャネルをシャットダウンします。
- ステップ 6** コントローラ上のすべての WLAN を無効にします。
- ステップ 7** [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。
- ステップ 8** [File Type] ドロップダウン リストから、[Code] を選択します。
- ステップ 9** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリリースで利用可能)
- ステップ 10** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
TFTP サーバを使用している場合は、[Maximum Retries] テキストボックスの 10 回の再試行および [Timeout] テキストボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。
- ステップ 11** TFTP サーバがソフトウェアのダウンロードを試行する最大回数を [Maximum Retries] テキストボックスに入力し、TFTP サーバがソフトウェアのダウンロードを試行する時間 (秒単位) を [Timeout] テキストボックスに入力します。
- ステップ 12** [File Path] テキスト ボックスに、ソフトウェアのディレクトリ パスを入力します。
- ステップ 13** [File Name] テキスト ボックスに、コントローラ ソフトウェア ファイルの名前 (*filename.aes*) を入力します。
- ステップ 14** FTP サーバを使用している場合は、次の手順に従います。
- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 15** [Download] をクリックして、ソフトウェアをコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。
- ステップ 16** アクセスポイントのイメージのプレダウンロードをグローバルに設定するには、[Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます。
- ステップ 17** [AP Image Pre-download] セクションで、次のいずれかを実行します。

- すべてのアクセス ポイントにプライマリ イメージをコントローラからプレダウンロードするよう指示する場合は、[AP Image Pre-download] で [Download Primary] をクリックします。
- すべてのアクセス ポイントにプライマリ イメージとバックアップ イメージを切り替えるよう指示する場合は、[Interchange Image] をクリックします。
- コントローラからイメージをダウンロードし、それをバックアップイメージとして保存する場合は、[Download Backup] をクリックします。
- プレダウンロード操作を中止するには、[Abort Predownload] をクリックします。

ステップ 18 [OK] をクリックします。

ステップ 19 [Apply] をクリックします。

アクセス ポイントへのイメージのプレダウンロードの設定 (GUI)

ステップ 1 コントローラ設定ファイルをサーバにアップロードしてバックアップします。

(注) コントローラ ソフトウェアをアップグレードする前に、コントローラの設定ファイルをバックアップしておくことを強く推奨します。バックアップを行わなかった場合は、コントローラを手動で再設定する必要があります。

ステップ 2 次の手順に従って、コントローラ ソフトウェアを入手します。

- Cisco Software Center (<http://www.cisco.com/cisco/software/navigator.html>) を参照します。
- 中央の選択ウィンドウから [Wireless] を選択します。
- [Wireless LAN Controllers] をクリックします。
[Integrated Controllers]、[Controller Modules]、および [Standalone Controllers] の各オプションがあります。
- 使用しているコントローラのプラットフォームに応じて、これらのオプションのいずれかをクリックします。
- コントローラのモデル番号または名前をクリックします。[Download Software] ページが表示されます。
- コントローラ ソフトウェア リリースをクリックします。ソフトウェア リリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。
[Early Deployment (ED)] : これらのソフトウェア リリースには、新機能、新しいハードウェアプラットフォーム サポート、およびバグ修正ファイルが付属しています。
[Maintenance Deployment (MD)] : これらのソフトウェア リリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。
[Deferred (DF)] : これらは延期されたソフトウェア リリースです。アップグレードしたリリースに移行することを推奨します。
- ソフトウェア リリース番号を選択します。
- ファイル名 (*filename.aes*) をクリックします。

- i) [Download] をクリックします。
- j) シスコのエンドユーザ ソフトウェアのライセンス契約を読み、[Agree] をクリックします。
- k) お使いのハード ドライブにファイルを保存します。
- l) ステップ a から k を繰り返して、他のファイルをダウンロードします。

ステップ 3 コントローラ ソフトウェアのファイル (*filename.aes*) を TFTP サーバまたは FTP サーバのデフォルトディレクトリにコピーします。

ステップ 4 (任意) 802.11 ネットワークを無効にします。
(注) 使用率の高いネットワークやコントローラ、または小規模なコントローラ プラットフォームでは、予防措置として 802.11 ネットワークを無効にすることをお勧めします。

ステップ 5 Cisco WiSM2 の場合、アクセス ポイントでソフトウェアのダウンロードが開始される前にコントローラでリポートできるように、Catalyst スイッチのコントローラ ポート チャネルをシャットダウンします。

ステップ 6 コントローラ上のすべての WLAN を無効にします。

ステップ 7 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

ステップ 8 [File Type] ドロップダウン リストから、[Code] を選択します。

ステップ 9 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- TFTP
- FTP
- SFTP (リリース 7.4 以降で使用可能)

ステップ 10 [IP Address] テキスト ボックスに、TFTP または FTP サーバの IP アドレスを入力します。
TFTP サーバを使用している場合は、[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。

ステップ 11 TFTP サーバがソフトウェアのダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバがソフトウェアのダウンロードを試行する時間 (秒単位) を [Timeout] テキスト ボックスに入力します。

ステップ 12 [File Path] テキスト ボックスに、ソフトウェアのディレクトリ パスを入力します。

ステップ 13 [File Name] テキスト ボックスに、コントローラ ソフトウェア ファイルの名前 (*filename.aes*) を入力します。

ステップ 14 FTP サーバを使用している場合は、次の手順に従います。

- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
- b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。

- c) [Server Port Number] テキストボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 15 [Download] をクリックして、ソフトウェアをコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 16 特定のアクセスポイントのプレダウンロードを設定するには、[Wireless] > [All APs] > [AP_Name] の順に選択して、選択した AP の [All AP Details] ページを開きます。

ステップ 17 [Advanced] タブをクリックします。

ステップ 18 [AP Image Pre-download] セクションで、次のいずれかを実行します。

- このアクセスポイントにプライマリイメージをコントローラからプレダウンロードするよう指示する場合は、[AP Image Pre-download] で [Download Primary] をクリックします。
- このアクセスポイントにプライマリイメージとバックアップイメージを切り替えるよう指示する場合は、[Interchange Image] をクリックします。
- コントローラからイメージをダウンロードし、それをバックアップイメージとして保存する場合は、[Download Backup] をクリックします。
- プレダウンロード操作を中止するには、[Abort Predownload] をクリックします。

ステップ 19 [OK] をクリックします。

ステップ 20 [Apply] をクリックします。

アクセスポイントへのイメージのプレダウンロード (CLI)

CLI を使用して、特定のアクセスポイントまたはすべてのアクセスポイントにイメージをプレダウンロードできます。

ステップ 1 次の手順に従って、コントローラソフトウェアを入手します。

- a) Cisco Software Center (<http://www.cisco.com/cisco/software/navigator.html>) を参照します。
- b) 中央の選択ウィンドウから [Wireless] を選択します。
- c) [Wireless LAN Controllers] をクリックします。
[Integrated Controllers]、[Controller Modules]、および [Standalone Controllers] の各オプションがあります。
- d) 使用しているコントローラのプラットフォームに応じて、これらのオプションのいずれかをクリックします。
- e) コントローラのモデル番号または名前をクリックします。[Download Software] ページが表示されます。
- f) コントローラソフトウェアリリースをクリックします。ソフトウェアリリースには、ダウンロードするリリースを判断する際に役立つように、次のようなラベルが付いています。
[Early Deployment (ED)] : これらのソフトウェアリリースには、新機能、新しいハードウェアプラットフォーム サポート、およびバグ修正ファイルが付属しています。

[Maintenance Deployment (MD)] : これらのソフトウェアリリースには、バグ修正ファイルおよび現時点のソフトウェア メンテナンスが付属しています。

[Deferred (DF)] : これらは延期されたソフトウェア リリースです。 アップグレードしたリリースに移行することを推奨します。

- g) ソフトウェア リリース番号を選択します。
- h) ファイル名 (*filename.aes*) をクリックします。
- i) [Download] をクリックします。
- j) シスコのエンドユーザ ソフトウェアのライセンス契約を読み、[Agree] をクリックします。
- k) お使いのハード ドライブにファイルを保存します。
- l) ステップ a から n を繰り返して、他のファイルをダウンロードします。

ステップ 2 コントローラ ソフトウェアのファイル (*filename.aes*) を TFTP サーバまたは FTP サーバのデフォルトディレクトリにコピーします。

ステップ 3 (任意) 802.11 ネットワークを無効にします。
(注) 使用率の高いネットワークやコントローラ、または小規模なコントローラ プラットフォームでは、予防措置として 802.11a/n ネットワークまたは 802.11b/g/n ネットワークを無効にすることを推奨します。

ステップ 4 Cisco WiSM2 の場合、アクセスポイントでソフトウェアのダウンロードが開始される前にコントローラでリブートできるように、Catalyst スイッチのコントローラ ポート チャネルをシャットダウンします。

ステップ 5 `config wlan disable wlan_id` コマンドを使用して、コントローラ上のすべての WLAN を無効にします。

ステップ 6 プレダウンロード イメージを受信するアクセス ポイントを指定します。
プレダウンロード先のアクセス ポイントを指定するには、次のコマンドのいずれかを使用します。

- プレダウンロード先のアクセス ポイントを指定するには、次のコマンドを入力します。

```
config ap image predownload {primary | backup} {ap_name | all}
```

プライマリ イメージが新しいイメージ、バックアップ イメージが古いイメージです。アクセス ポイントは常にプライマリ イメージでブートされます。

- アクセスポイントのプライマリ イメージとバックアップ イメージを切り替えるには、次のコマンドを入力します。

```
config ap image swap {ap_name | all}
```

- プレダウンロード先に指定されたアクセス ポイントの詳細情報を表示するには、次のコマンドを入力します。

```
show ap image {all | ap-name}
```

出力には、プレダウンロード用に指定されたアクセス ポイントがリストされ、各アクセス ポイントについて、プライマリ イメージおよびセカンダリ イメージのバージョン、プレダウンロード イメージのバージョン、プレダウンロードの試行時間 (必要な場合)、およびプレダウンロードの試行回数が見られます。また、出力には、各デバイスのプレダウンロードのステータスも示されます。アクセス ポイントのステータスは次のとおりです。

- None : プレダウンロード用のアクセス ポイントはスケジュールされません。

- **Predownloading** : アクセスポイントがイメージをプレダウンロードしています。
- **Not supported** : アクセスポイント (1120、1230、および 1310) が、プレダウンロードをサポートしていません。
- **Initiated** : 同時ダウンロード制限に達したため、アクセスポイントはプレダウンロードイメージを取得するために待機しています。
- **Failed** : アクセスポイントは 64 回、プレダウンロードの試行に失敗しました。
- **Complete** : アクセスポイントがプレダウンロードを完了しました。

ステップ 7 コントローラおよびアクセスポイントのリポート時間を設定します。
次のコマンドのいずれかを使用して、コントローラおよびアクセスポイントのリポートをスケジュールします。

- 次のコマンドを入力して、デバイスをリポートする前の遅延時間を指定します。

reset system in HH:MM:SS image {swap | no-swap} reset-aps [save-config]

(注) **reset** コマンドで **swap** オペランドを指定すると、コントローラとアクセスポイントの両方で、プライマリイメージとバックアップイメージが切り替えられます。

コントローラがすべての **join** されたアクセスポイントにリセットメッセージを送信したあと、コントローラはリセットされます。

- 次のコマンドを入力して、デバイスがリポートする日付と時刻を指定します。

reset system at YYYY-MM-DD HH:MM:SS image {swap | no-swap} reset-aps [save-config]

コントローラがすべての **join** されたアクセスポイントにリセットメッセージを送信したあと、コントローラはリセットされます。

(注) **reset** コマンドで **swap** オペランドを指定すると、コントローラとアクセスポイントの両方で、プライマリイメージとバックアップイメージが切り替えられます。

- 次のコマンドを入力して、次回のリセットを通知する SNMP トラップメッセージをセットアップします。

reset system notify-time minutes

コントローラでは、リセット前に通知トラップの設定された分数が送信されます。

- 次のコマンドを入力して、スケジュールされたリポートをキャンセルします。

reset system cancel

(注) リセット時間を設定して **config time** コマンドを使用し、コントローラのシステム時間を変更する場合、任意のスケジュールされたリセット時間はキャンセルされるため、システムの設定後にその時間を設定する必要があることがコントローラによって通知されます。

show reset コマンドを使用して、スケジュールされたリセットを表示します。

以下に類似した情報が表示されます。

```
System reset is scheduled for Apr 08 01:01:01 2010.
```

```
Current local time and date is Apr 07 02:57:44 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

コントローラとのファイルのやり取り

コントローラには、さまざまなファイルをアップロードまたはダウンロードするための組み込みユーティリティがあります。コントローラ GUI または CLI を使用してファイルをインポートするには、次の項の指示に従ってください。

- [ログインバナー ファイルのダウンロード](#)
- [デバイスの証明書のダウンロード](#)
- [CA 証明書のダウンロード](#)
- [PAC のアップロード](#)
- [設定ファイルのアップロードおよびダウンロード](#)

ログインバナー ファイルのダウンロード

ログインバナー ファイルのダウンロードは、GUI または CLI を使用して実行できます。ログインバナーとは、Telnet、SSH、およびコンソールポート接続を使用して、コントローラ GUI または CLI にアクセスしたときに、ユーザ認証の前にページに表示されるテキストのことです。

ログインバナー情報はテキストファイル (*.txt) で保存します。テキストファイルは 1296 文字以下、テキストは 16 行以下でなければなりません。



(注) ASCII 文字セットには、印刷可能な文字と印刷不可能な文字があります。ログインバナーでは、印刷可能な文字のみをサポートしています。

これはログインバナーの一例です。

```
Welcome to the Cisco Wireless Controller!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
```

この項の手順に従って、GUI または CLI を使用して、ログインバナーをコントローラにダウンロードします。ただし、ダウンロードを開始する前に、ファイルのダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。

- サービスポート経由でアップグレードする場合、サービスポートはルーティングできないため、TFTP または FTP サーバはサービスポートと同じサブネット上になければなりません。あるいは、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューションシステムネットワークポートを経由してアップグレードする場合、ディストリビューションシステムポートはルーティング可能なので、TFTP または FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。



(注) コントローラの設定をクリアしても、ログインバナーは削除されません。コントローラ GUI または CLI を使用したログインバナーの削除については、「[ログインバナーのクリア \(GUI\)](#)」の項を参照してください。



(注) コントローラには、1つのログインバナーファイルだけを含めることができます。別のログインバナーファイルをコントローラにダウンロードすると、最初のログインバナーファイルは上書きされます。

ログインバナー ファイルのダウンロード (GUI)

- ステップ 1** ログインバナー ファイルをサーバ上のデフォルトディレクトリにコピーします。
- ステップ 2** [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。
- ステップ 3** [File Type] ドロップダウン リストから、[Login Banner] を選択します。
- ステップ 4** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 5** [IP Address] テキスト ボックスに、ステップ 4 で選択したサーバタイプの IP アドレスを入力します。TFTP サーバを使用している場合は、[Maximum Retries] テキストボックスの 10 回の再試行および [Timeout] テキストボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。

- ステップ 6** TFTP サーバが証明書のダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバが証明書のダウンロードを試行する時間（秒単位）を [Timeout] テキスト ボックスに入力します。
- ステップ 7** [File Path] テキスト ボックスに、ログイン バナー ファイルのディレクトリ パスを入力します。
- ステップ 8** [File Name] テキスト ボックスに、ログイン バナー ファイル (*.txt) の名前を入力します。
- ステップ 9** FTP サーバを使用している場合は、次の手順に従います。
- [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 10** [Download] をクリックして、ログイン バナー ファイルをコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ログイン バナー ファイルのダウンロード (CLI)

- ステップ 1** コントローラの CLI にログインします。
- ステップ 2** 次のコマンドを入力して、設定ファイルのダウンロードに使用する転送モードを指定します。
transfer download mode {tftp | ftp | sftp}
- ステップ 3** 次のコマンドを入力して、コントローラのログイン バナーをダウンロードします。
transfer download datatype login-banner
- ステップ 4** 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。
transfer download serverip server-ip-address
- ステップ 5** 次のコマンドを入力して、ダウンロードする設定ファイルの名前を指定します。
transfer download path server-path-to-file
- ステップ 6** 次のコマンドを入力して、設定ファイルのディレクトリ パスを指定します。
transfer download filename filename.txt
- ステップ 7** TFTP サーバを使用している場合は、次のコマンドを入力します。
- transfer download tftpMaxRetries retries**
 - transfer download tftpPktTimeout timeout**
- (注) 10 回の再試行および 6 秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を *retries* パラメータ、ソフトウェアのダウンロードを試行する時間の合計（秒単位）を *timeout* パラメータに入力します。

ステップ 8 FTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

(注) port パラメータのデフォルト値は 21 です。

ステップ 9 **transfer download start** コマンドを入力して、ダウンロードの設定を表示します。現在の設定を確認してダウンロードプロセスを開始するプロンプトが表示されたら、y を入力します。

ログインバナーのクリア (GUI)

ステップ 1 [Commands] > [Login Banner] の順に選択して、[Login Banner] ページを開きます。

ステップ 2 [Clear] をクリックします。

ステップ 3 プロンプトが表示されたら、[OK] をクリックして、バナーをクリアします。
 コントローラ CLI を使用してコントローラからログインバナーをクリアするには、**clear login-banner** コマンドを入力します。

デバイスの証明書のダウンロード

各無線デバイス（コントローラ、アクセスポイント、およびクライアント）には独自のデバイスの証明書があります。たとえば、コントローラには、シスコによりインストールされたデバイスの証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレスクライアントの認証を行うために、EAP-FAST（PAC を使用していない場合）、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 により使用されます。ただし、ご自身のベンダー固有のデバイス証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。



(注) ローカル EAP の設定の詳細については、「ローカル EAP の設定」セクションを参照してください。

この項の手順に従って、GUI または CLI のいずれかを使用して、ベンダー固有のデバイスの証明書をコントローラにダウンロードします。ただし、ダウンロードを開始する前に、証明書のダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。

- サービスポート経由でアップグレードする場合、サービスポートはルーティングできないため、TFTP または FTP サーバはサービスポートと同じサブネット上になければなりません。あるいは、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューションシステムネットワークポートを経由してアップグレードする場合、ディストリビューションシステムポートはルーティング可能なので、TFTP または FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。



(注) コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

デバイスの証明書のダウンロード (GUI)

- ステップ 1** サーバ上のデフォルト ディレクトリにデバイス証明書をコピーします。
- ステップ 2** [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。
- ステップ 3** [File Type] ドロップダウンリストから、[Vendor Device Certificate] を選択します。
- ステップ 4** [Certificate Password] テキストボックスに、証明書を保護するために使用されたパスワードを入力します。
- ステップ 5** [Transfer Mode] ドロップダウンリストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 6** [IP Address] テキストボックスに、サーバの IP アドレスを入力します。
TFTP サーバを使用している場合は、[Maximum Retries] テキストボックスの 10 回の再試行および [Timeout] テキストボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。
- ステップ 7** TFTP サーバが証明書のダウンロードを試行する最大回数を [Maximum Retries] テキストボックスに入力し、TFTP サーバが証明書のダウンロードを試行する時間 (秒単位) を [Timeout] テキストボックスに入力します。
- ステップ 8** [File Path] テキストボックスに、証明書のディレクトリパスを入力します。
- ステップ 9** [File Name] テキストボックスに、証明書の名前を入力します。
- ステップ 10** FTP サーバを使用している場合は、次の手順に従います。

- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
- b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
- c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

ステップ 11 [Download] をクリックして、デバイスの証明書をコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。

ステップ 12 ダウンロードの完了後、[Commands] > [Reboot] > [Reboot] の順に選択します。

ステップ 13 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。

ステップ 14 [OK] をクリックし、変更内容を確定してコントローラをリブートします。

デバイスの証明書のダウンロード (CLI)

ステップ 1 コントローラの CLI にログインします。

ステップ 2 次のコマンドを入力して、設定ファイルのダウンロードに使用する転送モードを指定します。
transfer download mode {tftp | ftp | sftp}

ステップ 3 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。
transfer download datatype eapdevcert

ステップ 4 次のコマンドを入力して、証明書の秘密キーを指定します。
transfer download certpassword password

ステップ 5 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。
transfer download serverip server-ip-address

ステップ 6 次のコマンドを入力して、ダウンロードする設定ファイルの名前を指定します。
transfer download path server-path-to-file

ステップ 7 次のコマンドを入力して、設定ファイルのディレクトリ パスを指定します。
transfer download filename filename.pem

ステップ 8 TFTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

(注) 10 回の再試行および 6 秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を *retries* パラメータ、ソフトウェアのダウンロードを試行する時間の合計 (秒単位) を *timeout* パラメータに入力します。

ステップ 9 FTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

(注) port パラメータのデフォルト値は 21 です。

ステップ 10 **transfer download start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してダウンロードプロセスを開始するプロンプトが表示されたら、y と答えます。

ステップ 11 次のコマンドを入力して、コントローラをリブートします。
reset system

CA 証明書のダウンロード

コントローラとアクセスポイントには、デバイスの証明書の署名と確認に使用される Certificate Authority (CA; 認証局) の証明書があります。コントローラには、シスコによりインストールされた CA 証明書が付属しています。この証明書は、ローカル EAP 認証時にワイヤレスクライアントの認証を行うために、EAP-FAST (PAC を使用していない場合)、EAP-TLS、PEAP-GTC、および PEAP-MSCHAPv2 により使用できます。ただし、ご自身のベンダー固有の CA 証明書を使用する場合は、証明書をコントローラにダウンロードする必要があります。



(注) ローカル EAP の設定の詳細については、「ローカル EAP の設定」セクションを参照してください。

この項の手順に従って、GUI または CLI のいずれかを介して、CA 証明書をコントローラにダウンロードします。ただし、ダウンロードを開始する前に、証明書のダウンロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。

- サービスポート経由でアップグレードする場合、サービスポートはルーティングできないため、TFTP または FTP サーバはサービスポートと同じサブネット上になければなりません。あるいは、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューションシステムネットワークポートを経由してアップグレードする場合、ディストリビューションシステムポートはルーティング可能なので、TFTP または FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用するため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。



(注) コントローラにダウンロードする証明書はすべて、PEM 形式でなければなりません。

CA 証明書のダウンロード (GUI)

- ステップ 1** サーバ上のデフォルト ディレクトリに CA 証明書をコピーします。
- ステップ 2** [Commands] > [Download File] を選択して、[Download File to Controller] ページを開きます。
- ステップ 3** [File Type] ドロップダウン リストから、[Vendor CA Certificate] を選択します。
- ステップ 4** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 5** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
TFTP サーバを使用している場合は、[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。
- ステップ 6** TFTP サーバが証明書のダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバが証明書のダウンロードを試行する時間 (秒単位) を [Timeout] テキスト ボックスに入力します。
- ステップ 7** [File Path] テキスト ボックスに、証明書のディレクトリ パスを入力します。
- ステップ 8** [File Name] テキスト ボックスに、証明書の名前を入力します。
- ステップ 9** FTP サーバを使用している場合は、次の手順に従います。
- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 10** [Download] をクリックして、CA 証明書をコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示されます。
- ステップ 11** ダウンロードの完了後、[Commands] > [Reboot] > [Reboot] の順に選択します。
- ステップ 12** 変更を保存するように求めるプロンプトが表示されたら、[Save and Reboot] をクリックします。
- ステップ 13** [OK] をクリックし、変更内容を確定してコントローラをリブートします。

CA 証明書のダウンロード (CLI)

-
- ステップ 1** コントローラ CLI にログインします。
- ステップ 2** 次のコマンドを入力して、設定ファイルのダウンロードに使用する転送モードを指定します。
transfer download mode {*tftp* | *ftp* | *sftp*}
- ステップ 3** 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。
transfer download datatype *capdevcert*
- ステップ 4** 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。
transfer download serverip *server-ip-address*
- ステップ 5** 次のコマンドを入力して、設定ファイルのディレクトリパスを指定します。
transfer download path *server-path-to-file*
- ステップ 6** 次のコマンドを入力して、ダウンロードする設定ファイルの名前を指定します。
transfer download filename *filename.pem*
- ステップ 7** TFTP サーバを使用している場合は、次のコマンドを入力します。
- **transfer download tftpMaxRetries** *retries*
 - **transfer download tftpPktTimeout** *timeout*
- (注) 10 回の再試行および 6 秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を *retries* パラメータ、ソフトウェアのダウンロードを試行する時間の合計 (秒単位) を *timeout* パラメータに入力します。
- ステップ 8** FTP サーバを使用している場合は、次のコマンドを入力します。
- **transfer download username** *username*
 - **transfer download password** *password*
 - **transfer download port** *port*
- (注) *port* パラメータのデフォルト値は 21 です。
- ステップ 9** **transfer download start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してダウンロードプロセスを開始するプロンプトが表示されたら、*y* と答えます。
- ステップ 10** **reset system** コマンドを入力して、コントローラをリブートします。
-

PAC のアップロード

Protected Access Credential (PAC) は、自動または手動でプロビジョニングされる資格情報で、EAP-FAST 認証時にローカル EAP 認証で相互認証を実行するために使用されます。手動の PAC プロビジョニングが有効になっている場合、PAC ファイルはコントローラ上で手動で生成されません。

この項の手順に従って、GUI または CLI のいずれかを使用して、コントローラから PAC を生成してロードします。ただし、開始する前に、PAC のアップロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。

- サービスポート経由でアップロードする場合は、TFTP/FTP サーバがサービスポートと同じサブネット上になければなりません。サービスポートはルーティングできないからです。同じサブネット上にない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューションシステムネットワークポートを経由してアップロードする場合は、TFTP/FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。ディストリビューションシステムポートはルーティング可能であるためです。
- Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。

PAC のアップロード (GUI)

-
- ステップ 1** [Commands] > [Upload File] の順に選択して、[Upload File from Controller] ページを開きます。
- ステップ 2** [File Type] ドロップダウン リストから、[PAC (Protected Access Credential)] を選択します。
- ステップ 3** [User] テキストボックスに、PAC を使用するユーザ名を入力します。
- ステップ 4** [Validity] テキストボックスに、PAC が有効である日数を入力します。デフォルトの設定は、ゼロ (0) です。
- ステップ 5** [Password] テキストボックスおよび [Confirm Password] テキストボックスに、PAC を保護するためのパスワードを入力します。
- ステップ 6** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP

- SFTP (7.4 以降のリリースで利用可能)

- ステップ 7** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
- ステップ 8** [File Path] テキスト ボックスに、PAC のディレクトリ パスを入力します。
- ステップ 9** [File Name] テキスト ボックスに、PAC ファイルの名前を入力します。PAC ファイルには .pac 拡張子が付いています。
- ステップ 10** FTP サーバを使用している場合は、次の手順に従います。
- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、FTP サーバ上のアップロードが行われるポート番号を入力します。デフォルト値は 21 です。
- ステップ 11** [Upload] をクリックして、コントローラから PAC をアップロードします。アップロードのステータスを示すメッセージが表示されます。
- ステップ 12** ワイヤレスクライアントの手順に従って、クライアントデバイス上に PAC をアップロードします。必ず上記で入力したパスワードを使用するようにしてください。

PAC のアップロード (CLI)

- ステップ 1** コントローラ CLI にログインします。
- ステップ 2** 次のコマンドを入力して、設定ファイルのアップロードに使用する転送モードを指定します。
transfer upload mode {tftp | ftp | sftp}
- ステップ 3** 次のコマンドを入力して、Protected Access Credential (PAC) をアップロードします。
transfer upload datatype pac
- ステップ 4** 次のコマンドを入力して、ユーザ ID を指定します。
transfer upload pac username validity password
- ステップ 5** 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。
transfer upload serverip server-ip-address
- ステップ 6** 次のコマンドを入力して、設定ファイルのディレクトリ パスを指定します。
transfer upload path server-path-to-file
- ステップ 7** 次のコマンドを入力して、アップロードする設定ファイルの名前を指定します。
transfer upload filename manual.pac
- ステップ 8** FTP サーバを使用している場合は、次のコマンドを入力します。
- **transfer upload username username**

- **transfer upload password** *password*
- **transfer upload port** *port*

(注) port パラメータのデフォルト値は 21 です。

ステップ 9 **transfer upload start** コマンドを入力して、更新された設定を表示します。現在の設定を確認してアップロードプロセスを開始するプロンプトが表示されたら、**y** と答えます。

ステップ 10 ワイヤレスクライアントの手順に従って、クライアントデバイス上に PAC をアップロードします。必ず上記で入力したパスワードを使用するようにしてください。

設定ファイルのアップロードおよびダウンロード

コントローラの設定ファイルをバックアップのためにサーバにアップロードすることを推奨します。設定が失われた場合には、保存した設定をコントローラにダウンロードすることができます。



(注) 別のコントローラ プラットフォームからアップロードした設定ファイルをダウンロードしないよう注意してください。たとえば、Cisco 5500 シリーズコントローラでは、Cisco 2500 シリーズコントローラの設定ファイルはサポートしていません。

設定ファイルを使用する場合は、次の注意事項に従ってください。

- 無効な値を含む CLI はフィルタで除外され、XML 検証エンジンによってデフォルトに設定されます。検証はブートアップ中に行われます。検証に失敗した場合は、設定が拒否されることがあります。無効な CLI を使用すると、設定が失敗するおそれがあります。たとえば、WLAN を追加するための適切なコマンドを追加しないで WLAN を設定しようとする CLI を使用する可能性があります。
- 依存関係が正しくない場合は、設定が拒否されることがあります。たとえば、**add** コマンドを使用せずに、依存パラメータを設定しようとした場合です。XML 検証は正しく行われる場合がありますが、設定のダウンロードインフラストラクチャは検証エラーなしでただちに設定を拒否します。
- 無効な設定は、**show invalid-config** コマンドを使用して確認できます。**show invalid-config** コマンドは、ダウンロードプロセスの一部として、または XML 検証インフラストラクチャによって、コントローラから拒否された設定を報告します。



(注) 設定ファイルを読んで変更することもできます。

設定ファイルのアップグレード

GUI または CLI のいずれかを使用して、設定ファイルをアップロードできます。

設定ファイルのアップロード (GUI)

-
- ステップ 1** [Commands] > [Upload File] の順に選択して、[Upload File from Controller] ページを開きます。
- ステップ 2** [File Type] ドロップダウンリストから [Configuration] を選択します。
- ステップ 3** 設定ファイルを暗号化します。[Configuration File Encryption] チェックボックスをオンにして、[Encryption Key] テキスト ボックスに暗号キーを入力します。
- ステップ 4** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 5** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
- ステップ 6** [File Path] テキスト ボックスに、設定ファイルのディレクトリ パスを入力します。
- ステップ 7** [File Name] テキスト ボックスに、設定ファイルの名前を入力します。
- ステップ 8** FTP サーバを使用している場合は、次の手順に従います。
- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、FTP サーバ上のアップロードが行われるポート番号を入力します。デフォルト値は 21 です。
- ステップ 9** [Upload] をクリックして、設定ファイルをサーバにアップロードします。アップロードのステータスを示すメッセージが表示されます。アップロードに失敗すると、この手順が繰り返され、再試行されます。
-

設定ファイルのアップロード (CLI)

-
- ステップ 1** 次のコマンドを入力して、設定ファイルのアップロードに使用する転送モードを指定します。
transfer upload mode {tftp | ftp | sftp}
- ステップ 2** 次のコマンドを入力して、アップロードするファイルのタイプを指定します。
transfer upload datatype config
- ステップ 3** 次のコマンドを入力して、設定ファイルを暗号化します。
- **transfer encrypt enable**
 - **transfer encrypt set-key key** (key はファイルの暗号化に使用する暗号キーです)

ステップ 4 次のコマンドを入力して、サーバの IP アドレスを指定します。

transfer upload serverip *server-ip-address*

ステップ 5 次のコマンドを入力して、設定ファイルのディレクトリパスを指定します。

transfer upload path *server-path-to-file*

ステップ 6 次のコマンドを入力して、アップロードする設定ファイルの名前を指定します。

transfer upload filename *filename*

ステップ 7 FTP サーバを使用している場合、FTP サーバへのログインで使用するユーザ名およびパスワード、アップロードが発生するポート番号を指定するには、次のコマンドを入力します。

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

(注) port パラメータのデフォルト値は 21 です。

ステップ 8 次のコマンドを入力して、アップロードプロセスを開始します。

transfer upload start

ステップ 9 現在の設定を確認するプロンプトが表示されたら、**y** と答えます。以下に類似した情報が表示されます。

```
Mode..... TFTP
TFTP Server IP..... 10.10.10.4
TFTP Path..... Config/
TFTP Filename..... AS_4402_4_2_55_8_Config.xml
Data Type..... Config File
Encryption..... Disabled
```

```
*****
*** WARNING: Config File Encryption Disabled ***
*****
```

```
Are you sure you want to start? (y/N) Y
File transfer operation completed successfully.
```

アップロードに失敗すると、この手順が繰り返され、再試行されます。

設定ファイルのダウンロード

GUI または CLI のいずれかを使用して、設定ファイルをダウンロードできます。

設定ファイルのダウンロード (GUI)

-
- ステップ 1** [Commands] > [Download File] を選択して、[Download File to Controller] ページを開きます。
- ステップ 2** [File Type] ドロップダウン リストから [Configuration] を選択します。
- ステップ 3** 設定ファイルが暗号化されている場合は、[Configuration File Encryption] チェックボックスをオンにして、[Encryption Key] テキスト ボックスにファイルの暗号化解除に使用する暗号キーを入力します。
(注) ここで入力するキーは、アップロードプロセス中に入力したキーと一致させる必要があります。
- ステップ 4** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 5** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
TFTP サーバを使用している場合は、[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。
- ステップ 6** TFTP サーバが設定ファイルのダウンロードを試行する最大回数を [Maximum Retries] テキスト ボックスに入力し、TFTP サーバが設定ファイルのダウンロードを試行する時間 (秒単位) を [Timeout] テキスト ボックスに入力します。
- ステップ 7** [File Path] テキスト ボックスに、設定ファイルのディレクトリ パスを入力します。
- ステップ 8** [File Name] テキスト ボックスに、設定ファイルの名前を入力します。
- ステップ 9** FTP サーバを使用している場合は、次の手順に従います。
- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 10** [Download] をクリックして、ファイルをコントローラにダウンロードします。ダウンロードのステータスを示すメッセージが表示され、コントローラが自動的にリブートされます。ダウンロードに失敗すると、この手順が繰り返され、再試行されます。
-

設定ファイルのダウンロード (CLI)



(注) コントローラは差分設定のダウンロードをサポートしていません。設定ファイルには、ダウンロードが正常に完了するのに必要なすべてのコマンド（すべてのインターフェイスアドレス コマンド、読み取りおよび書き込み権限を持つ `mgmtuser` コマンド、およびインターフェイスポートまたはLAGを有効または無効にするコマンド）が含まれています。たとえば、設定ファイルの一部として `config time ntp server index server_address` コマンドのみをダウンロードすると、ダウンロードは失敗します。設定ファイルに含まれるコマンドだけがコントローラに適用されるため、ダウンロード前のコントローラの設定はすべて削除されます。

ステップ 1 次のコマンドを入力して、設定ファイルのダウンロードに使用する転送モードを指定します。

transfer download mode {tftp | ftp | sftp}

ステップ 2 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer download datatype config

ステップ 3 設定ファイルが暗号化されている場合は、次のコマンドを入力します。

- **transfer encrypt enable**
- **transfer encrypt set-key key**、ここで、*key* はファイルの暗号化解除に使用する暗号キーです。

(注) ここで入力するキーは、アップロードプロセス中に入力したキーと一致させる必要があります。

ステップ 4 次のコマンドを入力して、TFTP または FTP サーバの IP アドレスを指定します。

transfer download serverip server-ip-address

ステップ 5 次のコマンドを入力して、設定ファイルのディレクトリパスを指定します。

transfer download path server-path-to-file

ステップ 6 次のコマンドを入力して、ダウンロードする設定ファイルの名前を指定します。

transfer download filename filename

ステップ 7 TFTP サーバを使用している場合は、次のコマンドを入力します。

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

(注) 10 回の再試行および 6 秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。値を変更するには、TFTP サーバがソフトウェアのダウンロードを試行する最大回数を *retries* パラメータ、ソフトウェアのダウンロードを試行する時間の合計（秒単位）を *timeout* パラメータに入力します。

ステップ 8 FTP サーバを使用している場合、FTP サーバへのログインで使用するユーザ名およびパスワード、ダウンロードが発生するポート番号を指定するには、次のコマンドを入力します。

- **transfer upload username username**
- **transfer upload password password**

- **transfer upload port port**

(注) port パラメータのデフォルト値は 21 です。

ステップ 9 次のコマンドを入力して、更新された設定を表示します。

transfer download start

ステップ 10 現在の設定を確認し、ダウンロードプロセスを開始するプロンプトが表示されたら、y と答えます。以下に類似した情報が表示されます。

```
Mode..... TFTP
TFTP Server IP..... 10.10.10.4
TFTP Path..... Config/
TFTP Filename..... AS_4402_4_2_55_8_Config.xml
Data Type..... Config File
Encryption..... Disabled
```

```
*****
*** WARNING: Config File Encryption Disabled ***
*****
```

```
Are you sure you want to start? (y/N) y
```

```
File transfer operation completed successfully.
```

ダウンロードに失敗すると、この手順が繰り返され、再試行されます。

設定の保存

コントローラには、揮発性メモリと不揮発性メモリの2種類のメモリが搭載されています。次のいずれかのコマンドを使用して、アクティブな揮発性 RAM から不揮発性 RAM (NVRAM) に設定の変更を随時保存できます。

- **save config** : コントローラをリセットせずに、揮発性メモリから不揮発性メモリに設定を保存できます。
- **reset system** : コントローラをリブートする前に、設定の変更を保存するかどうかを確認するプロンプトが表示されます。
- **logout** : ログアウトの前に、設定の変更を保存するかどうかを確認するプロンプトが表示されます。

設定ファイルの編集

コントローラの設定を保存すると、コントローラはそれを XML 形式でフラッシュメモリに格納します。コントローラソフトウェアリリース 5.2 以降のリリースでは、設定ファイルを CLI 形式に変換し、簡単に読み取ったり修正したりすることができます。設定ファイルを TFTP、FTP、または SFTP サーバにアップロードすると、コントローラでは XML から CLI への変換が開始されます。さらに、サーバ上で CLI 形式の設定ファイルを読み取ったり、編集したりすることができます。操作を完了したら、コントローラにファイルをダウンロードして、XML 形式に再度変換し、保存します。

ステップ 1 次のいずれかを実行して、設定ファイルを TFTP、FTP、または SFTP サーバにアップロードします。

- コントローラ GUI を使用してファイルをアップロードします。
- コントローラ CLI を使用してファイルをアップロードします。

ステップ 2 サーバの設定ファイルを読み取るか、編集します。既存の CLI コマンドを修正または削除して、新しい CLI コマンドをファイルに追加できます。

(注) 設定ファイルを編集するには、Windows のメモ帳、ワードパッド、または Linux の VI エディタのいずれかを使用できます。

ステップ 3 変更をサーバ上の設定ファイルに保存します。

ステップ 4 次のいずれかを実行して、設定ファイルをコントローラにダウンロードします。

- コントローラ GUI を使用してファイルをダウンロードします。
- コントローラ CLI を使用してファイルをダウンロードします。

コントローラでは、設定ファイルが XML 形式に変換されて、フラッシュメモリに保存され、新しい設定を使用してリポートされます。既知のキーワードおよび正しい構文を持つ CLI コマンドは XML に変換されますが、不適切な CLI コマンドは無視されてフラッシュメモリに保存されます。無効な値を持つすべての CLI コマンドはデフォルトの値に置き換えられます。無視されたコマンドおよび無効な設定値を確認するには、次のコマンドを入力します。

show invalid-config

(注) このコマンドは **clear config** または **save config** コマンドのあとには実行できません。

ステップ 5 ダウンロードした設定に多数の無効な CLI コマンドが含まれている場合、分析のため、無効な設定を TFTP または FTP サーバにアップロードできます。無効な設定をアップロードするには、次のいずれかを実行します。

- コントローラ GUI を使用して無効な設定をアップロードします。「設定ファイルのアップロード (GUI)」の項の説明に従いますが、ステップ 2 で [File Type] ドロップダウンリストから [Invalid Config] を選択して、ステップ 3 をスキップします。

- コントローラ CLI を使用して無効な設定をアップロードします。「設定ファイルのアップロード (CLI)」の項の説明に従いますが、ステップ2で **transfer upload datatype invalid-config** コマンドを入力して、ステップ3をスキップします。

ステップ6 コントローラは、ポート設定CLIコマンドのアップロードおよびダウンロードをサポートしていません。コントローラ ポートを設定する場合は、次のコマンドを入力します。

- **config port linktrap** {port | all} {enable | disable} : 特定のコントローラ ポートまたはすべてのポートでアップリンク トラップおよびダウンリンク トラップを有効または無効にします。
- **config port adminmode** {port | all} {enable | disable} : 特定のコントローラ ポートまたはすべてのポートで管理モードを有効または無効にします。

ステップ7 次のコマンドを入力して、変更を保存します。
save config

コントローラの設定のクリア

ステップ1 次のコマンドを入力して、設定をクリアします。
clear config

操作を確認するプロンプトが表示されたら、**y** と入力します。

ステップ2 次のコマンドを入力して、システムをリブートします。
reset system

設定の変更を保存せずにリブートするには、**n** と入力します。コントローラをリブートすると、設定ウィザードが自動的に起動されます。

ステップ3 「設定ウィザードを使用したコントローラの設定」の項の説明に従って、初期設定を実行します。

コントローラ設定の消去

ステップ1 次のコマンドを入力して、設定をリセットします。
reset system

確認のプロンプトで**y** と入力して、設定変更を不揮発性メモリに保存します。コントローラがリブートします。

ステップ 2 ユーザ名の入力を求められたら、次のコマンドを入力して工場出荷時の設定に戻します。

recover-config

コントローラをリブートすると、設定ウィザードが自動的に起動します。

ステップ 3 「設定ウィザードを使用したコントローラの設定」の項の説明に従って、初期設定を実行します。

コントローラのリセット

次の2つの方法のうちいずれかを使用して、コントローラをリセットし、CLI コンソールにリブート処理を表示することができます。

- コントローラを一度オフにし、再びオンにします。
- CLI で `reset system` と入力します。確認のプロンプトで `y` と入力して、設定変更を不揮発性メモリに保存します。コントローラがリブートします。

コントローラがリブートすると、CLI コンソールに次のリブート情報が表示されます。

- システムの初期化。
- ハードウェア設定の検証。
- マイクロコードのメモリへのロード。
- オペレーティング システム ソフトウェアのロードの検証。
- 保存されている設定による初期化。
- ログイン プロンプトの表示。



第 23 章

ユーザ アカウントの管理

- [ゲストユーザ アカウントの設定, 237 ページ](#)
- [管理者のユーザ名とパスワードの設定, 241 ページ](#)
- [SNMP v3 ユーザのデフォルト値の変更, 242 ページ](#)
- [証明書署名要求の生成, 244 ページ](#)

ゲスト ユーザ アカウントの設定

ゲスト アカウントの作成について

コントローラは、WLAN 上でゲストユーザアクセスを提供できます。ゲストユーザアカウント作成の最初の手順では、ロビーアンバサダーアカウントとしても知られる、ロビー管理者ユーザを作成します。このアカウントを作成すると、ロビーアンバサダーはゲストユーザアカウントをコントローラ上で作成および管理できます。ロビーアンバサダーは、限定的な設定権限を持ち、ゲストアカウントを管理するために使用する Web ページのみにアクセスできます。

ロビーアンバサダーは、ゲストユーザアカウントを利用できる時間を指定できます。指定した時間を経過すると、ゲストユーザアカウントは、自動的に無効になります。

ユーザ アカウントの管理に関する制限

ローカルユーザデータベースは、最大エン트리数が 2048（デフォルト値）に制限されています。データベースは、ローカル管理ユーザ（ロビーアンバサダーを含む）、ローカルネットワークユーザ（ゲストユーザを含む）、MAC フィルタエン트리、除外リストエン트리、およびアクセスポイントの許可リストエン트리で共有します。これらを合わせて、設定されている最大値を超えることはできません。

Lobby Ambassador アカウントの作成

ロビー アンバサダー アカウントの作成 (GUI)

-
- ステップ 1** [Management] > [Local Management Users] の順に選択して、[Local Management Users] ページを開きます。このページには、ローカル管理ユーザの名前やアクセス権限の一覧が表示されます。
- (注) コントローラから任意のユーザアカウントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。ただし、デフォルトの管理ユーザを削除すると、GUI および CLI によるコントローラへのアクセスは両方とも禁止されます。したがって、デフォルトのユーザを削除する前に、管理権限 (ReadWrite) を持つユーザを作成しなければなりません。
- ステップ 2** [New] をクリックして、ロビー アンバサダー アカウントを作成します。[Local Management Users > New] ページが表示されます。
- ステップ 3** [User Name] テキスト ボックスに、ロビー アンバサダー アカウントのユーザ名を入力します。
- (注) 管理ユーザ名は、すべて単一データベース内に保存されるため、一意である必要があります。
- ステップ 4** [Password] テキスト ボックスおよび [Confirm Password] テキスト ボックスに、ロビー アンバサダー アカウントのパスワードを入力します。
- (注) パスワードは大文字と小文字が区別されます。管理の [User Details] のパラメータの設定は、[Password Policy] ページで行う設定によって異なります。パスワードについて、次の要件が実施されます。
- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
 - パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
 - パスワードに管理ユーザ名やユーザ名を逆にした文字列を含めることはできません。
 - パスワードには、Cisco、ocsic、admin、nimda などの単語や、大文字と小文字を変更する、および 1、|、または ! を代用する、または o の代わりに 0、s の代わりに \$ を使用することで作成したバリエーションを含めることはできません。
- ステップ 5** [User Access Mode] ドロップダウン リストから [LobbyAdmin] を選択します。このオプションを使用すると、ロビー アンバサダーでゲストユーザアカウントを生成できます。
- (注) [ReadOnly] オプションでは、読み取り専用の権限を持つアカウントを作成し、[ReadWrite] オプションでは、読み取りと書き込みの両方の権限を持つ管理アカウントを作成します。
- ステップ 6** [Apply] をクリックして、変更を確定します。ローカル管理ユーザのリストに、新しいロビー アンバサダー アカウントが表示されます。
- ステップ 7** [Save Configuration] をクリックして、変更を保存します。
-

ロビー アンバサダー アカウントの作成 (CLI)

ロビー アンバサダー アカウントを作成するには、次のコマンドを使用します。

```
config mgmtuser add lobbyadmin_username lobbyadmin_pwd lobby-admin
```



(注) **lobby-admin** を **read-only** に置き換えると、読み取り専用の権限を持つアカウントを作成します。**lobby-admin** を **read-write** に置き換えると、読み取りと書き込みの両方の権限を持つ管理アカウントを作成します。

ロビー アンバサダーとしてのゲストユーザアカウントの作成 (GUI)

- ステップ 1** ユーザ名とパスワードを使用して、ロビー アンバサダーとしてコントローラにログインします。 [Lobby Ambassador Guest Management] > [Guest Users List] ページが表示されます。
- ステップ 2** [New] をクリックして、ゲストユーザアカウントを作成します。 [Lobby Ambassador Guest Management] > [Guest Users List > New] ページが表示されます。
- ステップ 3** [User Name] テキスト ボックスに、ゲスト ユーザの名前を入力します。最大 24 文字を入力することができます。
- ステップ 4** 次のいずれかの操作を行います。
- このゲストユーザ用のパスワードを自動的に生成する場合は、[Generate Password] チェックボックスをオンにします。生成されたパスワードは、[Password] テキスト ボックスおよび [Confirm Password] テキスト ボックスに自動的に入力されます。
 - このゲストユーザ用にパスワードを作成する場合は、[Generate Password] チェックボックスをオフのままにし、[Password] および [Confirm Password] の両テキスト ボックスにパスワードを入力します。
- (注) パスワードは最大 24 文字まで含めることができ、大文字と小文字が区別されません。
- ステップ 5** [Lifetime] ドロップダウンリストから、このゲストユーザアカウントをアクティブにする時間（日数、時間数、分数、秒数）を選択します。4 つのテキスト ボックスの値をすべてゼロ (0) にすると、永続的なアカウントとなります。
- デフォルト：1 日
- 範囲：5 分から 30 日
- (注) 小さい方の値、またはゲストアカウントが作成された WLAN であるゲスト WLAN のセッションタイムアウトが、優先します。たとえば、WLAN セッションのタイムアウトが 30 分でも、ゲストアカウントのライフタイムが 10 分の場合、アカウントはゲストアカウントの失効に従い、10 分で削除されます。同様に、WLAN セッションがゲストアカウントのライフタイムより前にタイムアウトする場合、クライアントは、再認証を要求するセッションタイムアウトを繰り返すこととなります。

(注) ゼロ以外の値がライフタイムに設定されているゲストユーザアカウントの値は、アカウントがアクティブになっている間、いつでも別の値に変更できます。しかし、コントローラ GUI を使用してゲストユーザアカウントを永続的なアカウントにするには、そのアカウントを一度削除した後、再度アカウントを作成しなければなりません。必要に応じて、**config netuser lifetime user_name 0** コマンドを使用すれば、アカウントを削除してから再度作成することなく、ゲストユーザアカウントを永続的なアカウントにすることができます。

ステップ 6 [WLAN SSID] ドロップダウン リストから、ゲストユーザが使用する SSID を選択します。表示された WLAN だけが、レイヤ 3 の Web 認証が設定された WLAN です。

(注) 潜在的な競合を阻止するために、特定のゲスト WLAN を作成することを推奨します。ゲストアカウントの有効期限が切れ、RADIUS サーバ上でアカウント名が競合し、両アカウントとも同じ WLAN 上にある場合、両アカウントにアソシエートしているユーザのアソシエートが解除されてから、ゲストアカウントが削除されます。

ステップ 7 [Description] テキスト ボックスに、ゲストユーザアカウントの説明を入力します。最大 32 文字を入力することができます。

ステップ 8 [Apply] をクリックして、変更を確定します。新しいゲストユーザアカウントが、[Guest Users List] ページのゲストユーザリストに表示されます。

このページから、すべてのゲストユーザアカウント、それぞれの WLAN SSID およびライフタイムを表示できます。また、ゲストユーザアカウントを編集、または削除することができます。ゲストユーザアカウントを削除する場合、ゲスト WLAN を使用し、そのアカウントのユーザ名を使用してログインしているクライアントはすべて削除されます。

ステップ 9 新しいゲストユーザアカウントを作成するには、この手順を繰り返します。

ゲストユーザアカウントの表示

ゲストアカウントの表示 (GUI)

コントローラ GUI を使用してゲストユーザアカウントを表示するには、[Security]>[AAA]>[Local Net Users] を選択します。[Local Net Users] ページが表示されます。

このページから、すべてのローカル ネットユーザアカウント (ゲストユーザアカウントを含む) を表示し、必要に応じて編集または削除することができます。ゲストユーザアカウントを削除する場合、ゲスト WLAN を使用し、そのアカウントのユーザ名を使用してログインしているクライアントはすべて削除されます。

ゲストアカウントの表示 (CLI)

コントローラ CLI を使用して、すべてのローカル ネットユーザアカウント (ゲストユーザアカウントを含む) を表示するには、次のコマンドを入力します。

```
show netuser summary
```

管理者のユーザ名とパスワードの設定

管理者のユーザ名とパスワードの設定について

管理者のユーザ名とパスワードを設定しておくことで、権限のないユーザによるコントローラの設定変更や設定情報の表示を防ぐことができます。この項では、初期設定とパスワードリカバリの手順を説明します。

ユーザ名とパスワードの設定 (GUI)

ステップ 1 [Management] > [Local Management Users] を選択します。

ステップ 2 [New] をクリックします。

ステップ 3 ユーザ名およびパスワードを入力し、パスワードを確認します。
ユーザ名とパスワードは大文字と小文字が区別されます。いずれも、最大 24 文字の ASCII 文字列を使用できます。ユーザ名とパスワードにスペースを使用することはできません。

ステップ 4 [User Access Mode] として、次のいずれかを選択します。

- ReadOnly
- ReadWrite
- LobbyAdmin

ステップ 5 [Apply] をクリックします。

ユーザ名とパスワードの設定 (CLI)

ステップ 1 次のいずれかのコマンドを入力して、ユーザ名とパスワードを設定します。

- **config mgmtuser add username password read-write** : ユーザ名とパスワードのペアを作成して読み取りと書き込みの権限を付与します。
- **config mgmtuser add username password read-only** : ユーザ名とパスワードのペアを作成して読み取り専用権限を付与します。

ユーザ名とパスワードは大文字と小文字が区別されます。いずれも、最大 24 文字の ASCII 文字列を使用できます。ユーザ名とパスワードにスペースを使用することはできません。

(注) 既存のユーザ名のパスワードを変更する場合は、**config mgmtuser password username new_password** コマンドを入力します。

- ステップ 2 次のコマンドを入力して、設定されているユーザのリストを表示します。
show mgmtuser
-

パスワードの回復

はじめる前に

コンソール ポートを通じてコントローラ CLI にアクセスしていることを確認します。

- ステップ 1 コントローラのブート後に、「User」というプロンプトが表示されたら **Restore-Password** を入力します。
(注) セキュリティ上の理由により、入力したテキストはコントローラ コンソールには表示されません。
- ステップ 2 「Enter User Name」というプロンプトが表示されたら、新しいユーザ名を入力します。
- ステップ 3 「Enter Password」というプロンプトが表示されたら、新しいパスワードを入力します。
- ステップ 4 「Re-enter Password」というプロンプトが表示されたら、新しいパスワードを再入力します。入力した内容が検証されて、データベースに保存されます。
- ステップ 5 「User」というプロンプトが再び表示されたら、新しいユーザ名を入力します。
- ステップ 6 「Password」というプロンプトが表示されたら、新しいパスワードを入力します。新しいユーザ名とパスワードでコントローラにログインした状態になります。
-

SNMP v3 ユーザのデフォルト値の変更

SNMP v3 ユーザのデフォルト値の変更について

SNMP v3 ユーザのユーザ名、認証パスワード、およびプライバシー パスワードに対するコントローラのデフォルト値は、「default」が使用されています。これらの標準値を使用すると、セキュリティ上のリスクが発生します。したがって、これらの値を変更することを強く推奨します。



- (注) SNMP v3 は時間に依存しています。コントローラの時間および時間帯を正確に設定してください。
-

SNMP v3 ユーザのデフォルト値の変更 (GUI)

-
- ステップ 1** [Management] > [SNMP] > [SNMP V3 Users] の順に選択して [SNMP V3 Users] ページを開きます。
- ステップ 2** [User Name] カラムに「default」が表示されている場合は、そのユーザの青いドロップダウン矢印の上にカーソルを置き、[Remove] を選択してその SNMP v3 ユーザを削除します。
- ステップ 3** 新しい SNMP v3 ユーザを追加するには、[New] をクリックします。[SNMP V3 Users > New] ページが表示されます。
- ステップ 4** [User Profile Name] テキストボックスに、一意の名前を入力します。「default」は入力しないでください。
- ステップ 5** [Access Mode] ドロップダウンリストから [Read Only] または [Read/Write] を選択して、このユーザのアクセスレベルを指定します。デフォルト値は [Read Only] です。
- ステップ 6** [Authentication Protocol] ドロップダウンリストで、認証方式を [None]、[HMAC-MD5] (Hashed Message Authentication Coding-Message Digest 5)、および [HMAC-SHA] (Hashed Message Authentication Coding-Secure Hashing Algorithm) の中から選択します。デフォルト値は [HMAC-SHA] です。
- ステップ 7** [Auth Password] テキストボックスと [Confirm Auth Password] テキストボックスに、認証に使用する共有秘密キーを入力します。文字と数字の両方を含む少なくとも 12 文字を入力する必要があります。
- ステップ 8** [Privacy Protocol] ドロップダウンリストで、暗号化方式を [None]、[CBC-DES] (Cipher Block Chaining-Digital Encryption Standard)、および [CFB-AES-128] (Cipher Feedback Mode-Advanced Encryption Standard-128) の中から選択します。デフォルト値は [CFB-AES-128] です。
(注) CBC-DES 暗号化または CFB-AES-128 暗号化を設定するには、[ステップ 6](#) で認証プロトコルとして [HMAC-MD5] または [HMAC-SHA] を選択しておく必要があります。
- ステップ 9** [Priv Password] テキストボックスと [Confirm Priv Password] テキストボックスに、暗号化に使用する共有秘密キーを入力します。文字と数字の両方を含む少なくとも 12 文字を入力する必要があります。
- ステップ 10** [Apply] をクリックします。
- ステップ 11** [Save Configuration] をクリックします。
- ステップ 12** コントローラをリブートすると、追加した SNMP v3 ユーザが有効になります。
-

SNMP v3 ユーザのデフォルト値の変更 (CLI)

-
- ステップ 1** 次のコマンドを入力して、このコントローラに対する SNMP v3 ユーザの最新のリストを表示します。
show snmpv3user
- ステップ 2** [SNMP v3 User Name] カラムに「default」と表示されている場合は、次のコマンドを入力してこのユーザを削除します。
config snmp v3user delete username
username パラメータが SNMP v3 ユーザ名です (この場合は「default」)。

ステップ 3 次のコマンドを入力して、新しい SNMP v3 ユーザを作成します。

```
config snmp v3user create username {ro | rw} {none | hmacmd5 | hmacsha} {none | des | aescfb128} auth_key encrypt_key
```

値は次のとおりです。

- *username* は、SNMP v3 ユーザ名です。
- **ro** は読み取り専用モード、**rw** は読み書きモードです。
- **none**、**hmacmd5**、および **hmacsha** は、認証プロトコル オプションです。
- **none**、**des**、および **aescfb128** は、プライバシー プロトコル オプションです。
- *auth_key* は、認証用の共有秘密キーです。
- *encrypt_key* は、暗号化用の共有秘密キーです。

username、*auth_key*、および *encrypt_key* の各パラメータに「default」と入力しないでください。

ステップ 4 **save config** コマンドを入力します。

ステップ 5 追加した SNMP v3 ユーザを有効にするために、**reset system** コマンドを入力して、コントローラをリブートします。

証明書署名要求の生成

ステップ 1 OpenSSL のアプリケーションをインストールして開きます。

ステップ 2 次のコマンドを入力します。

```
OpenSSL> req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
```

コントローラは最大 2048 ビットのキー サイズをサポートします。

(注) 正しい共通名を指定する必要があります。証明書の作成に使用されるホスト名（共通名）が、コントローラの仮想インターフェイス IP に対するドメイン ネーム システム (DNS) のホスト名エントリに一致することを確認します。この名前は、DNS にも存在する必要があります。また、VIP インターフェイスへの変更後には、この変更を反映するためにシステムをリブートする必要があります。

コマンド投入後に、国、州、都市などの情報を入力するように促されます。

以下に類似した情報が表示されます。

```
OpenSSL> req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
writing new private key to 'mykey.pem'
-----
```

```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----

```

```

Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:Test@abc.com

```

```

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Test123
An optional company name []:
OpenSSL>

```

すべての必要な詳細を入力すると、2つのファイルが生成されます。

- 名前 *mykey.pem* を含む新しい秘密キー
- 名前 *myreq.pem* を含む CSR

ステップ 3 証明書署名要求 (CSR) の情報をコピーして CA の登録ツールに貼り付けます。サードパーティ CA に CSR を送信すると、サードパーティ CA は証明書にデジタル署名して、電子メールで署名付き証明書チェーンを返します。チェーン証明書の場合、CA から証明書のチェーン全体を受信します。上記の例のように中間証明書が 1 つのみであれば、CA から次の 3 種類の証明書を受信します。

- ルート証明書 (.pem)
- 中間証明書 (.pem)
- デバイス証明書 (.pem)

(注) 証明書が SHA1 暗号化との Apache 互換であることを確認します。

ステップ 4 3つすべての証明書を取得したら、次の順序で各 .pem ファイルの内容をコピーして別のファイルに貼り付けます。

```

-----BEGIN CERTIFICATE-----
*Device cert*
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
*Intermediate CA cert *
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
*Root CA cert *

```

```
-----END CERTIFICATE-----
```

ステップ 5 ファイルを *All-certs.pem* という名前で保存します。

ステップ 6 All-certs.pem 証明書を、CSR とともに生成した秘密キー（デバイス証明書の秘密キー、この例では mykey.pem）と組み合わせて、final.pem という名前でファイルを保存します。

ステップ 7 次のコマンドを入力して、All-certs.pem ファイルおよび final.pem ファイルを作成します。

```
openssl> pkcs12 -export -in All-certs.pem -inkey mykey.pem
          -out All-certs.p12 -clcerts -passin pass:check123
          -passout pass:check123
```

```
openssl> pkcs12 -in All-certs.p12 -out final-cert.pem
          -passin pass:check123 -passout pass:check123
```

final.pem ファイルをコントローラにダウンロードする必要があります。

(注) **-passin** および **-passout** パラメータのパスワードを入力する必要があります。 **-passout** パラメータに対して設定されたパスワードは、コントローラに設定されている certpassword パラメータに一致する必要があります。上記の例では、**-passin** と **-passout** の両方のパラメータに対して設定されるパスワードは check123 です。

次の作業

CLI または GUI を使用してコントローラに final.pem ファイルをダウンロードします。

サードパーティ証明書のダウンロード (GUI)

ステップ 1 デバイス証明書 final.pem を TFTP サーバのデフォルトディレクトリにコピーします。

ステップ 2 [Security] > [Web Auth] > [Certificate] を選択して、[Web Authentication Certificate] ページを開きます。

ステップ 3 [Download SSL Certificate] チェックボックスをオンにして、Download SSL Certificate From Server パラメータを表示します。

ステップ 4 [Server IP Address] テキストボックスに、TFTP サーバの IP アドレスを入力します。

ステップ 5 [File Path] テキストボックスに、証明書のディレクトリパスを入力します。

ステップ 6 [File Name] テキストボックスに、証明書の名前を入力します。

ステップ 7 [Certificate Password] テキストボックスに、証明書の保護に使用されたパスワードを入力します。

ステップ 8 [Apply] をクリックします。

ステップ 9 ダウンロードが完了したら、[Commands] > [Reboot] を選択して [Save and Reboot] をクリックします。

ステップ 10 変更を確定してコントローラをリブートするために [OK] をクリックします。

サードパーティ証明書のダウンロード (CLI)

ステップ 1 *final.pem* ファイルを TFTP サーバ上のデフォルトディレクトリに移動します。次のコマンドを入力して、ダウンロードの設定を変更します。

```
(Cisco Controller) > transfer download mode tftp
(Cisco Controller) > transfer download datatype webauthcert
(Cisco Controller) > transfer download serverip <TFTP server IP address>
(Cisco Controller) > transfer download path <absolute TFTP server path to the update file>
(Cisco Controller) > transfer download filename final.pem
```

ステップ 2 オペレーティングシステムが SSL キーと証明書を復号化できるように .pem ファイルのパスワードを入力します。

```
(Cisco Controller) > transfer download certpassword password
```

(注) *certpassword* の値が、CSR を生成する **-passout** パラメータと同じであることを確認します。

ステップ 3 次のコマンドを入力して、証明書およびキーのダウンロードを開始します。
transfer download start

例 :

```
(Cisco Controller) > transfer download start

Mode..... TFTP
Data Type..... Site Cert
TFTP Server IP..... 10.77.244.196
TFTP Packet Timeout..... 6
TFTP Max Retries..... 10
TFTP Path..... /
TFTP Filename..... final.pem

This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

ステップ 4 コントローラをリブートします。



第 24 章

Web 認証の管理

- Web 認証証明書の入手, 249 ページ
- Web 認証プロセス, 251 ページ
- デフォルトの Web 認証ログイン ページの選択, 254 ページ
- 外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの使用, 262 ページ
- カスタマイズされた Web 認証ログイン ページのダウンロード, 263 ページ
- WLAN ごとのログインページ、ログイン失敗ページ、およびログアウトページの割り当て, 267 ページ
- スリープ状態にあるクライアントの認証の設定, 270 ページ

Web 認証証明書の入手

Web 認証証明書について

コントローラのオペレーティングシステムが十分な機能を持つ Web 認証証明書を自動的に生成するため、何もすることなく、レイヤ 3 Web 認証で証明書を使用することができます。ただし、必要に応じて、新しい Web 認証証明書を生成するようにオペレーティングシステムに指示したり、外部で生成された SSL 証明書をダウンロードすることもできます。

チェーン証明書のサポート

Cisco WLC では、Web 認証用にデバイス証明書をチェーン証明書としてダウンロードできます（レベル 2 まで）。ワイルドカード証明書もサポートされます。チェーン証明書の詳細については、http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a0080a77592.shtmlで『Generate CSR for Third-Party Certificates and Download Chained Certificates to the WLC』を参照してください。

Web 認証証明書の入手（GUI）

-
- ステップ 1** [Security] > [Web Auth] > [Certificate] を選択して、[Web Authentication Certificate] ページを開きます。このページには、現在の Web 認証証明書の詳細が表示されます。
- ステップ 2** オペレーティング システムで生成された新しい Web 認証証明書を使用する手順は、次のとおりです。
- [Regenerate Certificate] をクリックします。オペレーティング システムが新しい Web 認証証明書を生成し、Web 認証証明書の生成が完了したことを示すメッセージが表示されます。
 - コントローラをリブートして、新しい証明書を登録します。
- ステップ 3** 外部で生成された Web 認証証明書を使用する手順は、次のとおりです。
- コントローラが TFTP サーバに ping を送ることができることを確認します。
 - [Download SSL Certificate] チェックボックスをオンにします。
 - [Server IP Address] テキスト ボックスに、TFTP サーバの IP アドレスを入力します。
[Maximum Retries] テキスト ボックスの 10 回の再試行および [Timeout] テキスト ボックスの 6 秒というデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。
 - 各ダウンロードを試行できる最大回数を [Maximum Retries] テキスト ボックスに入力し、各ダウンロードに許容される時間（秒単位）を [Timeout] テキスト ボックスに入力します。
 - [Certificate File Path] テキスト ボックスに、証明書のディレクトリパスを入力します。
 - [Certificate File Name] テキスト ボックスに、証明書の名前を入力します（**certname.pem**）。
 - [Certificate Password] テキスト ボックスに、証明書のパスワードを入力します。
 - [Apply] をクリックして、変更を確定します。オペレーティング システムが TFTP サーバから新しい証明書をダウンロードします。
 - コントローラをリブートして、新しい証明書を登録します。
-

Web 認証証明書の入手（CLI）

-
- ステップ 1** 次のコマンドを入力して、現在の Web 認証証明書を表示します。
- ```
show certificate summary
```

以下に類似した情報が表示されます。

```
Web Administration Certificate..... Locally Generated
Web Authentication Certificate..... Locally Generated
Certificate compatibility mode:..... off
```

- ステップ 2** オペレーティング システムで新しい Web 認証証明書を生成する手順は、次のとおりです。
- 新しい証明書を生成するには、次のコマンドを入力します。



**config certificate generate webauth**

- b) コントローラをリブートして、新しい証明書を登録するには、次のコマンドを入力します。
- ```
reset system
```

ステップ 3 外部で生成された Web 認証証明書を使用する手順は、次のとおりです。

(注) クライアントのブラウザが Web 認証 URL と Web 認証証明書のドメインを照合できるように、外部で生成された Web 認証証明書の Common Name (CN) は 1.1.1.1 (または相当する仮想インターフェイス IP アドレス) にすることを推奨します。

- 1 次のコマンドを入力して、ダウンロードする証明書の名前、パス、およびタイプを指定します。

```
transfer download mode tftp
```

```
transfer download datatype webauthcert
```

```
transfer download serverip server_ip_address
```

```
transfer download path server_path_to_file
```

```
transfer download filename certname.pem
```

```
transfer download certpassword password
```

```
transfer download tftpMaxRetries retries
```

```
transfer download tftpPktTimeout timeout
```

(注) 10回の再試行および6秒のタイムアウトというデフォルト値は、調整しなくても適切に機能します。ただし、これらの値は変更できます。そのためには、各ダウンロードを試行できる最大回数を *retries* パラメータに、各ダウンロードに許容される時間 (秒単位) を *timeout* パラメータに入力します。

- 2 次のコマンドを入力して、ダウンロードプロセスを開始します。

```
transfer download start
```

- 3 次のコマンドを入力して、コントローラをリブートして新しい証明書を登録します。

```
reset system
```

Web 認証プロセス

Web 認証は、レイヤ 3 セキュリティ機能です。これにより、コントローラは、クライアントが有効なユーザ名およびパスワードを正しく提供しない限り、そのクライアントに対する IP トラフィック (DHCP 関連パケットを除く) を許可しません。Web 認証を使用してクライアントを認証する場合、各クライアントのユーザ名とパスワードを定義する必要があります。クライアントは、ワイヤレス LAN に join する際に、ログイン ページの指示に従ってユーザ名とパスワードを入力する必要があります。



- (注) クライアントが使用する DNS 解決済みアドレスが 20 を超えると、コントローラは、Mobile Station Control Block (MSCB) テーブルの最初のアドレス空間で 21 番目のアドレスを上書きしますが、最初のアドレスはクライアントに保持されます。クライアントが最初のアドレスを再び使用しようとする、コントローラにはクライアントの MSCB テーブルの許可アドレスリストにこのアドレスがないため、使用できません。



- (注) ワンタイム パスワード (OTP) は、Web 認証ではサポートされていません。

Web 認証プロセスのセキュリティアラートの無効化

Web 認証が (レイヤ 3 セキュリティ下で) 有効になっている場合、ユーザが、最初にある URL にアクセスしようとした際に、Web ブラウザにセキュリティ警告が表示されることがあります。

図 19: 一般的な Web ブラウザセキュリティ警告ウィンドウ



- (注) VPN ユーザを許可するよう設定されている事前認証 ACL でクライアントが WebAuth SSID に接続すると、クライアントは数分ごとに SSID から切断されます。Webauth SSID の接続には、Web ページでの認証が必要です。

ユーザが [Yes] をクリックして続行した後（または、クライアントのブラウザにセキュリティ警告が表示されない場合）、Web 認証システムのログイン ページが表示されます。

- ステップ 1** [Security Alert] ページで [View Certificate] をクリックします。
- ステップ 2** [Install Certificate] をクリックします。
- ステップ 3** [Certificate Import Wizard] が表示されたら、[New] をクリックします。
- ステップ 4** [Place all certificates in the following store] を選択して、[Browse] をクリックします。
- ステップ 5** [Place all certificates in the following store] を選択して、[Browse] をクリックします。
- ステップ 6** [Trusted Root Certification Authorities] フォルダを展開して、[Local Computer] を選択します。
- ステップ 7** [OK] をクリックします。
- ステップ 8** [Next] > [Finish] の順にクリックします。
- ステップ 9** 「The import was successful」というメッセージが表示されたら、[OK] をクリックします。コントローラの自己署名証明書の issuer テキストボックスは空白であるため、Internet Explorer を開いて、[Tools] > [Internet Options] > [Advanced] の順に選択し、[Security] の下の [Warn about Invalid Site Certificates] チェックボックスをオフにして、[OK] をクリックします。
- ステップ 10** PC をリブートします。次回 Web 認証を試みる際には、ログイン ページが表示されます。

次の図は、デフォルトの Web 認証ログイン ページを示しています。

図 20: デフォルトの Web 認証ログイン ページ

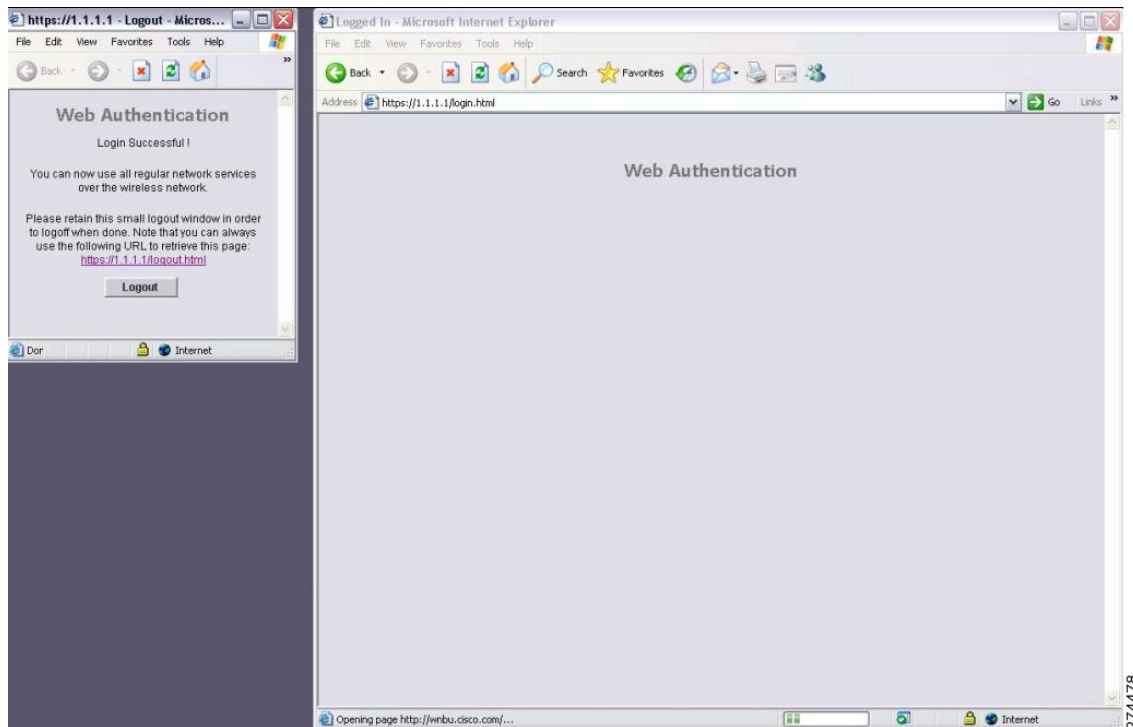
デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。Web 認証システムが次のいずれかを表示するように選択できます。

- デフォルトのログイン ページ
- デフォルトのログイン ページの変更バージョン
- 外部の Web サーバに設定する、カスタマイズされたログイン ページ
- コントローラにダウンロードする、カスタマイズされたログイン ページ

デフォルトの Web 認証ログイン ページのセクションを選択すると、Web 認証ログイン ページの表示方法を選択する手順が記載されています。

Web 認証ログイン ページで、ユーザが有効なユーザ名とパスワードを入力し、[Submit] をクリックすると、Web 認証システムは、ログインに成功したことを示すページを表示し、認証されたクライアントは要求した URL にリダイレクトされます。

図 21: ログイン成功ページ



デフォルトのログイン成功ページには、`https://<IP address>/logout.html` 形式で仮想ゲートウェイアドレスの URL へのポインタが表示されます。コントローラの仮想インターフェイスに設定した IP アドレスは、ログインページのリダイレクトアドレスとして機能します。

デフォルトの Web 認証ログインページの選択

デフォルトの Web 認証ログインページについて

内部コントローラの Web サーバによって処理されるカスタムの webauth bundle を使用する場合は、ページに 5 つを超える要素 (HTML、CSS、イメージなど) を含めることはできません。これは、内部コントローラの Web サーバが実装する DoS 保護メカニズムにより、各クライアントが開く同時 TCP 接続が負荷に応じて最大 5 つに制限されるためです。ブラウザが DoS 保護を処理する方法によっては、ページに多くの要素が含まれているためにページのロードが遅くなること

があり、一部のブラウザは、同時に 5 つを超える TCP セッションを開こうとする場合があります (Firefox 4 など)。

ユーザが SSLv2 専用に設定されているブラウザを使用して Web ページに接続するのを防止する場合は、**config network secureweb cipher-option sslv2 disable** コマンドを入力して、Web 認証に対して SSLv2 を無効にできます。このコマンドを使用すると、ユーザは、SSLv3 以降のリリースなどによりセキュアなプロトコルを使用するように設定したブラウザを使用しなければなりません。デフォルト値はディセーブルです。



(注) Cisco TAC はカスタム Web 認証バンドルを作成する責任を負いません。

複雑なカスタムの Web 認証モジュールが存在する場合は、コントローラ上の外部 Web 認証設定を使用して、完全なログインページが外部 Web サーバでホストされるようにすることを推奨します。

デフォルトの Web 認証ログインページの選択 (GUI)

- ステップ 1 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。
- ステップ 2 [Web Authentication Type] ドロップダウンリストから [Internal (Default)] を選択します。
- ステップ 3 デフォルトの Web 認証ログイン ページをそのまま使用する場合、[ステップ 8](#)に進みます。デフォルトのログイン ページを変更する場合は、[ステップ 4](#)に進みます。
- ステップ 4 デフォルト ページの右上に表示されている Cisco ロゴを非表示にするには、[Cisco Logo] の [Hide] オプションを選択します。表示する場合は、[Show] オプションをクリックします。
- ステップ 5 ログイン後にユーザを特定の URL (会社の URL など) にダイレクトさせる場合、[Redirect URL After Login] テキストボックスに必要な URL を入力します。最大 254 文字を入力することができます。
(注) コントローラでは、HTTP (HTTP over TCP) サーバへの Web 認証リダイレクトのみがサポートされています。HTTPS (HTTP over SSL) サーバへの Web 認証リダイレクトはサポートしていません。
- ステップ 6 ログインページで独自のヘッドラインを作成する場合、[Headline] テキストボックスに必要なテキストを入力します。最大 127 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco wireless network」です。
- ステップ 7 ログインページで独自のメッセージを作成する場合、[Message] テキストボックスに必要なテキストを入力します。最大 2047 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。
- ステップ 8 [Apply] をクリックして、変更を確定します。
- ステップ 9 [Preview] をクリックして、Web 認証ログイン ページを表示します。
- ステップ 10 ログインページの内容と外観に満足したら、[Save Configuration] をクリックして変更を保存します。納得いかない場合は、納得する結果を得られるように必要に応じて上記手順を繰り返します。

デフォルトの Web 認証ログインページの選択 (CLI)

ステップ 1 次のコマンドを入力して、デフォルトの Web 認証タイプを指定します。

```
config custom-web webauth_type internal
```

ステップ 2 デフォルトの Web 認証ログインページをそのまま使用する場合、ステップ 7 に進みます。デフォルトのログインページを変更する場合は、ステップ 3 に進みます。

ステップ 3 デフォルトのログインページの右上に表示されている Cisco ロゴの表示/非表示を切り替えるには、次のコマンドを入力します。

```
config custom-web weblogo {enable | disable}
```

ステップ 4 ユーザをログイン後に特定の URL (会社の URL など) に転送させる場合、次のコマンドを入力します。

```
config custom-web redirecturl url
```

URL には最大 130 文字を入力することができます。リダイレクト先をデフォルトの設定に戻すには、**clear redirecturl** コマンドを入力します。

(注) コントローラでは、HTTP (HTTP over TCP) サーバへの Web 認証リダイレクトのみがサポートされています。HTTPS (HTTP over SSL) サーバへの Web 認証リダイレクトはサポートしていません。

ステップ 5 ログインページで独自のヘッダラインを作成する場合、次のコマンドを入力します。

```
config custom-web webtitle title
```

最大 130 文字を入力することができます。デフォルトのヘッダラインは、「Welcome to the Cisco wireless network」です。ヘッダラインをデフォルトの設定に戻すには、**clear webtitle** コマンドを入力します。

ステップ 6 ログインページで独自のメッセージを作成する場合、次のコマンドを入力します。

```
config custom-web webmessage message
```

最大 130 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.」です。メッセージをデフォルトの設定に戻すには、**clear webmessage** コマンドを入力します。

ステップ 7 [web authentication logout] ポップアップ ウィンドウを有効または無効にするには、次のコマンドを入力します。

```
config custom-web logout-popup {enable | disable}
```

ステップ 8 **save config** コマンドを入力して、設定を保存します。

ステップ 9 次の手順で独自のロゴを Web 認証ログインページにインポートします。

1 Trivial File Transfer Protocol (TFTP) サーバがダウンロードのために使用可能であることを確認します。TFTP サーバをセットアップするときには、次のガイドラインに従ってください。

- サービス ポート経由でダウンロードする場合、サービス ポートはルーティングできないため、TFTP サーバはサービス ポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。

- ディストリビューション システム ネットワーク ポートを経由してダウンロードする場合、ディストリビューション システム ポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバを Cisco Prime Infrastructure と同じ PC 上で実行することはできません。Prime Infrastructure 内蔵 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。

- 2 次のコマンドを入力して、コントローラが TFTP サーバと通信可能であることを確認します。

ping ip-address

- 3 TFTP サーバのデフォルトディレクトリにロゴファイル (.jpg、.gif、または.png 形式) を移動します。ファイルサイズは 30 キロビット以内です。うまく収まるようにするには、ロゴは、横 180 ピクセル X 縦 360 ピクセル前後の大きさにします。

- 4 次のコマンドを入力して、ダウンロード モードを指定します。

transfer download mode tftp

- 5 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。

transfer download datatype image

- 6 次のコマンドを入力して、TFTP サーバの IP アドレスを指定します。

transfer download serverip tftp-server-ip-address

(注) TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ (/) を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。

- 7 次のコマンドを入力して、ダウンロード パスを指定します。

transfer download path absolute-tftp-server-path-to-file

- 8 次のコマンドを入力して、ダウンロードするファイルを指定します。

transfer download filename {filename.jpg | filename.gif | filename.png}

- 9 次のコマンドを入力して、更新した設定を表示し、プロンプトに y と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。

transfer download start

- 10 次のコマンドを入力して、設定を保存します。

save config

(注) Web 認証ログイン ページからロゴを削除するには、**clear webimage** コマンドを入力します。

ステップ 10 Web 認証ログイン ページの設定の確認 (CLI) , (266 ページ) の項の指示に従って、設定を確認します。

例：カスタマイズされた Web 認証ログインページの作成

この項では、カスタマイズされた Web 認証ログインページの作成について説明します。作成後は、外部 Web サーバからアクセスできるようになります。

Web 認証ログインページのテンプレートを次に示します。カスタマイズされたページを作成する際に、モデルとして使用できます。

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
  var link = document.location.href;
  var searchString = "redirect=";
  var equalIndex = link.indexOf(searchString);
  var redirectUrl = "";

  if (document.forms[0].action == "") {
    var url = window.location.href;
    var args = new Object();
    var query = location.search.substring(1);
    var pairs = query.split("&");
    for(var i=0;i<pairs.length;i++){
      var pos = pairs[i].indexOf('=');
      if(pos == -1) continue;
      var argname = pairs[i].substring(0,pos);
      var value = pairs[i].substring(pos+1);
      args[argname] = unescape(value);
    }
    document.forms[0].action = args.switch_url;
  }

  if(equalIndex >= 0) {
    equalIndex += searchString.length;
    redirectUrl = "";
    redirectUrl += link.substring(equalIndex);
  }
  if(redirectUrl.length > 255)
    redirectUrl = redirectUrl.substring(0,255);
  document.forms[0].redirect_url.value = redirectUrl;
  document.forms[0].buttonClicked.value = 4;
  document.forms[0].submit();
}

function loadAction(){
  var url = window.location.href;
  var args = new Object();
  var query = location.search.substring(1);
  var pairs = query.split("&");
  for(var i=0;i<pairs.length;i++){
    var pos = pairs[i].indexOf('=');
    if(pos == -1) continue;
    var argname = pairs[i].substring(0,pos);
    var value = pairs[i].substring(pos+1);
    args[argname] = unescape(value);
  }
}
//alert( "AP MAC Address is " + args.ap_mac);
//alert( "The Switch URL to post user credentials is " + args.switch_url);
document.forms[0].action = args.switch_url;

// This is the status code returned from webauth login action
// Any value of status code from 1 to 5 is error condition and user
// should be shown error as below or modify the message as it suits
// the customer
```


- **statusCode** : コントローラの Web 認証サーバから戻されるステータス コード。
- **wlan** : 無線ユーザがアソシエートされている WLAN SSID。

使用できるステータス コードは、次のとおりです。

- ステータス コード 1 : 「You are already logged in. No further action is required on your part.」
- ステータス コード 2 : 「You are not configured to authenticate against web portal. No further action is required on your part.」
- ステータス コード 3 : 「The username specified cannot be used at this time. Perhaps the username is already logged into the system?」
- ステータス コード 4 : 「You have been excluded.」
- ステータス コード 5 : 「The User Name and Password combination you have entered is invalid. Please try again.」

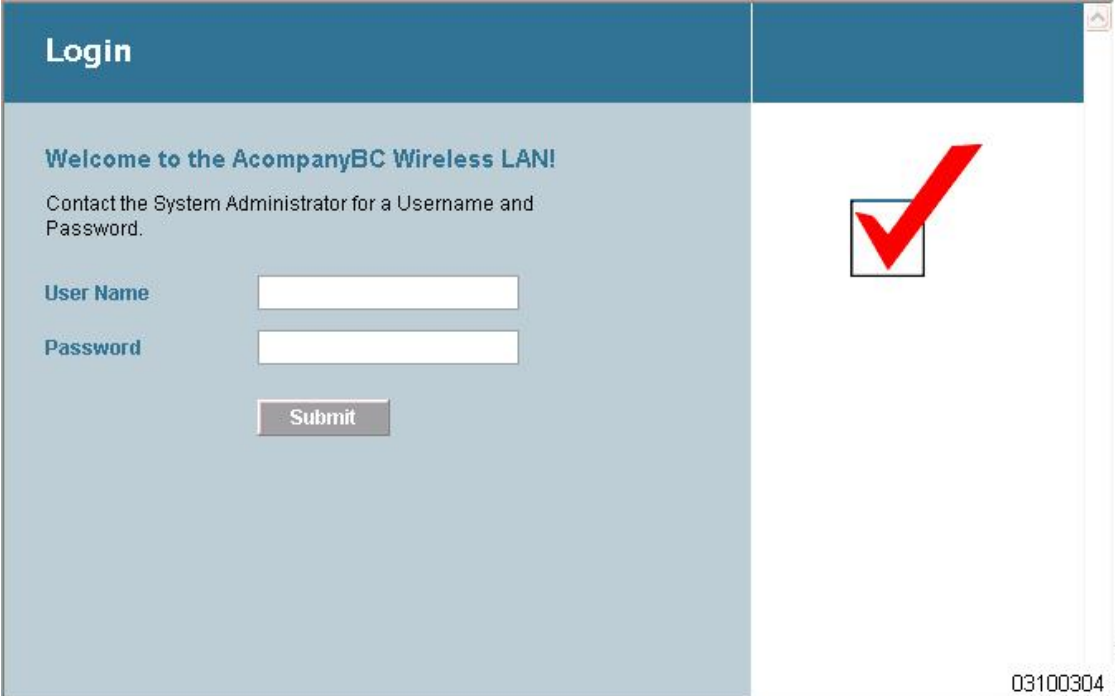


(注) 詳細については、次の URL にある『*External Web Authentication with Wireless LAN Controllers Configuration Example*』を参照してください。 http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml

例：変更されたデフォルトの Web 認証ログイン ページの例

次の図に、変更されたデフォルトの Web 認証ログイン ページの例を示します。

図 22：変更されたデフォルトの Web 認証ログイン ページの例



The screenshot shows a web browser window displaying a custom login page. The page has a blue header with the word "Login". Below the header, it says "Welcome to the AcompanyBC Wireless LAN!" and "Contact the System Administrator for a Username and Password." There are two input fields labeled "User Name" and "Password", and a "Submit" button. A large red checkmark is overlaid on the right side of the page. The page number "03100304" and a small vertical number "142262" are visible in the bottom right corner.

このログイン ページは、次の CLI コマンドを使用して作成されました。

- `config custom-web weblogo disable`
- `config custom-web webtitle Welcome to the AcompanyBC Wireless LAN!`
- `config custom-web webmessage Contact the System Administrator for a Username and Password.`
- `transfer download start`
- `config custom-web redirecturl url`

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの使用

カスタマイズされた Web 認証ログイン ページについて

Web 認証ログイン ページをカスタマイズして、外部 Web サーバにリダイレクトすることができます。この機能を有効にすると、ユーザは、外部 Web サーバ上のカスタマイズされたログイン ページへダイレクトされます。

外部 Web サーバに対して、WLAN 上で事前認証アクセスコントロールリスト (ACL) を設定し、[Security Policies > Web Policy on the WLANs > Edit] ページで、WLAN 事前認証 ACL としてこの ACL を選択する必要があります。

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 (GUI)

-
- ステップ 1 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。
- ステップ 2 [Web Authentication Type] ドロップダウン リストから [External (Redirect to external server)] を選択します。
- ステップ 3 [Redirect URL after login] テキスト ボックスに、ログイン後にユーザをリダイレクトさせる URL を入力します。
たとえば、会社の URL を入力すると、ユーザがログインした後にその URL へ転送されます。最大入力長は 254 文字です。デフォルトでは、ユーザは、ログイン ページが機能する前にユーザのブラウザに入力された URL にリダイレクトされます。Web サーバ上でカスタマイズされた Web 認証ログイン ページの URL を入力します。最大 252 文字を入力することができます。
- ステップ 4 [External Webauth URL] テキスト ボックスに、外部 Web 認証に使用する URL を入力します。
- ステップ 5 [Apply] をクリックします。
- ステップ 6 [Save Configuration] をクリックします。
-

外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択 (CLI)

-
- ステップ 1 次のコマンドを入力して、Web 認証タイプを指定します。
config custom-web webauth_type external
- ステップ 2 次のコマンドを入力して、Web サーバ上でカスタマイズされた Web 認証ログイン ページの URL を指定します。
config custom-web ext-webauth-url url

URL には最大 252 文字を入力することができます。

ステップ 3 次のコマンドを入力して、Web サーバの IP アドレスを指定します。
config custom-web ext-webserver {add | delete} server_IP_address

ステップ 4 **save config** コマンドを入力して、設定を保存します。

ステップ 5 [Web 認証ログインページの設定の確認 \(CLI\)](#) , (266 ページ) の項の指示に従って、設定を確認します。

カスタマイズされた Web 認証ログインページのダウンロード

Web 認証ログインページに使用するページやイメージファイルを .tar ファイルに圧縮してコントローラへダウンロードできます。これらのファイルは、**webauth bundle** と呼ばれています。ファイルの最大許容サイズは、非圧縮の状態です。1 MB です。 .tar ファイルがローカル TFTP サーバからダウンロードされる際、コントローラのファイルシステムに、展開済みファイルとして取り込まれます。

ログインページ例を Cisco Prime インフラストラクチャからダウンロードし、カスタマイズされたログイン・ページの開始点として利用できます。詳細については、Cisco Prime インフラストラクチャのドキュメントを参照してください。



(注) **webauth bundle** を GNU に準拠していない .tar 圧縮アプリケーションでロードすると、コントローラはこの bundle のファイルを解凍できず、「Extracting error」および「TFTP transfer failed」というエラーメッセージが表示されます。このため、PicoZip など GNU 標準に準拠するアプリケーションを使用して、**webauth bundle** の .tar ファイルを圧縮することを推奨します。



(注) 設定のバックアップには、**webauth bundle** や外部ライセンスなど、ダウンロードしてコントローラに格納した付加的なファイルやコンポーネントは含まれないため、このようなファイルやコンポーネントの外部バックアップ コピーは手動で保存する必要があります。



(注) カスタマイズされた **webauth bundle** に異なる要素が 4 つ以上含まれる場合は、コントローラ上の TCP レート制限ポリシーが原因で発生するページの読み込み上の問題を防ぐために、外部サーバを使用してください。

カスタマイズされた Web 認証ログイン ページのダウンロードの前提条件

- ログイン ページの名前を login.html とします。 コントローラは、この名前に基づいて Web 認証 URL を作成します。 webauth bundle の展開後にこのファイルが見つからない場合、bundle は破棄され、エラー メッセージが表示されます。
- ユーザ名とパスワードの両方に入力テキスト ボックスを提供する。
- リダイレクト先の URL を元の URL から抽出後、非表示入力アイテムとして保持する。
- 元の URL からアクション URL を抽出して、ページに設定する。
- リターン ステータス コードをデコードするスクリプトを提供する。
- メインページで使用されているすべてのパス（たとえば、イメージを参照するパス）を確認する。
- バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

カスタマイズされた Web 認証ログイン ページのダウンロード (GUI)

ステップ 1 ログイン ページが含まれる .tar ファイルをサーバのデフォルトディレクトリに移動します。

ステップ 2 [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

ステップ 3 [File Type] ドロップダウン リストから、[Webauth Bundle] を選択します。

ステップ 4 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- TFTP
- FTP
- SFTP (7.4 以降のリリースで利用可能)

ステップ 5 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。

ステップ 6 TFTP サーバを使用している場合は、コントローラによる .tar ファイルのダウンロードの最大試行回数を [Maximum Retries] テキスト ボックスに入力します。

指定できる範囲は 1 ~ 254 です。

デフォルトは 10 です。

ステップ 7 TFTP サーバを使用している場合は、コントローラによる *.tar ファイルのダウンロード試行がタイムアウトするまでの時間 (秒数) を [Timeout] テキスト ボックスに入力します。

指定できる範囲は 1 ~ 254 秒です。

デフォルトは 6 秒です。

- ステップ 8 [File Path] テキスト ボックスに、ダウンロードする .tar ファイルのパスを入力します。デフォルト値は「/」です。
- ステップ 9 [File Name] テキスト ボックスに、ダウンロードする .tar ファイルの名前を入力します。
- ステップ 10 FTP サーバを使用している場合は、次の手順に従います。
- 1 [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - 2 [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - 3 [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。
- ステップ 11 [Download] をクリックして、.tar ファイルをコントローラへダウンロードします。
- ステップ 12 [Security] > [Web Auth] > [Web Login Page] の順に選択して、[Web Login] ページを開きます。
- ステップ 13 [Web Authentication Type] ドロップダウン リストから [Customized (Downloaded)] を選択します。
- ステップ 14 [Apply] をクリックします。
- ステップ 15 [Preview] をクリックして、カスタマイズされた Web 認証ログインページを表示します。
- ステップ 16 ログイン ページの内容と外観に満足したら、[Save Configuration] をクリックします。

カスタマイズされた Web 認証ログインページのダウンロード (CLI)

- ステップ 1 ログイン ページが含まれる .tar ファイルをサーバのデフォルトディレクトリに移動します。
- ステップ 2 次のコマンドを入力して、ダウンロード モードを指定します。
transfer download mode {tftp | ftp | sftp}
- ステップ 3 次のコマンドを入力して、ダウンロードするファイルのタイプを指定します。
transfer download datatype webauthbundle
- ステップ 4 次のコマンドを入力して、TFTP サーバの IP アドレスを指定します。
transfer download serverip *tftp-server-ip-address*
- (注) TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ (/) を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。
- ステップ 5 次のコマンドを入力して、ダウンロードパスを指定します。
transfer download path *absolute-tftp-server-path-to-file*
- ステップ 6 次のコマンドを入力して、ダウンロードするファイルを指定します。
transfer download filename *filename.tar*

ステップ 7 次のコマンドを入力して、更新した設定を表示し、プロンプトに **y** と応答して現在のダウンロード設定を確認し、ダウンロードを開始します。

transfer download start

ステップ 8 次のコマンドを入力して、Web 認証タイプを指定します。

config custom-web webauth_type customized

ステップ 9 **save config** コマンドを入力して、設定を保存します。

例：カスタマイズされた Web 認証ログイン ページ

次の図に、カスタマイズされた Web 認証ログイン ページの例を示します。

図 23: カスタマイズされた Web 認証ログイン ページの例

Web 認証ログイン ページの設定の確認 (CLI)

次のコマンドを入力して、Web 認証ログイン ページに対する変更内容を確認します。

show custom-web

WLAN ごとのログインページ、ログイン失敗ページ、およびログアウトページの割り当て

WLAN ごとのログインページ、ログイン失敗ページ、およびログアウトページの割り当てについて

ユーザに対して、WLAN ごとに異なる Web 認証ログインページ、ログイン失敗ページ、ログアウトページを表示できます。この機能を使用すると、ゲストユーザや組織内のさまざまな部署の従業員など、さまざまなネットワークユーザに対し、ユーザ固有の Web 認証ページを表示できます。

すべての Web 認証タイプ ([Internal]、[External]、[Customized]) で異なるログインページを使用できます。ただし、Web 認証タイプで [Customized] を選んだ場合に限り、異なるログイン失敗ページとログアウトページを指定できます。

WLAN ごとのログインページ、ログイン失敗ページ、およびログアウトページの割り当て (GUI)

-
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** Web ログインページ、ログイン失敗ページ、またはログアウトページを割り当てる WLAN の ID 番号をクリックします。
- ステップ 3** [Security] > [Layer 3] の順に選択します。
- ステップ 4** [Web Policy] と [Authentication] が選択されていることを確認します。
- ステップ 5** グローバル認証設定 Web 認証ページを無効にするには、[Override Global Config] チェックボックスをオンにします。
- ステップ 6** [Web Auth Type] ドロップダウンリストが表示されたら、次のオプションのいずれかを選択して、無線ゲストユーザ用の Web 認証ページを定義します。
- [Internal] : コントローラのデフォルト Web ログインページを表示します。これは、デフォルト値です。
 - [Customized] : カスタム Web ログインページ、ログイン失敗ページ、ログアウトページを表示します。このオプションを選択すると、ログインページ、ログイン失敗ページ、ログアウトページに対して 3 つの個別のドロップダウンリストが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウンリストで [None] を選択します。
- (注) これらオプションのログインページ、ログイン失敗ページ、ログアウトページは、webauth.tar ファイルとしてコントローラにダウンロードされます。

- [External] : 認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

[WLANs > Edit] ([Security] > [AAA Servers]) ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 7 ステップ 6 で Web 認証タイプとして [External] を選択した場合は、[AAA Servers] を選択して、ドロップダウン リストから最大 3 つの RADIUS サーバおよび LDAP サーバを選択します。

(注) RADIUS および LDAP の外部サーバは、[WLANs > Edit] ([Security] > [AAA Servers]) ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 8 次の手順で、Web 認証で接続するサーバの優先順位を指定します。

(注) デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

- 1 [Up] ボタンと [Down] ボタンの隣にあるボックスで、最初に接続するサーバの種類 ([Local]、[Radius]、[LDAP]) を強調表示します。
- 2 希望のサーバタイプがボックスの先頭になるまで、[Up] および [Down] をクリックします。
- 3 [<] 矢印をクリックして、そのサーバタイプを左側の優先順位ボックスに移動します。
- 4 この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

WLAN ごとのログインページ、ログイン失敗ページ、およびログアウト ページの割り当て (CLI)

ステップ 1 次のコマンドを入力して、Web ログイン ページ、ログイン失敗ページ、ログアウト ページを割り当てる WLAN の ID 番号を決定します。

```
show wlan summary
```

ステップ 2 カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに無線ゲストユーザをログインさせる場合は、次のコマンドを入力して Web 認証ページのファイル名および表示する WLAN を指定します。

- **config wlan custom-web login-page page_name wlan_id** : 指定した WLAN に対するカスタマイズしたログインページを定義します。
- **config wlan custom-web loginfailure-page page_name wlan_id** : 指定した WLAN に対するカスタマイズしたログイン失敗ページを定義します。

(注) コントローラのデフォルトのログイン失敗ページを使用するには、**config wlan custom-web loginfailure-page none wlan_id** コマンドを入力します。

- **config wlan custom-web logout-page page_name wlan_id** : 指定した WLAN に対するカスタマイズしたログアウト ページを定義します。

(注) コントローラのデフォルトのログアウト ページを使用するには、**config wlan custom-web logout-page none wlan_id** コマンドを入力します。

ステップ 3 次のコマンドを入力して外部サーバの URL を指定することにより、Web ログイン ページにアクセスする前に無線ゲスト ユーザを外部サーバにリダイレクトします。

config wlan custom-web ext-webauth-url ext_web_url wlan_id

ステップ 4 次のコマンドを入力して、Web 認証サーバの接続順序を定義します。

config wlan security web-auth server-precedence wlan_id {local | ldap | radius} {local | ldap | radius} {local | ldap | radius}

サーバの Web 認証は、デフォルトではローカル、RADIUS、LDAP の順になっています。

(注) すべての外部サーバをコントローラで事前に設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらを設定できます。

ステップ 5 次のコマンドを入力して、無線ゲスト ユーザ用の Web 認証ページを定義します。

config wlan custom-web webauth-type {internal | customized | external} wlan_id

値は次のとおりです。

- **internal** は、コントローラのデフォルト Web ログイン ページを表示します。これは、デフォルト値です。

- **customized** は、ステップ 2 で設定したカスタム Web ログイン ページを表示します。

(注) ログイン失敗ページとログアウト ページは常にカスタマイズされているため、ステップ 5 で Web 認証タイプを定義する必要はありません。

- **external** は、ステップ 3 で設定した URL にユーザをリダイレクトします。

ステップ 6 次のコマンドを入力して、グローバルカスタム Web 設定ではなく、WLAN 固有のカスタム Web 設定を使用します。

config wlan custom-web global disable wlan_id

(注) **config wlan custom-web global enable wlan_id** コマンドを入力すると、カスタム Web 認証がグローバル レベルで使用されます。

ステップ 7 次のコマンドを入力して、変更を保存します。

save config

スリープ状態にあるクライアントの認証の設定

スリープ状態にあるクライアントの認証について

Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間 (30 日) で、デフォルトは 12 時間です。WLAN にマッピングされるユーザグループポリシーと WLAN に、期間を設定できます。スリープタイマーは、アイドルタイムアウト後に有効になります。クライアントタイムアウトが WLAN のスリープタイマーに設定された時間より短い場合、クライアントのライフタイムがスリープ時間として使用されます。



(注) スリープタイマーは 6 分ごとに期限切れになります。

この機能は FlexConnect のローカルスイッチング、中央認証のシナリオでサポートされています。



注意

スリープモードに切り替わったクライアント MAC アドレスがスプーフィングされた場合、ラップトップなどの偽のデバイスを認証することができます。

次に、モビリティシナリオでの注意事項を示します。

- 同じサブネットの L2 ローミングがサポートされています。
- アンカー スリープタイマーを適用できます。
- スリープ状態にあるクライアントの情報は、クライアントがアンカー間を移動する場合に、複数の自動アンカー間で共有されます。

サポートされるモビリティシナリオ

スリープ状態にあるクライアントは、次のシナリオでは再認証が必要ありません。

- モビリティグループに 2 台のコントローラがあるとしします。1 台のコントローラに関連付けられているクライアントがスリープ状態になり、その後復帰して他方のコントローラに関連付けられます。
- モビリティグループに 3 台のコントローラがあるとしします。1 台目のコントローラにアンカーされた 2 台目のコントローラに関連付けられたクライアントは、スリープ状態から復帰して、3 台目のコントローラに関連付けられます。
- クライアントはスリープ状態から復帰して、エクスポートアンカーにアンカーされた同じまたは別のエクスポート外部コントローラに関連付けられます。

スリープ状態にあるクライアントの制限

- スリープ状態にあるクライアントは WLAN ごとにのみ設定できます。
- スリープ状態にあるクライアントの認証機能は、レイヤ2セキュリティおよびWeb認証が有効な場合はサポートされません。
- スリープ状態にあるクライアントの認証機能は、レイヤ3セキュリティが有効な WLAN でのみサポートされています。
- スリープ状態にあるクライアントの中央 Web 認証はサポートされていません。
- スリープ状態にあるクライアントの認証機能は、ゲスト LAN およびリモート LAN ではサポートされていません。
- ローカル ユーザ ポリシーを持つスリープ状態のゲスト アクセス クライアントはサポートされません。この場合、WLAN 固有のタイマーが適用されます。
- ハイ アベイラビリティのシナリオでは、クライアント エントリがアクティブとスタンバイの間で同期されますが、スリープ タイマーは同期されません。アクティブ コントローラに障害が発生した場合、クライアントはスタンバイ コントローラにアソシエートするときに再認証される必要があります。
- サポートされるスリープ状態にあるクライアントの数は、コントローラプラットフォームによって異なります。
 - Cisco 2500 シリーズ ワイヤレス LAN コントローラ : 500
 - Cisco 5500 シリーズ ワイヤレス LAN コントローラ : 1000
 - Cisco Flex 7500 シリーズ ワイヤレス LAN コントローラ : 9000
 - Cisco 8500 シリーズ ワイヤレス LAN コントローラ : 9000
 - Cisco WiSM2 : 1000
 - Cisco 仮想ワイヤレス LAN コントローラ : 500
 - Cisco Services Ready Engine (SRE) の Cisco ワイヤレス コントローラ : 500
- 新しいモビリティはサポートされていません。

スリープ状態のクライアントの認証の設定 (GUI)

-
- ステップ 1** [WLANs] を選択します。
- ステップ 2** 対応する WLAN ID をクリックします。

[WLANs > Edit] ページが表示されます。

- ステップ 3** [Security] タブをクリックして、[Layer 3]タブをクリックします。
- ステップ 4** スリープ状態のクライアントに対する認証を有効にするには、[Sleeping Client] チェックボックスをオンにします。
- ステップ 5** 再認証が必要になる前にスリープ状態にあるクライアントを記録する期間を [Sleeping Client Timeout] に入力します。
デフォルトのタイムアウトは 12 時間です。
- ステップ 6** [Apply] をクリックします。
- ステップ 7** [Save Configuration] をクリックします。
-

スリープ状態のクライアントの認証の設定 (CLI)

- 次のコマンドを入力して、WLANのスリープ状態のクライアントの認証を有効または無効にします。
config wlan custom-web sleep-client {enable | disable} wlan-id
- 次のコマンドを入力して、WLANにスリープ状態のクライアントのタイムアウトを設定します。
config wlan custom-web sleep-client timeout wlan-id duration
- 次のコマンドを入力して、WLANのスリープ状態のクライアントの設定を表示します。
show wlan wlan-id
- 次のコマンドを入力して、不要なスリープ状態のクライアントのエントリを削除します。
config custom-web sleep-client delete client-mac-addr
- 次のコマンドを入力して、すべてのスリープ状態にあるクライアントのエントリの要約を表示します。
show custom-web sleep-client summary
- 次のコマンドを入力して、クライアント MAC アドレスに基づいてスリープ状態にあるクライアントのエントリの詳細を表示します。
show custom-web sleep-client detail client-mac-addr



第 25 章

有線ゲスト アクセスの設定

- [有線ゲスト アクセスについて, 273 ページ](#)
- [有線ゲストのアクセスを設定するための前提条件, 274 ページ](#)
- [有線ゲストのアクセスの設定に関する制限, 274 ページ](#)
- [有線ゲスト アクセスの設定 \(GUI\) , 275 ページ](#)
- [有線ゲスト アクセスの設定 \(CLI\) , 277 ページ](#)
- [IPv6 クライアントのゲストアクセスのサポート, 279 ページ](#)

有線ゲスト アクセスについて

有線ゲスト アクセスにより、ゲスト ユーザはゲスト アクセス用に指定および設定されている有線イーサネット接続からゲスト アクセス ネットワークに接続できます。有線ゲスト アクセス ポートは、ゲスト オフィスからまたは会議室の特定のポートを介して利用することもできます。無線ゲスト ユーザアカウントのように、有線ゲスト アクセス ポートが Lobby Ambassador 機能を使用するネットワークに追加されます。

有線ゲスト アクセスは、スタンドアロン設定または、アンカーコントローラと外部コントローラの両方を使用するデュアル コントローラ設定で設定できます。この後者の設定は、有線ゲスト アクセストラフィックをさらに隔離するために使用されますが、有線ゲスト アクセスの展開には必須ではありません。

有線ゲスト アクセス ポートは最初、レイヤ 2 アクセス スイッチ上で、または有線ゲスト アクセストラフィック用の VLAN インターフェイスで設定されているスイッチポート上で終端します。有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへとランクされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。



(注) 2つのコントローラが展開される時、有線ゲストアクセスはアンカーと外部アンカーによって管理されますが、有線ゲストアクセスクライアントではモビリティがサポートされていません。この場合、DHCP およびクライアントの Web 認証は、アンカー コントローラによって処理されます。



(注) QoS ロールと帯域幅コントラクトを設定することにより、ネットワーク内の有線ゲスト ユーザに割り当てられている帯域幅の量を指定できます。

基本的なピアツーピア WLAN ACL を作成して有線ゲスト WLAN に適用できます。これはピアツーピア トラフィックをブロックしないので、ゲスト ユーザは互いに通信できます。

有線ゲストのアクセスを設定するための前提条件

無線ネットワーク上で有線ゲスト アクセスを設定するには、次の手順を実行する必要があります。

- 1 有線ゲスト ユーザ アクセス用の動的インターフェイス (VLAN) を設定します。
- 2 ゲスト ユーザ アクセス用の有線 LAN を作成します。
- 3 コントローラを設定します。
- 4 アンカー コントローラを設定します (別のコントローラでトラフィックを終端する場合)。
- 5 ゲスト LAN 用のセキュリティを設定します。
- 6 設定を確認します。

有線ゲストのアクセスの設定に関する制限

- 有線ゲスト アクセス インターフェイスは、タグ付きである必要があります。
- 有線ゲスト アクセス ポートは、外部コントローラと同じレイヤ 2 ネットワークになければなりません。
- コントローラ上で、最大 5 つの有線ゲスト アクセス LAN を設定できます。また、有線ゲスト アクセス LAN では、複数のアンカーがサポートされます。
- 有線ゲスト アクセス クライアントに対して、レイヤ 3 Web 認証と Web パススルーがサポートされています。レイヤ 2 セキュリティはサポートされていません。
- 予期しない結果が生じる場合があるため、有線ゲスト VLAN を複数の外部コントローラにトランクしないでください。

有線ゲストアクセスの設定 (GUI)

- ステップ 1 有線ゲストユーザアクセス用の動的インターフェイスを作成するために、[Controller]>[Interfaces]の順に選択します。[Interfaces]ページが表示されます。
- ステップ 2 [New]をクリックして、[Interfaces>New]ページを開きます。
- ステップ 3 新しいインターフェイスの名前と VLAN ID を入力します。
- ステップ 4 [Apply]をクリックして、変更を確定します。
- ステップ 5 [Port Number] テキストボックスに、有効なポート番号を入力します。0～25（両端の値を含む）の数値を入力できます。
- ステップ 6 [Guest LAN] チェックボックスをオンにします。
- ステップ 7 [Apply]をクリックして、変更を確定します。
- ステップ 8 ゲストユーザアクセス用に有線 LAN を作成するために、[WLANs]を選択します。
- ステップ 9 [WLANs]ページで、ドロップダウンリストから[Create New]を選択して、[Go]をクリックします。[WLANs>New]ページが表示されます。
- ステップ 10 [Type] ドロップダウンリストから、[Guest LAN]を選択します。
- ステップ 11 [Profile Name] テキストボックスに、ゲスト LAN を識別する名前を入力します。スペースを使用しないでください。
- ステップ 12 [WLAN ID] ドロップダウンリストから、このゲスト LAN の ID 番号を選択します。
(注) 最大5つのゲスト LAN を作成できるので、[WLAN ID] オプションは1～5（両端の値を含む）です。
- ステップ 13 [Apply]をクリックして、変更を確定します。
- ステップ 14 [Status] パラメータの [Enabled] チェックボックスをオンにします。
- ステップ 15 Web 認証 ([Web-Auth]) は、デフォルトのセキュリティポリシーです。Web パススルーに変更する場合は、ステップ 16 とステップ 17 を完了してから [Security] タブを選択します。
- ステップ 16 [Ingress Interface] ドロップダウンリストから、ステップ 3 で作成した VLAN を選択します。この VLAN は、レイヤ 2 アクセススイッチを経由して、有線ゲストクライアントとコントローラとの間のパスを提供します。
- ステップ 17 [Egress Interface] ドロップダウンリストから、インターフェイスの名前を選択します。この WLAN は、有線ゲストクライアントトラフィックのコントローラから送信されるパスを提供します。
- ステップ 18 認証方式を変更する（たとえば、Web 認証から Web パススルーへ）場合、[Security]>[Layer 3]の順に選択します。[WLANs>Edit] ([Security]>[Layer 3]) ページが表示されます。
- ステップ 19 [Layer 3 Security] ドロップダウンリストから、次のいずれかを選択します。
 - [None] : レイヤ 3 セキュリティが無効になっています。
 - [Web Authentication] : 無線ネットワークに接続する際に、ユーザにユーザ名とパスワードの入力を求めます。これは、デフォルト値です。

- [Web Passthrough] : ユーザがユーザ名とパスワードを入力せずに、ネットワークにアクセスすることを許可します。

(注) ゲスト有線 VLAN にはレイヤ 3 ゲートウェイが存在しないようにしてください。コントローラによる Web 認証がバイパスされるためです。

ステップ 20 [Web Passthrough] オプションを選択する場合、[Email Input] チェックボックスが表示されます。ユーザがネットワークに接続しようとしたとき、電子メールアドレスの入力を求める場合は、このチェックボックスをオンにします。

ステップ 21 [Web Login Page] に設定されているグローバル認証設定を無効にするには、[Override Global Config] チェックボックスをオンにします。

ステップ 22 [Web Auth Type] ドロップダウンリストが表示されたら、次のオプションのいずれかを選択して、有線ゲストユーザ用の Web 認証ページを定義します。

- [Internal] : コントローラのデフォルト Web ログイン ページを表示します。これは、デフォルト値です。

- [Customized] : カスタム Web ログイン ページ、ログイン失敗ページ、ログアウト ページを表示します。このオプションを選択すると、ログイン ページ、ログイン失敗ページ、ログアウト ページに対して 3 つの個別のドロップダウンリストが表示されます。3 つのオプションすべてに対してカスタマイズしたページを定義する必要はありません。カスタマイズしたページを表示しないオプションに対しては、該当するドロップダウン リストで [None] を選択します。

(注) これらオプションのログイン ページ、ログイン失敗ページ、ログアウト ページは、webauth.tar ファイルとしてコントローラにダウンロードされます。

- [External] : 認証のためにユーザを外部サーバにリダイレクトします。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

[WLANs > Edit] ([Security] > [AAA Servers]) ページで、外部認証を行う特定の RADIUS サーバまたは LDAP サーバを選択できます。また、サーバによる認証の優先順位を定義することもできます。

ステップ 23 ステップ 22 で Web 認証タイプとして [External] を選択した場合は、[AAA Servers] を選択して、ドロップダウン リストから最大 3 つの RADIUS サーバおよび LDAP サーバを選択します。

(注) RADIUS および LDAP の外部サーバは、[WLANs > Edit] ([Security] > [AAA Servers]) ページでオプションを選択できるようにするため、あらかじめ設定しておく必要があります。[RADIUS Authentication Servers] ページと [LDAP Servers] ページでこれらのサーバを設定できます。

ステップ 24 次の手順で、Web 認証で接続するサーバの優先順位を指定します。

(注) デフォルトでは、[Local]、[RADIUS]、[LDAP] の順になっています。

- 1 [Up] ボタンと [Down] ボタンの隣にあるボックスで、最初に接続するサーバの種類 ([Local]、[Radius]、[LDAP]) を強調表示します。
- 2 希望のサーバタイプがボックスの先頭になるまで、[Up] および [Down] をクリックします。
- 3 [←] 矢印をクリックして、そのサーバタイプを左側の優先順位ボックスに移動します。
- 4 この手順を繰り返して他のサーバにも優先順位を割り当てます。

ステップ 25 [Apply] をクリックします。

ステップ 26 [Save Configuration] をクリックします。

ステップ 27 2 番目の (アンカー) コントローラがネットワークで使用中の場合は、このプロセスを繰り返します。

有線ゲストアクセスの設定 (CLI)

ステップ 1 次のコマンドを入力して、有線ゲストユーザのアクセス用の動的インターフェイス (VLAN) を作成します。

```
config interface create interface_name vlan_id
```

ステップ 2 リンク集約トランクが設定されていない場合、次のコマンドを入力して、物理ポートをインターフェイスにマッピングします。

```
config interface port interface_name primary_port {secondary_port}
```

ステップ 3 次のコマンドを入力して、ゲスト LAN VLAN を有効または無効にします。

```
config interface guest-lan interface_name {enable | disable}
```

この VLAN は、ステップ 5 で作成した入力インターフェイスに後でアソシエートされます。

ステップ 4 有線クライアントトラフィック用の有線 LAN を作成して、インターフェイスにアソシエートさせるには、次のコマンドを入力します。

```
config guest-lan create guest_lan_id interface_name
```

ゲスト LAN ID は、1 ~ 5 (両端の値を含む) にする必要があります。

(注) 有線ゲスト LAN を削除するには、**config guest-lan delete guest_lan_id** コマンドを入力します。

ステップ 5 レイヤ 2 アクセススイッチ経由で、有線ゲストクライアントとコントローラ間のパスを提供する有線ゲスト VLAN の入力インターフェイスを設定するには、次のコマンドを入力します。

```
config guest-lan ingress-interface guest_lan_id interface_name
```

ステップ 6 コントローラから有線ゲストトラフィックを送信するように出力インターフェイスを設定するには、次のコマンドを入力します。

```
config guest-lan interface guest_lan_id interface_name
```

(注) 有線ゲストトラフィックが別のコントローラで終端する場合は、終点の (アンカー) コントローラに対してステップ 4 とステップ 6 を繰り返し、起点の (外部) コントローラに対してステップ 1 からステップ 5 を繰り返します。また、両方のコントローラに対して次のコマンドを設定します。**config mobility group anchor add {guest-lan guest_lan_id | wlan wlan_id} IP_address**

ステップ 7 有線ゲスト LAN のセキュリティポリシーを設定するには、次のコマンドを入力します。

```
config guest-lan security {web-auth enable guest_lan_id | web-passthrough enable guest_lan_id}
```

(注) Web 認証はデフォルト設定です。

ステップ 8 有線ゲスト LAN を有効または無効にするには、次のコマンドを入力します。

```
config guest-lan {enable | disable} guest_lan_id
```

ステップ 9 カスタマイズされた Web ログイン ページ、ログイン失敗ページ、ログアウト ページに有線ゲスト ユーザをログインさせる場合は、次のコマンドを入力して、Web 認証ページのファイル名および表示するゲスト LAN を指定します。

- **config guest-lan custom-web login-page page_name guest_lan_id** : Web ログイン ページを定義します。
- **config guest-lan custom-web loginfailure-page page_name guest_lan_id** : Web ログイン失敗ページを定義します。
(注) コントローラのデフォルトのログイン失敗ページを使用するには、**config guest-lan custom-web loginfailure-page noneguest_lan_id** コマンドを入力します。
- **config guest-lan custom-web logout-page page_name guest_lan_id** : Web ログアウト ページを定義します。
(注) コントローラのデフォルトのログアウト ページを使用するには、**config guest-lan custom-web logout-page noneguest_lan_id** コマンドを入力します。

ステップ 10 有線ゲスト ユーザが Web ログイン ページにアクセスする前に有線ゲスト ユーザを外部サーバにリダイレクトする場合は、次のコマンドを入力して、外部サーバの URL を指定します。

```
config guest-lan custom-web ext-webauth-url ext_web_url guest_lan_id
```

ステップ 11 ローカル (コントローラ) または外部 (RADIUS、LDAP) の Web 認証サーバの接続順序を定義するには、次のコマンドを入力します。

```
config wlan security web-auth server-precedence wlan_id {local | ldap | radius} {local | ldap | radius} {local | ldap | radius}
```

サーバの Web 認証は、デフォルトではローカル、RADIUS、LDAP の順になっています。

- (注) すべての外部サーバをコントローラで事前に設定しておく必要があります。[RADIUS Authentication Servers] ページまたは [LDAP Servers] ページでこれらを設定できます。

ステップ 12 有線ゲスト ユーザ用の Web ログイン ページを定義するには、次のコマンドを入力します。

```
config guest-lan custom-web webauth-type {internal | customized | external} guest_lan_id
```

値は次のとおりです。

- **internal** は、コントローラのデフォルト Web ログイン ページを表示します。これは、デフォルト値です。
- **customized** では、ステップ 9 で設定したカスタム Web ページ (ログイン ページ、ログイン失敗ページ、またはログアウト ページ) が表示されます。
- **external** は、ステップ 10 で設定した URL にユーザをリダイレクトします。

ステップ 13 グローバル カスタム Web 設定ではなく、ゲスト LAN 固有のカスタム Web 設定を使用するには、次のコマンドを入力します。

```
config guest-lan custom-web global disable guest_lan_id
```

(注) **config guest-lan custom-web global enable guest_lan_id** コマンドを入力すると、グローバルレベルのカスタム Web 認証設定が使用されます。

ステップ 14 次のコマンドを入力して、変更を保存します。

save config

(注) 設定された Web 認証ページの情報、**show run-config** コマンドおよび **show running-config** コマンドの両方に表示されます。

ステップ 15 次のコマンドを入力して、特定のゲスト LAN に対するカスタマイズ Web 認証設定を表示します。

show custom-web {all | guest-lan guest_lan_id}

(注) 内部の Web 認証が設定されていると、Web Authentication Type は、外部 (コントローラレベル) またはカスタマイズ (WLAN プロファイルレベル) ではなく内部として表示されます。

ステップ 16 次のコマンドを入力して、ローカルインターフェイスの要約を表示します。

show interface summary

(注) この例の有線ゲスト LAN のインターフェイス名は、*wired-guest*、VLAN ID は 236 です。

次のコマンドを入力して、詳細なインターフェイス情報を表示します。

show interface detailed interface_name

ステップ 17 次のコマンドを入力して、特定の有線ゲスト LAN の設定を表示します。

show guest-lan guest_lan_id

(注) **show guest-lan summary** コマンドを入力して、コントローラ上で設定されているすべての有線ゲスト LAN を表示します。

ステップ 18 次のコマンドを入力して、アクティブな有線ゲスト LAN クライアントを表示します。

show client summary guest-lan

ステップ 19 次のコマンドを入力して、特定のクライアントの詳細情報を表示します。

show client detail client_mac

IPv6 クライアントのゲストアクセスのサポート

クライアントが認証されるまで、クライアントは WebAuth 状態です。コントローラは、この状態の IPv4 トラフィックと IPv6 トラフィックの両方を代行受信し、コントローラの仮想 IP アドレスにリダイレクトします。認証されると、ユーザの MAC アドレスが RUN 状態に移行し、IPv4 トラフィックと IPv6 トラフィックの両方が通過を許可されます。

IPv6 専用クライアントのリダイレクションをサポートするために、コントローラは、コントローラに設定された IPv4 仮想アドレスに基づいて IPv6 仮想アドレスを自動的に作成します。仮想 IPv6 アドレスは、`[::ffff:<仮想 IPv4 アドレス>]` という表記法に従います。たとえば、仮想 IP アドレス 192.0.2.1 は、`[::ffff:192.0.2.1]` に変換されます。IPv6 キャプティブポータルが表示されるためには、ユーザは、DNSv6 (AAAA) レコードを返す、IPv6 に解決できる DNS エントリ (`ipv6.google.com` など) を要求する必要があります。



第 26 章

Ethernet over GRE トンネル

- [Ethernet over GRE トンネルについて](#), 281 ページ
- [EoGRE トンネリングに関する制約事項](#), 285 ページ
- [Cisco WLC での EoGRE の設定 \(GUI\)](#), 286 ページ
- [WLC での EoGRE の設定 \(CLI\)](#), 288 ページ
- [FlexConnect AP の EoGRE の設定 \(GUI\)](#), 289 ページ
- [FlexConnect AP の EoGRE の設定 \(CLI\)](#), 289 ページ

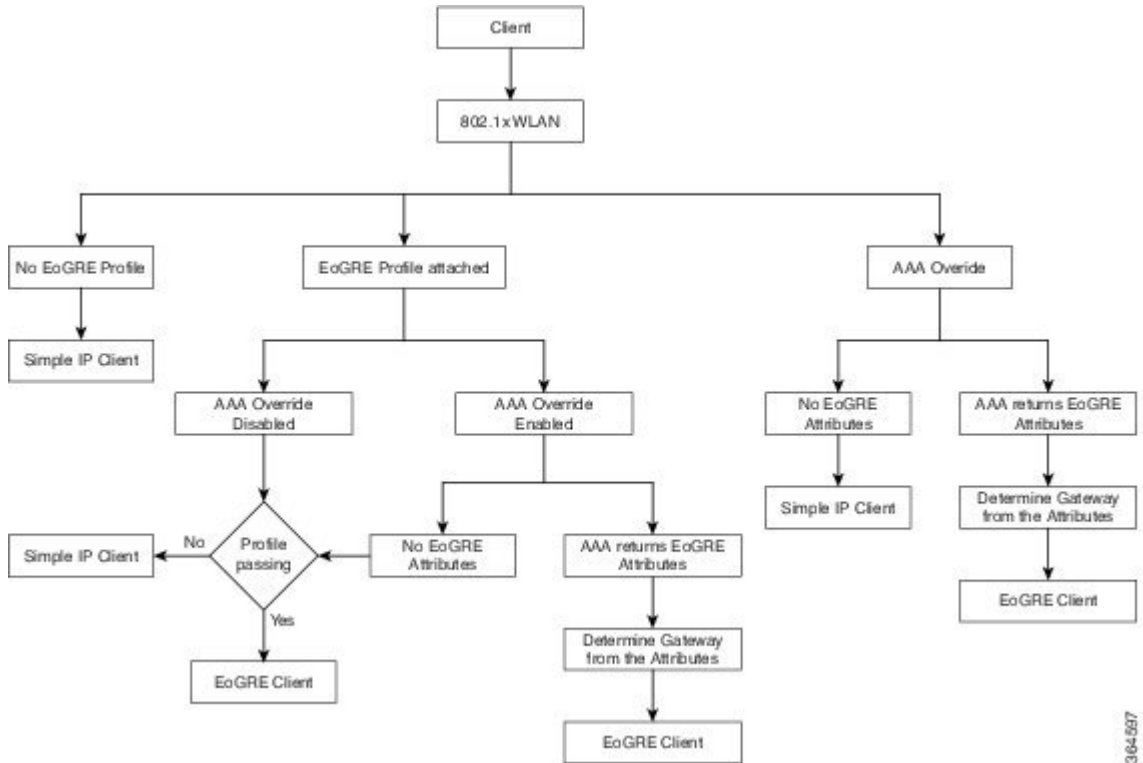
Ethernet over GRE トンネルについて

Ethernet over GRE (EoGRE) は、ホットスポットから送信された Wi-Fi トラフィックを集約するための新しいアグリゲーションソリューションです。このソリューションでは、顧客宅内機器 (CPE) デバイスで、エンドホストから届いたイーサネットトラフィックをブリッジし、そのトラフィックを IP GRE トンネルでイーサネットパケットにカプセル化できます。IP GRE トンネルがサービスプロバイダーのブロードバンドネットワーク ゲートウェイで終わると、エンドホストのトラフィックは終了し、エンドホスト用にサブスクライバセッションが開始します。

Cisco WLC と Cisco FlexConnect AP の EoGRE の設計と導入に関する詳細は、『[EoGRE Deployment Guide](#)』を参照してください。

802.1X 認証ベースの WLAN の EoGRE

図 24 : 802.1X 認証ベースの WLAN の EoGRE ワークフロー

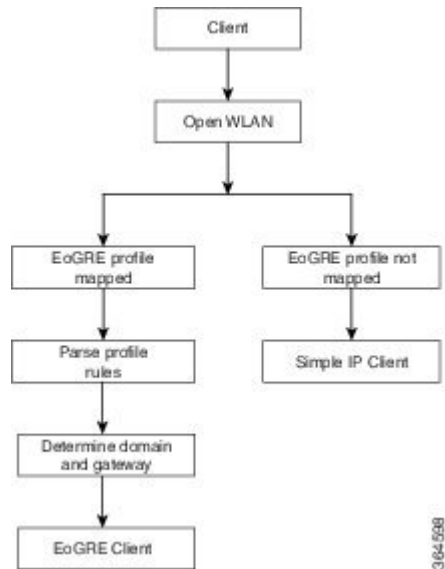


802.1X 認証	スイッチング	AP モード	EoGRE	SimpleIP
Central+No FlexConnect バックアップ RADIUS サーバ	ローカル	接続済み	クライアントは EoGRE として参加できます	クライアントは SimpleIP として参加します
Central+No FlexConnect バックアップ RADIUS サーバ	ローカル	スタンドアロン	新しいクライアントは参加できません。既存のクライアントが機能します	新しいクライアントは参加できません。既存のクライアントが機能します
Central+No FlexConnect バックアップ RADIUS サーバ	ローカル	スタンドアロンのブート	クライアントは参加できません	クライアントは参加できません

802.1X 認証	スイッチング	AP モード	EoGRE	SimpleIP
ローカル AP Auth+No FlexConnect バックアップ RADIUS サーバ	ローカル	接続済み	クライアントは SimpleIP になります	クライアントは SimpleIP として参加します
ローカル AP Auth+No FlexConnect バックアップ RADIUS サーバ	ローカル	スタンドアロン	クライアントは SimpleIP になります	既存のクライアントと新規クライアントが予定どおりに動作します
ローカル AP Auth+No FlexConnect バックアップ RADIUS サーバ	ローカル	スタンドアロンのブート	クライアントは SimpleIP になります	クライアントが参加できます
Central+FlexConnect バックアップ RADIUS サーバ	ローカル	接続済み	クライアントは EoGRE として参加します	既存のクライアントと新規クライアントが予定どおりに動作します
Central+FlexConnect バックアップ RADIUS サーバ	ローカル	スタンドアロン	既存のクライアントは引き続き EoGRE であり、新規クライアントは SimpleIP として参加します	既存のクライアントと新規クライアントが予定どおりに動作します
Central+FlexConnect バックアップ RADIUS サーバ	ローカル	スタンドアロンのブート	クライアントは SimpleIP になります	既存のクライアントと新規クライアントが予定どおりに動作します

オープン認証ベースの WLAN の EoGRE

図 25: オープン認証ベースの WLAN の EoGRE ワークフロー



(注) オープンな WLAN では、プロファイルは *ルールという 1 つのルールのみ持つことができます。オープン認証 WLAN に複数のルールがあるプロファイルのマッピングはサポートされていません。すべてのクライアントが EoGRE クライアントです。

オープン認証	スイッチング	AP モード	EoGRE
中央	ローカル	接続済み	クライアントは EoGRE として参加します
中央	ローカル	スタンドアロン	新規クライアントは参加できません。既存クライアントが参加します
中央	ローカル	スタンドアロンのブート	クライアントは参加できません

トンネル送信元の変更

リリース 8.2 以前は、管理 IP アドレスをトンネルエンドポイントとして使用していました。リリース 8.2 では、必要に応じて、管理インターフェイス以外の任意の L3 動的インターフェイスをトンネルエンドポイントとして指定できるようになりました。

その他の参考資料

- 『Ethernet over GRE Tunnels』
- 『Service Provider Wi-Fi: Support for Integrated Ethernet Over GRE』
- 『Intelligent Wireless Access Gateway Configuration Guide』

EoGRE トンネリングに関する制約事項

- EoGRE-AP 機能は、Cisco 700 シリーズ アクセス ポイントではサポートされていません。
- プロファイルが WLAN に関連付けられている場合、トンネル プロファイルを編集または削除することはできません。WLAN からプロファイルの関連付けを解除してから、プロファイルを編集または削除します。
- ゲートウェイがすでにドメインに関連付けられている場合、トンネルゲートウェイを編集または削除することはできません。ドメインからトンネルゲートウェイの関連付けを解除してから、トンネルゲートウェイを編集または削除します。
- ドメインがすでにトンネル プロファイル ルールに関連付けられている場合、ドメインを編集または削除することはできません。トンネル プロファイル ルールからドメインの関連付けを解除してから、ドメインを編集または削除します。
- ドメインがすぐに変更される場合、ドメインに関連付けられているクライアントは認証解除されます。
- ICMP パケットをブロックする可能性があるファイアウォールは設定しないことをお勧めします。
- AAA としてのトンネルゲートウェイ (TGW) および RADIUS レルム機能は同時に使用してはなりません。
- AAA としてのトンネルゲートウェイ (TGW) は、FlexConnect AP の EoGRE ではサポートされていません。
- FlexGroup name DHCP オプション 82 は、第 1 世代タイプ AP シリーズでは機能しません。
- オープンな WLAN では、プロファイルは * ルールという 1 つのルールのみ持つことができます。オープン認証 WLAN に複数のルールがあるプロファイルのマッピングはサポートされていません。
- EoGRE クライアントはローカル スイッチング VLAN から IPv6 アドレスを取得します。
- ローカル スイッチング VLAN のブロードキャスト/マルチキャスト トラフィックは EoGRE クライアントに到達します。
- FlexConnect+Bridge モードはサポートされていません。
- スタンドアロンモード: EoGRE クライアントの高速ローミングはサポートされていません。
- WebAuth はサポートされていません。

- FlexConnect AP ローカル認証はサポートされていません。
- FlexConnect AP バックアップ RADIUS サーバはサポートされていません。
- スタティック IP を持つ EoGRE クライアントはサポートされていません。
- WLAN の FlexConnect ACL は EoGRE クライアントでは動作しません。
- 耐障害性の後、クライアントタイプは SimpleIP です。これは、30 秒後に EoGRE に変更されます。
- パス MTU ディスカバリは FlexConnect AP ではサポートされていません。AP ゲートウェイの MTU は 1500 バイトです。

Cisco WLC での EoGRE の設定 (GUI)

ステップ 1 トンネル ゲートウェイを作成し、ハートビートを設定します。

- a) [Controller] > [Tunneling] > [EoGRE] の順に選択します。
- b) [Interface Name] を入力します。
トンネルの送信元として使用するコントローラにあるインターフェイス。
- c) [Heartbeat Interval] を設定します。デフォルト インターバルは 60 秒です。
シスコ ワイヤレス コントローラ (WLC) はキープアライブ ping を 60 秒ごとに送信します。
- d) [Max Heartbeat Skip Count] を設定します。デフォルト値は 3 に設定されています。
3 つのキープアライブ ping の後に TGW が応答しない場合、Cisco WLC は TGW を動作不能にマークします。スキップカウント数により TGW が動作不能であると認識される前に、TGW が何回連続で応答をスキップできるか決定します。
- e) [TGW Name] を指定します。
- f) [TGW IP Address] を指定します。
IPv4 アドレス形式のみサポートされています。該当のトンネル ゲートウェイは、最大 10 個作成できます。
- g) [Domain Name] を指定します。
- h) 作成したトンネルとして [TGW-1] をプライマリ トンネル ゲートウェイとして指定し、[Add] をクリックします。
トンネル ゲートウェイが到達可能であれば、状態が [TGW List] で UP として表示されるはずです。
ドメインは、冗長性の目的で使用されている 1 つ以上のトンネルの仮想コレクションを表しています。最大 16 のトンネルがドメインに存在できます。1 つのトンネルで障害が発生すると、トラフィックは別の TGW にリダイレクトされます。

ステップ 2 ネットワーク プロファイルを作成します。

- a) [Controller] > [Tunneling] > [Profiles] の順に選択します。
- b) プロファイル名を指定して、[Add] をクリックします。

プロファイル名は [Profile List] の下に表示されます。

ステップ 3 トンネルプロファイルルールを定義します。

- a) 作成したトンネルプロファイルをクリックします。
- b) [Rule] タブで、特定のレلمをプロファイルにマッピングするために、レلم名を入力します。レلمは user_name@realm など、@ の後の文字列です。[Realm] に一致させるには、* を使用し、すべてのレلمは受け入れます。
- c) [EoGRE] として [Tunnel Type] を選択します。
- d) [VLAN] を [0] に設定します。
- e) ステップ 1 で作成した [Gateway Domain] を選択します。
- f) [Add] をクリックして、このルールをトンネルプロファイルに追加します。

ステップ 4 トンネルパラメータを指定します。

- a) [Tunnel Parameters] タブで、[Gateway as AAA Proxy] および [Gateway as Accounting Proxy] (任意) チェックボックスをオンにして、トンネルゲートウェイを AAA プロキシおよびアカウンティングプロキシとして設定します。
- b) (任意) [DHCP Option-82] チェックボックスをオンにします。
(注) DHCP オプション 82 の設定は、IPv6 クライアントではサポートされていません。
- c) DHCP オプション 82 の形式として [Binary] または [ASCII] を選択します。
- d) [DHCP Option 82 Delimiter] を指定します。デフォルトは「;」です。
- e) [Circuit-ID] および [Remote-ID] 情報を指定します。それぞれフィールドを最大 5 つまで選択し、適宜ソートできます。
- f) [Apply] をクリックします。

ステップ 5 ステップ 1 で指定したトンネルゲートウェイの IP アドレスをサーバの IP アドレスとして指定して RADIUS 認証サーバまたはアカウンティングサーバ、あるいはその両方を作成し、[Tunnel Proxy] を有効にします。RADIUS サーバを作成する方法については、『Security Solutions』の「Configuring RADIUS」の章を参照してください。

ステップ 6 WLAN にトンネルプロファイルを関連付けます。

- a) [WLANs] を選択し、トンネルプロファイルを関連付ける必要がある WLAN ID をクリックします。
- b) [Tunneling] の [Advanced] タブで、[Tunnel Profile] を選択します。
- c) (任意) WLAN に AAA Override を有効にするよう選択できます。つまり、Cisco WLC が RADIUS サーバから返される属性を受け入れることができます。
- d) 設定を保存します。

ステップ 7 トンネルが正しく設定されているかどうか確認します。

- a) [Controller] > [Tunneling] > [Profiles] の順に選択します。
- b) プロファイル名が正しい WLAN にマッピングされているかどうか確認します。

WLC での EoGRE の設定 (CLI)

- 次のコマンドを入力して、キープアライブ ping パラメータを設定します。
 - **config tunnel eogre heart-beat interval***seconds*
 - **config tunnel eogre heart-beat max-skip-count***number*
- 次のコマンドを入力して、新しい EoGRE トンネル ゲートウェイを追加する、または既存のゲートウェイを削除または変更します。
 - **config tunnel eogre gateway add***name***ipv4-address***ip-addr*
 - **config tunnel eogre gateway delete***name*
 - **config tunnel eogre gateway modify***name***ipv4-address***ip-addr*
- 次のコマンドを入力して、EoGRE トンネル ゲートウェイ ドメインを設定します。
 - **config tunnel eogre domain {create | delete} domain-name**
 - **config tunnel eogre domain {add | remove} domain-name gateway-name**
- 次のコマンドを入力して、トンネル プロファイルを設定します。
 - **config tunnel eogre profile {create | copy | delete | rule | eogre}**

CLI に表示される手順に従って各パラメータを設定します。
- 次のコマンドを入力して、ゲートウェイを AAA プロキシとして設定します。
 - **config tunnel profile eogre profile-name gateway-radius-proxy {enable | disable}**
 - **config tunnel profile eogre profile-name gateway-radius-proxy accounting {enable | disable}**
- 次のコマンドを入力して、トンネル プロファイルの DHCP オプション 82 を設定します。



(注) DHCP オプション 82 の設定は、IPv6 クライアントではサポートされていません。

- **config tunnel profile eogre profile-name DHCP-Opt-82 {enable | disable}**
 - **config tunnel profile eogre profile-name DHCP-Opt-82 format {binary | ascii}**
 - **config tunnel profile eogre profile-name DHCP-Opt-82 delimiter***character*
 - **config tunnel profile eogre profile-name DHCP-Opt-82 {circuit-id | remote-id} supported-parameter**
- 次のコマンドを入力して、EoGRE トンネル インターフェイスを設定します。
 - **config tunnel eogre interface***interface-name*



(注) トンネル送信元のインターフェイスを設定する前に、インターフェイスに関連付けられた WLAN を無効にします。

• 次のコマンドを入力して、EoGRE トンネリングの詳細を表示します。

- **show tunnel eogre {domain | gateway} summary**
- **show tunnel eogre summary**
- **show tunnel eogre statistics**
- **show tunnel profile summary**
- **show tunnel profile detail***profile-name*

FlexConnect AP の EoGRE の設定 (GUI)

- AP が FlexConnect モードになっていることを確認します。
- Cisco WLC のトンネル設定は、トンネルプロファイルが WLAN に関連付けられている場合、Cisco FlexConnect AP にも適用されます。

ステップ 1 [WLANs] > [WLANs] の順に選択します。

ステップ 2 [WLAN ID] をクリックします。

ステップ 3 [FlexConnect] の [Advanced] タブで、[FlexConnect Local Switching] を有効にします。

(注) FlexConnect ローカルスイッチングオプションのみ FlexConnect AP または FlexConnect グループで設定し、FlexConnect AP トンネルを有効にします。

ステップ 4 設定を保存します。

FlexConnect AP の EoGRE の設定 (CLI)

- AP が FlexConnect モードになっていることを確認します。
- Cisco WLC のトンネル設定は、トンネルプロファイルが WLAN に関連付けられている場合、Cisco FlexConnect AP にも適用されます。

ステップ 1 次のコマンドを入力して、WLAN に関連付けられた FlexConnect AP のローカルスイッチングを有効にします。

config wlan flexconnect local-switching*wlan-identable*

ステップ 2 次のコマンドを入力して、EoGRE 設定をモニタします。

show ap eogre {**domain** | **gateway**} *ap-name*



第 27 章

トラブルシューティング

- [LED の解釈, 291 ページ](#)
- [システム メッセージ, 292 ページ](#)
- [システム リソースの表示, 296 ページ](#)
- [CLI を使用したトラブルシューティング, 297 ページ](#)
- [システム ロギングとメッセージ ロギングの設定, 299 ページ](#)
- [アクセス ポイント イベント ログの表示, 306 ページ](#)
- [ログとクラッシュ ファイルのアップロード, 307 ページ](#)
- [コントローラからのコア ダンプのアップロード, 309 ページ](#)
- [パケット キャプチャ ファイルのアップロード, 313 ページ](#)
- [メモリ リークの監視, 316 ページ](#)
- [CCXv5 クライアント デバイスのトラブルシューティング, 318 ページ](#)
- [デバッグ ファシリティの使用法, 329 ページ](#)
- [無線スニファの設定, 334 ページ](#)
- [Telnet または SSH_old を使用したアクセス ポイントのトラブルシューティング, 337 ページ](#)
- [アクセス ポイント監視サービスのデバッグ, 339 ページ](#)
- [OfficeExtend アクセス ポイントのトラブルシューティング, 340 ページ](#)

LED の解釈

LED の解釈について

ここでは、コントローラ LED と Lightweight アクセス ポイント LED を解釈する方法について説明します。

コントローラの LED の解釈

LED パターンの説明については、各コントローラのクイック スタート ガイドを参照してください。コントローラのリストおよびそれらに対応するマニュアルについては、<http://www.cisco.com/en/US/products/hw/wireless/index.html> を参照してください。

Lightweight アクセス ポイント LED の解釈

LED パターンの説明については、各アクセス ポイントのクイック スタート ガイドまたはハードウェア インストール ガイドを参照してください。アクセス ポイントのリストおよびそれらに対応するマニュアルについては、<http://www.cisco.com/en/US/products/hw/wireless/index.html> を参照してください。

システム メッセージ

システム メッセージについて

次の表に、一般的なシステム メッセージとその説明を示します。すべてのシステム メッセージの一覧については、『Cisco Wireless LAN Controller System Message Guide, Release 7.0』を参照してください。

表 6: システム メッセージとその説明

エラー メッセージ	説明
apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	クライアントは、セキュリティが有効になっている WLAN 上でアソシエーション要求を送信していますが、アソシエーション要求の Capability フィールド内の保護ビットが 0 に設定されています。設計されたとおりに、コントローラはアソシエーション要求を却下し、クライアントにはアソシエーション エラーが表示されます。
dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	コントローラの Network Processing Unit (NPU) はタイムアウト メッセージを中央処理装置 (CPU) に送信し、特定のクライアントがタイムアウトまたは期限切れであることを知らせます。この状況は、通常、CPU が内部データベースからワイヤレス クライアントを削除したことを NPU に通知していない場合に起こります。クライアントは NPU データベースにとどまるため、ネットワーク プロセッサで期限切れになり、CPU に通知されます。CPU はデータベースにないクライアントを検出して、このメッセージを送信します。

エラーメッセージ	説明
STATION_DISASSOCIATE	クライアントが使用を意図的に中断したか、サービスの中断を受けた可能性があります。
STATION_DEAUTHENTICATE	クライアントが使用を意図的に中断したか、認証上の問題があることを示しています。
STATION_AUTHENTICATION_FAIL	設定の有効性、キーの不一致、またはその他の問題を確認してください。
STATION_ASSOCIATE_FAIL	Cisco Radio 上の負荷または信号の品質に問題がないか確認します。
LRAD_ASSOCIATED	アソシエートされた Lightweight アクセスポイントがこのコントローラで管理されるようになりました。
LRAD_DISASSOCIATED	Lightweight アクセスポイントが他のコントローラにアソシエートされているか、完全に接続不可能になっている可能性があります。
LRAD_UP	Lightweight アクセスポイントは正常に動作しています。処理は必要ありません。
LRAD_DOWN	Lightweight アクセスポイントに問題があるか、管理上無効にされています。
LRADIF_UP	Cisco Radio は稼働状態です。
LRADIF_DOWN	Cisco Radio に問題があるか、管理上無効にされています。
LRADIF_LOAD_PROFILE_FAILED	クライアント密度がシステム キャパシティを超えている可能性があります。
LRADIF_NOISE_PROFILE_FAILED	802.11 以外のノイズが設定しきい値を超えました。
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 干渉がチャネル上のしきい値を超えました。チャネルの割り当てを確認してください。
LRADIF_COVERAGE_PROFILE_FAILED	カバレッジホールの可能性が検出されました。Lightweight アクセスポイント履歴を調べて、一般的な問題がないかどうかを確認し、必要に応じて Lightweight アクセスポイントを追加してください。
LRADIF_LOAD_PROFILE_PASSED	負荷がしきい値の制限内に戻りました。

エラーメッセージ	説明
LRADIF_NOISE_PROFILE_PASSED	検出されたノイズがしきい値より小さくなりました。
LRADIF_INTERFERENCE_PROFILE_PASSED	検出された干渉がしきい値より小さくなりました。
LRADIF_COVERAGE_PROFILE_PASSED	不良電波を受信しているクライアント数はしきい値内です。
LRADIF_CURRENT_TXPOWER_CHANGED	情報メッセージ。
LRADIF_CURRENT_CHANNEL_CHANGED	情報メッセージ。
LRADIF_RTS_THRESHOLD_CHANGED	情報メッセージ。
LRADIF_ED_THRESHOLD_CHANGED	情報メッセージ。
LRADIF_FRAGMENTATION_THRESHOLD_CHANGED	情報メッセージ。
RRM_DOT11_A_GROUPING_DONE	情報メッセージ。
RRM_DOT11_B_GROUPING_DONE	情報メッセージ。
ROGUE_AP_DETECTED	セキュリティ上の問題がある可能性があります。マップとトレンドを使用して調べてください。
ROGUE_AP_REMOVED	検出された不正なアクセスポイントがタイムアウトしました。ユニットがシャットダウンしたか、カバレッジエリア外に移動しました。
AP_MAX_ROGUE_COUNT_EXCEEDED	現在のアクティブな不正なアクセスポイント数がシステムのしきい値を超えました。
LINK_UP	肯定的な確認メッセージです。
LINK_DOWN	ポートに問題があるか、管理上無効にされています。
LINK_FAILURE	ポートに問題があるか、管理上無効にされています。
AUTHENTICATION_FAILURE	セキュリティ違反の試行が検出されました。調査してください。
STP_NEWROOT	情報メッセージ。
STP_TOPOLOGY_CHANGE	情報メッセージ。

エラーメッセージ	説明
IPSEC_ESP_AUTH_FAILURE	WLAN IPsec の設定を確認してください。
IPSEC_ESP_REPLAY_FAILURE	IP アドレスのスプーフィング試行がないかどうか確認してください。
IPSEC_ESP_POLICY_FAILURE	WLAN とクライアントの間で IPsec 設定が矛盾していないかどうか確認してください。
IPSEC_ESP_INVALID_SPI	情報メッセージ。
IPSEC_OTHER_POLICY_FAILURE	WLAN とクライアントの間で IPsec 設定が矛盾していないかどうか確認してください。
IPSEC_IKE_NEG_FAILURE	WLAN とクライアントの間で IPsec IKE 設定が矛盾していないかどうか確認してください。
IPSEC_SUITE_NEG_FAILURE	WLAN とクライアントの間で IPsec IKE 設定が矛盾していないかどうか確認してください。
IPSEC_INVALID_COOKIE	情報メッセージ。
RADIOS_EXCEEDED	サポートされる Cisco Radio の最大数を超過しました。同じレイヤ2ネットワークでコントローラの障害を調べるか、別のコントローラを追加してください。
SENSED_TEMPERATURE_HIGH	ファン、空調、その他の冷却装置を確認してください。
SENSED_TEMPERATURE_LOW	室温が低くないか、低温の原因が他にないかどうかを調べてください。
TEMPERATURE_SENSOR_FAILURE	温度センサーをできるだけ早く交換してください。
TEMPERATURE_SENSOR_CLEAR	温度センサーは正常に動作しています。
POE_CONTROLLER_FAILURE	ポートを確認してください。深刻な障害が発生している可能性があります。
MAX_ROGUE_COUNT_EXCEEDED	現在のアクティブな不正なアクセス ポイント数がシステムのしきい値を超過しました。
SWITCH_UP	コントローラは SNMP のポーリングに応答しています。
SWITCH_DOWN	コントローラは SNMP のポーリングに応答していません。コントローラと SNMP の設定を確認してください。

エラー メッセージ	説明
RADIUS_SERVERS_FAILED	RADIUS とコントローラとの間のネットワーク接続を確認してください。
CONFIG_SAVED	実行コンフィギュレーションがフラッシュに保存されました。この設定はリブート後にアクティブになります。
MULTIPLE_USERS	同じユーザ名の別のユーザがログインしています。
FAN_FAILURE	コントローラの温度を監視して、オーバーヒートしないようにしてください。
POWER_SUPPLY_CHANGE	電源が故障していないか確認してください。
COLD_START	コントローラはリブートされた可能性があります。
WARM_START	コントローラはリブートされた可能性があります。

システム リソースの表示

システム リソースの表示について

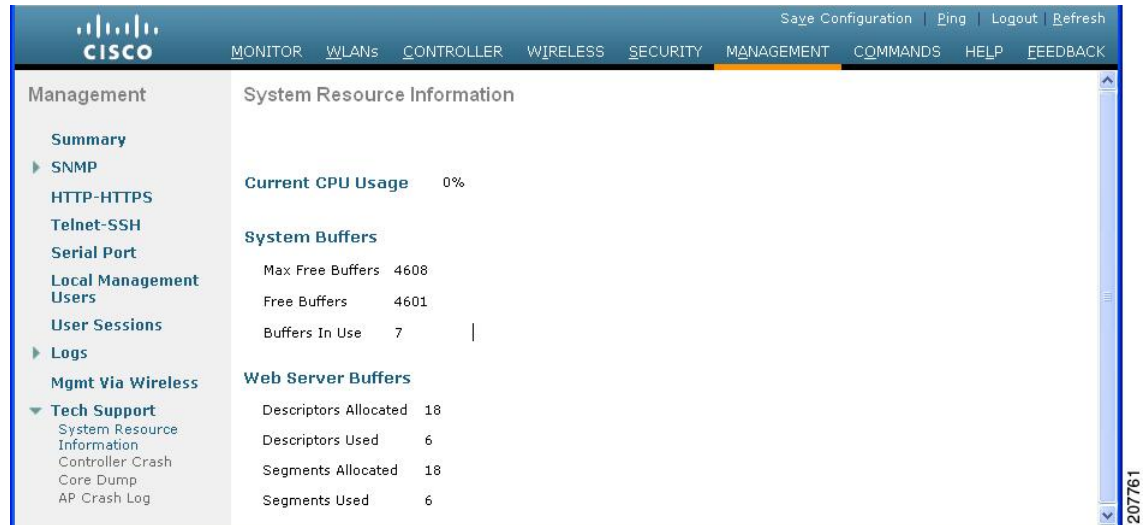
コントローラによって使用されているシステムリソースの量を調べることができます。具体的には、現在のコントローラ CPU 使用率、システム バッファ、および Web サーバ バッファの状態が表示されます。

Cisco 5500 シリーズ コントローラでは、複数の CPU が搭載されているため、個々の CPU の使用率を表示できます。各 CPU について、その CPU の使用率と、割り込みレベルにおける CPU 使用時間の割合が、たとえば 0%/3% のように表示されます。

システム リソースの表示（GUI）

コントローラ GUI で、[Management] > [Tech Support] > [System Resource Information] を選択します。[System Resource Information] ページが表示されます。

図 26 : [System Resource Information] ページ



システム リソースの表示（CLI）

コントローラ CLI で、次のコマンドを入力します。

- **show cpu**

ここで、最初の数値は、コントローラがユーザアプリケーションの実行に使用した CPU の割合です。2 番目の数値は、コントローラが OS サービスの実行に使用した CPU の割合です。

- **show tech-support**

CLI を使用したトラブルシューティング

お使いのコントローラで問題が発生した場合には、この項のコマンドを使用して情報を収集し、問題をデバッグすることができます。

- **show process cpu** : システム内で各タスクが使用している CPU の現状を表示します。このコマンドは、1 つのタスクが CPU を独占したり、他のタスクの実行を妨げたりしていないかを理解するのに便利です。

[Priority] フィールドには、1) 実際のファンクション コールから生成されたタスクの最初の優先順位、2) システムの各優先順位で割ったタスクの優先順位の 2 つの値が表示されます。

[CPU Use] フィールドは、それぞれのタスクの CPU 利用率です。

[Reaper]フィールドには、1) ユーザモードの操作でそのタスクが予定されている所要時間、2) システムモードの操作でそのタスクが予定されている所要時間、3) そのタスクがReaperタスク モニタで監視されているかどうか（監視されている場合は「T」で表示）の3つの値が表示されます。タスクがReaperタスク モニタで監視されている場合は、タスク モニタに警告するまでのタイムアウト値も秒単位で示されます。



(注) CPU 総利用率を % で表示するには、**show cpu** コマンドを入力してください。

- **show process memory** : システム内で各プロセスが割り当てているメモリと、割り当て解除されているメモリの現状を表示します。

上の例のフィールドの説明は、次のとおりです。

[Name] フィールドは、CPU が実行対象としているタスクです。

[Priority] フィールドには、1) 実際のファンクション コールから生成されたタスクの最初の優先順位、2) システムの各優先順位で割ったタスクの優先順位の2つの値が表示されます。

[BytesInUse] フィールドは、ダイナミック メモリの割り当てでそのタスクに使用される実際のバイト数です。

[BlocksInUse] フィールドは、そのタスクを実行する際に割り当てられる連続メモリです。

[Reaper]フィールドには、1) ユーザモードの操作でそのタスクが予定されている所要時間、2) システムモードの操作でそのタスクが予定されている所要時間、3) そのタスクがReaperタスク モニタで監視されているかどうか（監視されている場合は「T」で表示）の3つの値が表示されます。タスクがReaperタスク モニタで監視されている場合は、タスク モニタに警告するまでのタイムアウト値も秒単位で示されます。

- **show tech-support** : 現在の設定内容、最新のクラッシュファイル、CPU利用率、メモリ利用率など、システムの状態についての一連の情報を表示します。
- **show run-config** : コントローラのすべての設定内容を表示します。アクセスポイント設定を除外するには、**show run-config no-ap** コマンドを使用します。



(注) パスワードをクリア テキストで表示する場合は、**config passwd-cleartext enable** コマンドを入力します。このコマンドを実行するには、admin パスワードを入力する必要があります。このコマンドは、この特定のセッションだけで有効です。リブート後には保存されません。

- **show run-config commands** : このコントローラに対して設定されているコマンドのリストが表示されます。このコマンドで表示されるのは、ユーザが設定した値だけです。システムにより設定されたデフォルト値は表示されません。

システム ロギングとメッセージ ロギングの設定

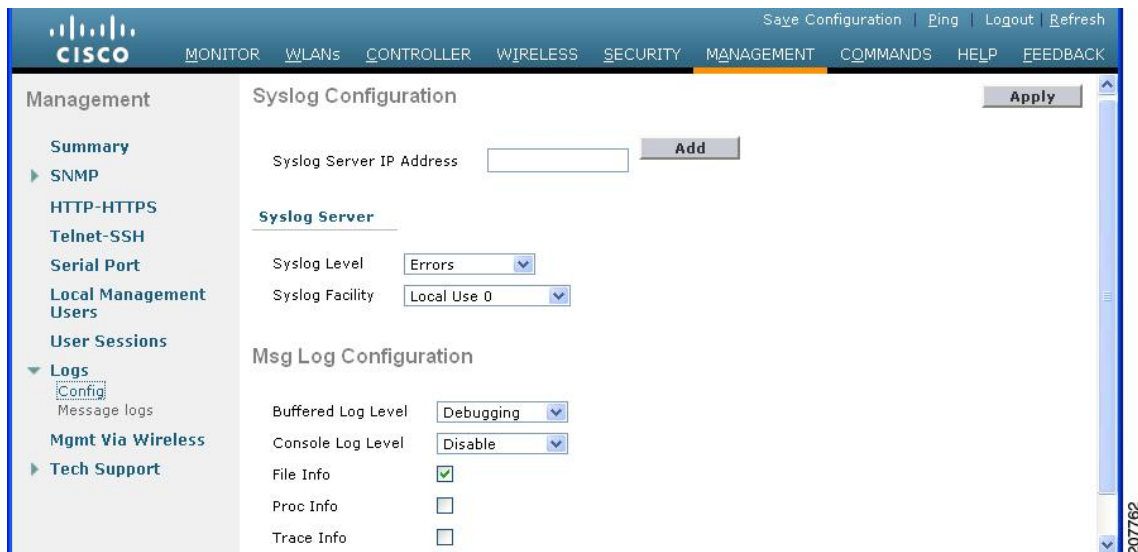
システム ロギングとメッセージ ロギングについて

システム ロギングを使用すると、コントローラのシステム イベントを最大 3 台のリモート syslog サーバにログできるようになります。syslog メッセージはコントローラに設定されている syslog サーバごとにログされるため、コントローラは各 syslog メッセージのコピーを送信します。複数のサーバに syslog メッセージを送信できるため、1 台の syslog サーバが一時的に使用できなくなってもメッセージが失われることはありません。メッセージロギングを使用すると、システムメッセージをコントローラのバッファまたはコンソールにログできるようになります。

システム ロギングとメッセージ ロギングの設定 (GUI)

ステップ 1 [Management] > [Logs] > [Config] の順に選択します。[Syslog Configuration] ページが表示されます。

図 27 : [Syslog Configuration] ページ



ステップ 2 [Syslog Server IP Address] テキスト ボックスに、syslog メッセージの送信先となるサーバの IP アドレスを入力し、[Add] をクリックします。コントローラには最大 3 台の syslog サーバを追加できます。このテキスト ボックスの下には、すでにコントローラに追加されている syslog サーバのリストが表示されます。

(注) コントローラから syslog サーバを削除するには、目的のサーバの右側の [Remove] をクリックします。

ステップ 3 syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、[Syslog Level] ドロップダウン リストから次のいずれかのオプションを選択します。

- [Emergencies] = 重大度レベル 0
- [Alerts] = 重大度レベル 1 (デフォルト値)
- [Critical] = 重大度レベル 2
- [Errors] = 重大度レベル 3
- [Warnings] = 重大度レベル 4
- [Notifications] = 重大度レベル 5
- [Informational] = 重大度レベル 6
- [Debugging] = 重大度レベル 7

syslog レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、syslog サーバに送信されます。たとえば、syslog レベルを [Warnings] (重大度レベル 4) に設定した場合は、重大度が 0 ~ 4 のメッセージしか syslog サーバに送信されません。

ステップ 4 syslog メッセージを syslog サーバに送信するファシリティを設定するには、[Syslog Facility] から次のいずれかのオプションを選択します。ドロップダウン リスト：

- [Kernel] = ファシリティ レベル 0
- [User Process] = ファシリティ レベル 1
- [Mail] = ファシリティ レベル 2
- [System Daemons] = ファシリティ レベル 3
- [Authorization] = ファシリティ レベル 4
- [Syslog] = ファシリティ レベル 5 (デフォルト値)
- [Line Printer] = ファシリティ レベル 6
- [USENET] = ファシリティ レベル 7
- [Unix-to-Unix Copy] = ファシリティ レベル 8
- [Cron] = ファシリティ レベル 9
- [FTP Daemon] = ファシリティ レベル 11
- [System Use 1] = ファシリティ レベル 12
- [System Use 2] = ファシリティ レベル 13
- [System Use 3] = ファシリティ レベル 14
- [System Use 4] = ファシリティ レベル 15
- [Local Use 0] = ファシリティ レベル 16
- [Local Use 2] = ファシリティ レベル 17

- [Local Use 3] = ファシリティ レベル 18
- [Local Use 4] = ファシリティ レベル 19
- [Local Use 5] = ファシリティ レベル 20
- [Local Use 5] = ファシリティ レベル 21
- [Local Use 5] = ファシリティ レベル 22
- [Local Use 5] = ファシリティ レベル 23

ステップ 5 [Apply] をクリックします。

ステップ 6 コントローラのバッファとコンソールに対するログ メッセージの重大度レベルを設定するには、[Buffered Log Level] ドロップダウンリストおよび [Console Log Level] ドロップダウンリストから次のいずれかのオプションを選択します。

- [Emergencies] = 重大度レベル 0
- [Alerts] = 重大度レベル 1
- [Critical] = 重大度レベル 2
- [Errors] = 重大度レベル 3 (デフォルト値)
- [Warnings] = 重大度レベル 4
- [Notifications] = 重大度レベル 5
- [Informational] = 重大度レベル 6
- [Debugging] = 重大度レベル 7
- [Disable] : このオプションは、コンソール ログ レベルの場合にのみ使用できます。このオプションを選択すると、コンソール ログが無効になります。

ログ レベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ログ レベルを Warnings (重大度レベル 4) に設定した場合は、重大度が 0 ~ 4 のメッセージしかログされません。

ステップ 7 ソース ファイルの情報をメッセージ ログに含める場合は、[File Info] チェックボックスをオンにします。デフォルト値はイネーブルです。

ステップ 8 トレースバック情報をメッセージ ログに含める場合は、[Trace Info] チェックボックスをオンにします。デフォルトでは無効になっています。

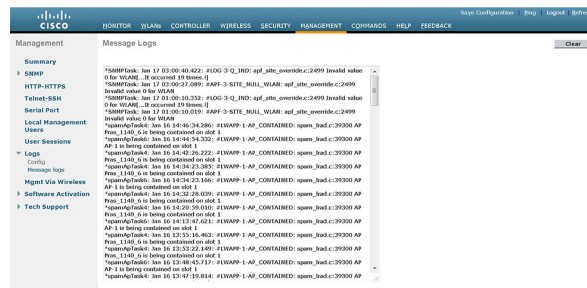
ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

メッセージ ログの表示 (GUI)

コントローラの GUI を使用してメッセージ ログを表示するには、[Management]>[Logs]>[Message Logs] の順に選択します。[Message Logs] ページが表示されます。

図 28 : [Message Logs] ページ



(注) コントローラから現在のメッセージ ログをクリアするには、[Clear] をクリックします。

システム ログとメッセージ ログの設定 (CLI)

ステップ 1 次のコマンドを入力して、システム ログを有効にし、syslog メッセージの送信先である syslog サーバの IP アドレスを設定します。

```
config logging syslog host server_IP_address
```

コントローラには最大 3 台の syslog サーバを追加できます。

(注) syslog サーバをコントローラから削除するには、次のコマンドを入力します。 **config logging syslog host server_IP_address delete**

ステップ 2 次のコマンドを入力して、syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定します。

```
config logging syslog level severity_level
```

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5

- informational = 重大度レベル 6
- debugging = 重大度レベル 7

(注) 代わりに、*severity_level* パラメータに 0 ~ 7 の数を入力することもできます。

(注) *syslog* レベルを設定する場合は、重大度がそのレベル以下であるメッセージだけが *syslog* サーバに送信されます。たとえば、*syslog* レベルを Warnings (重大度レベル 4) に設定した場合は、重大度が 0 ~ 4 のメッセージしか *syslog* サーバに送信されません。

ステップ 3 次のコマンドを入力して、特定のアクセスポイントまたはすべてのアクセスポイントに対する *syslog* メッセージのフィルタリングの重大度レベルを設定します。

```
config ap logging syslog level severity_level {Cisco_AP | all}
```

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

(注) *syslog* レベルを設定する場合は、重大度がそのレベル以下のメッセージだけがアクセスポイントに送信されます。たとえば、*syslog* レベルを警告 (重大度 4) に設定した場合は、重大度が 0 ~ 4 のメッセージだけがアクセスポイントに送信されます。

ステップ 4 次のコマンドを入力して、*syslog* サーバへ発信する *syslog* メッセージのファシリティを設定します。

```
config logging syslog facility facility_code
```

facility_code は、次のいずれかです。

- authorization = 許可システム。ファシリティ レベル = 4。
- auth-private = 許可システム (プライベート)。ファシリティ レベル = 10。
- cron = cron/at ファシリティ。ファシリティ レベル = 9。
- daemon = システム デーモン。ファシリティ レベル = 3。
- ftp = FTP デーモン。ファシリティ レベル = 11。
- kern = カーネル。ファシリティ レベル = 0。
- local0 = ローカル使用。ファシリティ レベル = 16。
- local1 = ローカル使用。ファシリティ レベル = 17。

- local2 = ローカル使用。 ファシリティ レベル = 18。
- local3 = ローカル使用。 ファシリティ レベル = 19。
- local4 = ローカル使用。 ファシリティ レベル = 20。
- local5 = ローカル使用。 ファシリティ レベル = 21。
- local6 = ローカル使用。 ファシリティ レベル = 22。
- local7 = ローカル使用。 ファシリティ レベル = 23。
- lpr = ライン プリンタ システム。 ファシリティ レベル = 6。
- mail = メール システム。 ファシリティ レベル = 2。
- news = USENET ニュース。 ファシリティ レベル = 7。
- sys12 = システム使用。 ファシリティ レベル = 12。
- sys13 = システム使用。 ファシリティ レベル = 13。
- sys14 = システム使用。 ファシリティ レベル = 14。
- sys15 = システム使用。 ファシリティ レベル = 15。
- syslog = syslog 自体。 ファシリティ レベル = 5。
- user = ユーザ プロセス。 ファシリティ レベル = 1。
- uucp = UNIX 間コピー システム。 ファシリティ レベル = 8。

ステップ 5 コントローラのバッファとコンソールに対するロギングメッセージの重大度レベルを設定するには、次のコマンドを入力します。

- **config logging buffered *severity_level***
- **config logging console *severity_level***

severity_level は、次のいずれかです。

- emergencies = 重大度レベル 0
- alerts = 重大度レベル 1
- critical = 重大度レベル 2
- errors = 重大度レベル 3
- warnings = 重大度レベル 4
- notifications = 重大度レベル 5
- informational = 重大度レベル 6
- debugging = 重大度レベル 7

(注) 代わりに、*severity_level* パラメータに 0 ~ 7 の数を入力することもできます。

(注) ログレベルを設定する場合は、重大度がそのレベルと等しいかそれ以下であるメッセージのみ、コントローラにログされます。たとえば、ログレベルを Warnings (重大度レベル 4) に設定した場合は、重大度が 0 ~ 4 のメッセージしかログされません。

ステップ 6 次のコマンドを入力して、コントローラ バッファ、コントローラ コンソール、または syslog サーバに対するデバッグ メッセージを保存します。

- **config logging debug buffered {enable | disable}**
- **config logging debug console {enable | disable}**
- **config logging debug syslog {enable | disable}**

デフォルトでは、console コマンドは有効 (enable)、buffered コマンドおよび syslog コマンドは無効 (disable) です。

ステップ 7 コントローラがメッセージ ログ内にソース ファイルの情報を含めるようにする、またはこの情報を表示しないようにするには、次のコマンドを入力します。

config logging fileinfo {enable | disable}

デフォルト値はイネーブルです。

ステップ 8 次のコマンドを入力して、プロセス情報をメッセージ ログに含めるように、またはこの情報を表示しないようにコントローラを設定します。

config logging procinfo {enable | disable}

デフォルト値はディセーブルです。

ステップ 9 次のコマンドを入力して、トレースバック情報をメッセージ ログに含めるように、またはこの情報を表示しないようにコントローラを設定します。

config logging traceinfo {enable | disable}

デフォルト値はディセーブルです。

ステップ 10 次のコマンドを入力して、ログ メッセージおよびデバッグ メッセージのタイムスタンプを有効または無効にします:

- **config service timestamps log {datetime | disable}**
- **config service timestamps debug {datetime | disable}**

値は次のとおりです。

- **datetime** = 標準の日付と時刻がタイムスタンプとしてメッセージに付加されます。これは、デフォルト値です。
- **disable** = メッセージにタイムスタンプは付加されません。

ステップ 11 次のコマンドを入力して、変更を保存します。

save config

システム ログとメッセージ ログの表示 (CLI)

ロギングパラメータとバッファの内容を表示するには、次のコマンドを入力します。

```
show logging
```

アクセスポイントイベントログの表示

アクセスポイントイベントログについて

アクセスポイントのイベントログには、すべてのシステムメッセージ（重大度が **notifications** 以上のもの）が記録されます。イベントログには最大 1024 行のメッセージを格納できます。1 行あたりの長さは最大 128 文字です。イベントログがいっぱいになったときは、新しいイベントメッセージを記録するために、最も古いメッセージが削除されます。イベントログはアクセスポイントフラッシュ上のファイルに保存されるので、リブートしても消去されません。アクセスポイントフラッシュへの書き込み回数を最小限にするために、イベントログの内容がイベントログファイルに書き込まれるのは、通常のリロード時またはクラッシュ時だけとなっています。

アクセスポイントイベントログの表示 (CLI)

アクセスポイントイベントログを表示する、またはコントローラから削除するには、次の CLI コマンドを使用します。

- コントローラに **join** されたアクセスポイントのイベントログファイルの内容を表示するには、次のコマンドを入力します。

```
show ap eventlog Cisco_AP
```

以下に類似した情報が表示されます。

```
AP event log download has been initiated
Waiting for download to complete

AP event log download completed.
===== AP Event log Contents =====
*Sep 22 11:44:00.573: %CAPWAP-5-CHANGED: CAPWAP changed state to IMAGE
*Sep 22 11:44:01.514: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to down
*Sep 22 11:44:01.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to down
*Sep 22 11:44:53.539: *** Access point reloading. Reason: NEW IMAGE DOWNLOAD ***
*Mar 1 00:00:39.078: %CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
*Mar 1 00:00:42.142: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:42.151: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:42.158: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:43.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to up
*Mar 1 00:00:43.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to up
*Mar 1 00:00:48.078: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
```



```
*Mar 1 00:01:42.144: %CDP PD-4-POWER OK: Full power - NEGOTIATED inline power source
*Mar 1 00:01:48.121: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP manager
  IP addresses remain
*Mar 1 00:01:48.122: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
```

- コントローラに join された特定のアクセス ポイントまたはすべてのアクセス ポイントの既存のイベント ログ ファイルを削除して空のイベント ログ ファイルを作成するには、次のコマンドを入力します。

```
clear ap-eventlog {specific Cisco_AP | all}
```

ログとクラッシュ ファイルのアップロード

ログとクラッシュ ファイルをアップロードするための前提条件

- この項の手順に従って、コントローラからログとクラッシュ ファイルをアップロードします。ただし、開始する前に、ファイルのアップロードに TFTP または FTP サーバを使用できることを確認します。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。
 - サービス ポート経由でアップロードする場合は、TFTP/FTP サーバがサービス ポートと同じサブネット上になければなりません。サービス ポートはルーティングできないからです。同じサブネット上にない場合は、コントローラ上に静的ルートを作成する必要があります。
 - ディストリビューション システム ネットワーク ポートを経由してアップロードする場合は、TFTP/FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。ディストリビューション システム ポートはルーティング可能であるためです。
 - Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。

ログとクラッシュ ファイルのアップロード (GUI)

ステップ 1 [Command] > [Upload File] を選択します。[Upload File from Controller] ページが表示されます。

ステップ 2 [File Type] ドロップダウン リストから、次のいずれかを選択します。

- Event Log
- Message Log

- **Trap Log**
- **Crash File**

ステップ3 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- TFTP
- FTP
- SFTP (7.4 以降のリリースで利用可能)

ステップ4 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。

ステップ5 [File Path] テキスト ボックスに、ログまたはクラッシュ ファイルのディレクトリ パスを入力します。

ステップ6 [File Name] テキスト ボックスに、ログまたはクラッシュ ファイルの名前を入力します。

ステップ7 [Transfer Mode] として [FTP] を選択した場合は、次の手順を実行します。

- 1 [Server Login Username] テキスト ボックスに、FTP サーバのログイン名を入力します。
- 2 [Server Login Password] テキスト ボックスに、FTP サーバのログイン パスワードを入力します。
- 3 [Server Port Number] テキスト ボックスに、FTP サーバのポート番号を入力します。サーバポートのデフォルト値は 21 です。

ステップ8 [Upload] をクリックすると、ログまたはクラッシュファイルがコントローラからアップロードされます。アップロードのステータスを示すメッセージが表示されます。

ログとクラッシュ ファイルのアップロード (CLI)

ステップ1 ファイルをコントローラからサーバに転送するには、次のコマンドを入力します。

```
transfer upload mode {tftp | ftp | sftp}
```

ステップ2 アップロードするタイプを指定するには、次のコマンドを入力します。

```
transfer upload datatype datatype
```

datatype には、次のオプションのいずれかを指定します。

- **crashfile** : システムのクラッシュ ファイルをアップロードします。
- **errorlog** : システムのエラー ログをアップロードします。
- **panic-crash-file** : カーネルパニックが発生した場合にカーネルパニック情報をアップロードします。
- **systemtrace** : システムのトレース ファイルをアップロードします。
- **traplog** : システムのトラップ ログをアップロードします。

- **watchdog-crash-file** : クラッシュ後にソフトウェア ウォッチドッグによってリポートが行われたときに生成されたコンソール ダンプをアップロードします。ソフトウェア ウォッチドッグ モジュールによって、内部ソフトウェアの整合性が定期的にチェックされるので、システムが不整合または非動作の状態が長時間続くことはなくなります。

ステップ 3 ファイルへのパスを指定するには、次のコマンドを入力します。

- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

ステップ 4 FTP サーバを使用している場合は、次のコマンドも入力します。

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

(注) *port* パラメータのデフォルト値は 21 です。

ステップ 5 更新された設定を表示するには、次のコマンドを入力します。

transfer upload start

ステップ 6 現在の設定を確認してソフトウェアアップロードを開始するよう求めるプロンプトが表示されたら、**y** と入力します。

コントローラからのコア ダンプのアップロード

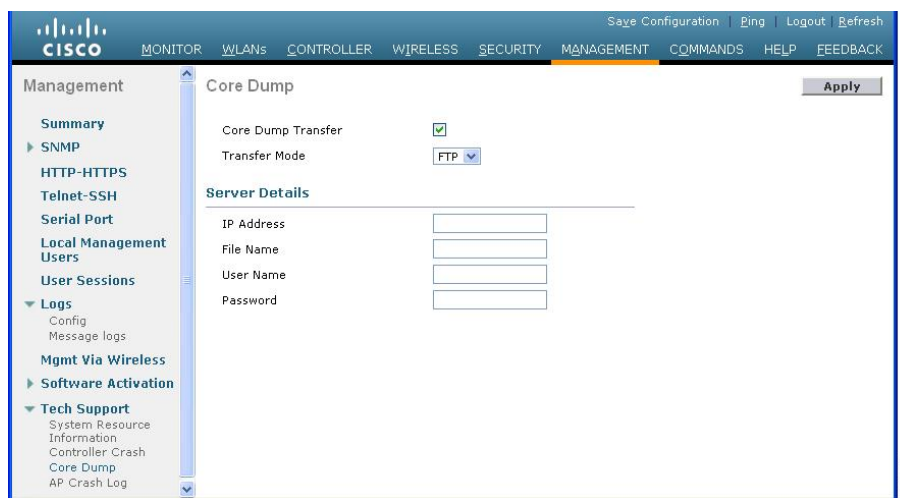
コントローラからのコア ダンプのアップロードについて

コントローラクラッシュのトラブルシューティングに役立てるために、クラッシュ後に自動的にコア ダンプ ファイルを FTP サーバにアップロードするようコントローラを設定することができます。コア ダンプ ファイルを FTP または TFTP サーバに直接アップロードすることはできませんが、クラッシュ ファイルを FTP または TFTP サーバにアップロードすることはできます。コントローラがクラッシュしたときは、コア ダンプ ファイルがフラッシュ メモリに保存されます。

コア ダンプを自動的に FTP サーバにアップロードするようにコントローラを設定する (GUI)

ステップ 1 [Management] > [Tech Support] > [Core Dump] の順に選択して [Core Dump] ページを開きます。

図 29 : [Core Dump] ページ



ステップ 2 コントローラがクラッシュ後にコア ダンプ ファイルを生成できるようにするには、[Core Dump Transfer] チェックボックスをオンにします。

ステップ 3 コア ダンプ ファイルのアップロード先のサーバのタイプを指定するには、[Transfer Mode] ドロップダウンリストから [FTP] を選択します。

ステップ 4 [IP Address] テキスト ボックスに、FTP サーバの IP アドレスを入力します。
(注) コントローラからその FTP サーバに到達可能でなければなりません。

ステップ 5 [File Name] テキスト ボックスに、コア ダンプ ファイルを識別するための名前を入力します。

ステップ 6 [User Name] テキスト ボックスに、FTP ログインのユーザ名を入力します。

ステップ 7 [Password] テキスト ボックスに、FTP ログインのパスワードを入力します。

ステップ 8 [Apply] をクリックして、変更を確定します。

ステップ 9 [Save Configuration] をクリックして、変更を保存します。

コア ダンプを自動的に FTP サーバにアップロードするようにコントローラを設定する (CLI)

ステップ 1 コントローラ クラッシュ後のコア ダンプ ファイルの自動生成を有効または無効にするには、次のコマンドを入力します。

```
config coredump {enable | disable}
```

ステップ 2 コア ダンプ ファイルのアップロード先の FTP サーバを指定するには、次のコマンドを入力します。

```
config coredump ftp server_ip_address filename
```

値は次のとおりです。

- *server_ip_address* は、コントローラがコア ダンプ ファイルを送信する FTP サーバの IP アドレスです。

(注) コントローラからその FTP サーバに到達可能でなければなりません。

- *filename* は、コントローラのコア ダンプ ファイルを識別するための名前です。

ステップ 3 FTP ログインのユーザ名とパスワードを指定するには、次のコマンドを入力します。

```
config coredump username ftp_username password ftp_password
```

ステップ 4 変更を保存するには、次のコマンドを入力します。

```
save config
```

ステップ 5 コントローラのコア ダンプ ファイルの概要を表示するには、次のコマンドを入力します。

例：

以下に類似した情報が表示されます。

```
show coredump summary
```

以下に類似した情報が表示されます。

```
Core Dump is enabled
```

```
FTP Server IP..... 10.10.10.17
FTP Filename..... file1
FTP Username..... ftpuser
FTP Password..... *****
```

コントローラからサーバへのコア ダンプのアップロード (CLI)

ステップ 1 フラッシュ メモリ内のコア ダンプ ファイルの情報を表示するには、次のコマンドを入力します。
show coredump summary

以下に類似した情報が表示されます。

```
Core Dump is disabled

Core Dump file is saved on flash

Sw Version..... 6.0.83.0
Time Stamp..... Wed Feb  4 13:23:11 2009
File Size..... 9081788
File Name Suffix..... filename.gz
```

ステップ 2 ファイルをコントローラからサーバに転送するには、次のコマンドを入力します。

- **transfer upload mode {tftp | ftp | sftp}**
- **transfer upload datatype coredump**
- **transfer upload serverip *server_ip_address***
- **transfer upload path *server_path_to_file***
- **transfer upload filename *filename***

(注) ファイルがアップロードされた後は、末尾に **.gz** という接尾辞が付加されます。必要に応じて、同じコア ダンプ ファイルを何度も、名前を変えて別のサーバにアップロードすることもできます。

ステップ 3 FTP サーバを使用している場合は、次のコマンドも入力します。

- **transfer upload username *username***
transfer upload password *password*
- **transfer upload port *port***

(注) *port* パラメータのデフォルト値は 21 です。

ステップ 4 更新された設定を表示するには、次のコマンドを入力します。
transfer upload start

ステップ 5 現在の設定を確認してソフトウェアアップロードを開始するよう求めるプロンプトが表示されたら、**y** と入力します。

パケットキャプチャファイルのアップロード

パケットキャプチャファイルのアップロードについて

Cisco 5500 シリーズ コントローラ のデータ プレーン がクラッシュすると、コントローラ が受信した最後の 50 パケットがフラッシュ メモリに格納されます。この情報は、クラッシュのトラブルシューティングに役立ちます。

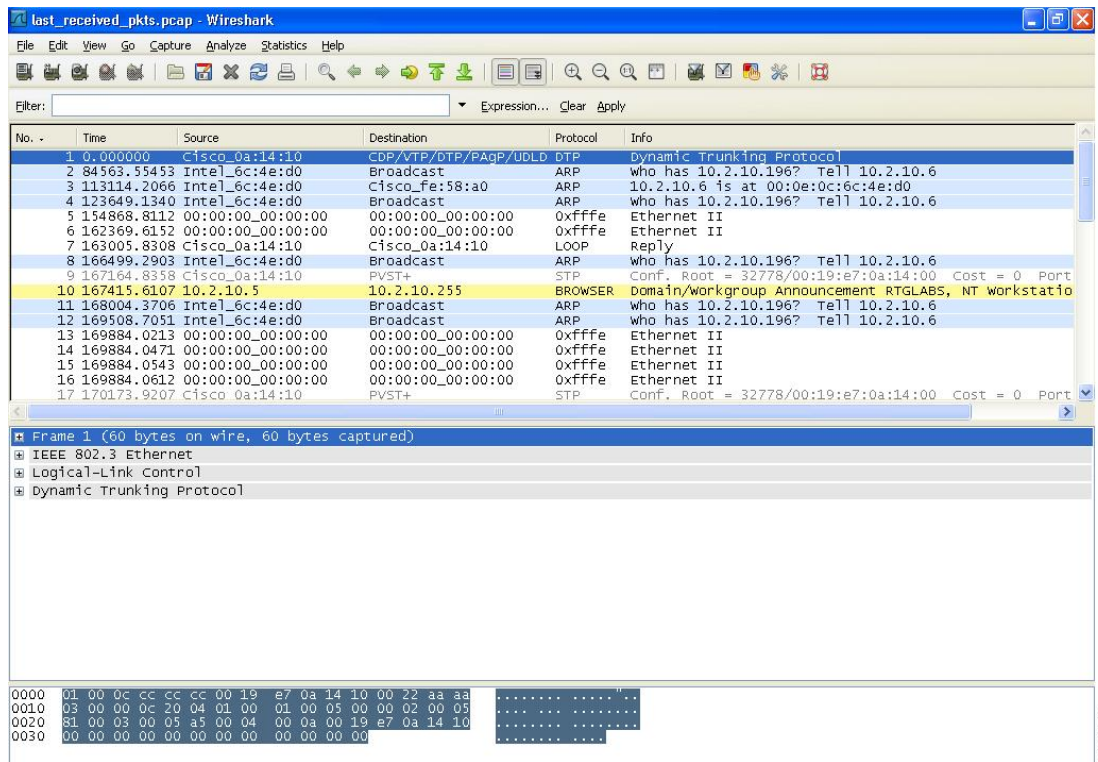
クラッシュが発生すると、新しいパケットキャプチャファイル (*.pcap ファイル) が作成され、次のようなメッセージがコントローラ クラッシュ ファイルに出力されます。

```
Last 5 packets processed at each core are stored in
"last_received_pkts.pcap" captured file.
- Frame 36,38,43,47,49, processed at core #0.
- Frame 14,27,30,42,45, processed at core #1.
- Frame 15,18,20,32,48, processed at core #2.
- Frame 11,29,34,37,46, processed at core #3.
- Frame 7,8,12,31,35, processed at core #4.
- Frame 21,25,39,41,50, processed at core #5.
- Frame 16,17,19,22,33, processed at core #6.
- Frame 6,10,13,23,26, processed at core #7.
- Frame 9,24,28,40,44, processed at core #8.
- Frame 1,2,3,4,5, processed at core #9.
```

コントローラ GUI または CLI を使用して、このパケットキャプチャファイルをコントローラからアップロードすることができます。このファイルの内容を表示して分析するには、Wireshark などの標準的なパケットキャプチャ ツールを使用します。

次の図に、Wireshark でのパケット キャプチャの出力例を示します。

図 30: Wireshark でのパケット キャプチャ ファイルのサンプル出力



パケットキャプチャファイルのアップロードに関する制約事項

- パケットキャプチャファイルを生成するのは Cisco 5500 シリーズ コントローラだけです。この機能は、他のコントローラプラットフォームでは利用できません。
- ファイルのアップロードに TFTP または FTP サーバを使用できることを確認してください。TFTP または FTP サーバをセットアップする場合は、次のガイドラインに従ってください。
 - サービスポート経由でアップロードする場合は、TFTP/FTP サーバがサービスポートと同じサブネット上になければなりません。サービスポートはルーティングできないからです。同じサブネット上にない場合は、コントローラ上に静的ルートを作成する必要があります。
 - ディストリビューション システム ネットワーク ポートを経由してアップロードする場合は、TFTP/FTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。ディストリビューション システム ポートはルーティング可能であるためです。
 - Prime Infrastructure 内蔵 TFTP または FTP サーバとサードパーティの TFTP または FTP サーバは同じ通信ポートを使用する必要があるため、サードパーティの TFTP または FTP サーバは Cisco Prime Infrastructure と同じコンピュータ上で実行できません。

パケットキャプチャファイルのアップロード (GUI)

-
- ステップ 1** [Commands] > [Upload File] の順に選択して、[Upload File from Controller] ページを開きます。
- ステップ 2** [File Type] ドロップダウン リストから、[Packet Capture] を選択します。
- ステップ 3** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 4** [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
- ステップ 5** [File Path] テキスト ボックスに、パケットキャプチャファイルのディレクトリパスを入力します。
- ステップ 6** [File Name] テキスト ボックスに、パケットキャプチャファイルの名前を入力します。このファイルには、.pcap という拡張子が付いています。
- ステップ 7** FTP サーバを使用している場合は、次の手順に従います。
- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、FTP サーバ上のアップロードが行われるポート番号を入力します。デフォルト値は 21 です。
- ステップ 8** [Upload] をクリックすると、パケットキャプチャファイルがコントローラからアップロードされます。アップロードのステータスを示すメッセージが表示されます。
- ステップ 9** Wireshark などの標準的なパケットキャプチャツールを使用してパケットキャプチャファイルを開くと、コントローラが受信した最後の 50 パケットを見ることができます。
-

パケットキャプチャファイルのアップロード (CLI)

- ステップ1 コントローラ CLI にログインします。
- ステップ2 **transfer upload mode** {tftp | ftp | sftp} コマンドを入力します。
- ステップ3 **transfer upload datatype packet-capture** コマンドを入力します。
- ステップ4 **transfer upload serverip** *server-ip-address* コマンドを入力します。
- ステップ5 **transfer upload path** *server-path-to-file* コマンドを入力します。
- ステップ6 **transfer upload filename** *last_received_pkts.pcap* コマンドを入力します。
- ステップ7 FTP サーバを使用している場合は、次のコマンドを入力します。
- **transfer upload username** *username*
 - **transfer upload password** *password*
 - **transfer upload port** *port*
- (注) *port* パラメータのデフォルト値は 21 です。
- ステップ8 **transfer upload start** コマンドを入力して更新後の設定を表示します。その後、現在の設定を確認するプロンプトが表示されたら y と答え、アップロードプロセスを開始します。このコマンドの出力例は、次のとおりです。
- ステップ9 Wireshark などの標準的なパケットキャプチャツールを使用してパケットキャプチャファイルを開くと、コントローラが受信した最後の 50 パケットを見ることができます。

メモリリークの監視

この項では、解決や再現が難しいメモリの問題をトラブルシューティングする手順を説明します。



注意 この項のコマンドはシステムに悪影響を及ぼす可能性があるため、Cisco Technical Assistance Center (TAC) の指示を受けた場合に限り実行する必要があります。

メモリリークの監視 (CLI)

- ステップ1 メモリエラーおよびメモリリークの監視を有効にするには、次のコマンドを入力します。
- config memory monitor errors** {enable | disable}

デフォルト値はディセーブルです。

(注) ここでの変更は、リブートすると破棄されます。コントローラのリブート後は、この機能のデフォルト設定が使用されます。

ステップ 2 メモリリークが発生したと考えられる場合は、次のコマンドを入力して、2つのメモリしきい値 (KB 単位) 間の自動リーク分析を実行するようにコントローラを設定します。

config memory monitor leaks low_thresh high_thresh

空きメモリが *low_thresh* しきい値を下回ると、システムがクラッシュしてクラッシュファイルが生成されます。このパラメータのデフォルト値は 10000 KB です。これより低い値には設定できません。

high_thresh しきい値は、現在の空きメモリの大きさ以上に設定してください。このようにすると、システムは自動リーク分析モードになります。空きメモリの大きさが、指定された *high_thresh* しきい値を下回ると、メモリ割り当てのトラッキングと解放のプロセスが開始します。その結果、**debug memory events enable** コマンドによってすべての割り当ておよび空きメモリが示され、**show memory monitor detail** コマンドによってメモリリークの疑いの検出が開始されます。このパラメータのデフォルト値は 30000 KB です。

ステップ 3 メモリの問題が見つかった場合にその概要を表示するには、次のコマンドを入力します。

show memory monitor

以下に類似した情報が表示されます。

```
Memory Leak Monitor Status:
low_threshold(10000), high_threshold(30000), current status(disabled)
```

```
-----

Memory Error Monitor Status:
Crash-on-error flag currently set to (disabled)
No memory error detected.
```

ステップ 4 メモリのリークまたは破損の詳細を表示するには、次のコマンドを入力します。

show memory monitor detail

以下に類似した情報が表示されます。

```
Memory error detected. Details:
-----
- Corruption detected at pmalloc entry address:          (0x179a7ec0)
- Corrupt entry:headerMagic(0xdeadf00d),trailer(0xabcd),poison(0xreadceef),
entrysize(128),bytes(100),thread(Unknown task name, task id = (332096592)),
file(pmalloc.c),line(1736),time(1027)

Previous 1K memory dump from error location.
-----
(179a7ac0): 00000000 00000000 00000000 ceef00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c alb7cee6 00000000 00000000
```

```
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7bc0): 00000002 00000002 00000010 00000001 00000002 00000000 0000001e 00000013
(179a7be0): 0000001a 00000089 00000000 00000000 000000d8 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
```

ステップ 5 メモリリークが発生した場合は、次のコマンドを入力してメモリ割り当て中のエラーまたはイベントのデバッグを有効にします。

```
debug memory {errors | events} {enable | disable}
```

CCXv5 クライアント デバイスのトラブルシューティング

CCXv5 クライアント デバイスのトラブルシューティングについて

コントローラと CCXv5 クライアントとの通信に関する問題のトラブルシューティングに使用できる機能には、診断チャンネル、クライアントレポート、およびローミング診断とリアルタイム診断の3つがあります。

CCXv5 クライアント デバイスの制約事項

診断チャンネル、クライアントレポート、クライアントローミング、およびリアルタイム診断の機能は、CCXv5 クライアントでのみサポートされます。CCX 以外のクライアントでの使用や、以前のバージョンの CCX を実行するクライアントでの使用はサポートされていません。

診断チャンネルの設定

クライアントの WLAN による通信で問題が生じる理由についてトラブルシューティングする診断チャンネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセスポイントをテストできます。診断チャンネルを有効にするには、コントローラの GUI や CLI を使用します。また、診断テストを実行するには、コントローラの CLI を使用します。

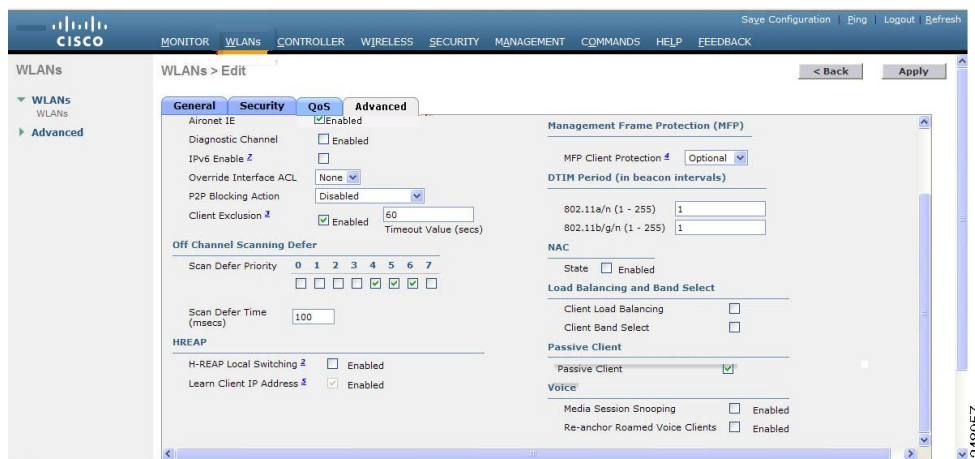


(注) 診断チャンネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされました

診断チャネルの設定 (GUI)

- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** 新しい WLAN を作成するか、既存の WLAN の ID 番号をクリックします。
(注) 診断テストを実行するための新しい WLAN を作成することを推奨します。
- ステップ 3** [WLANs > Edit] ページが表示されたら、[Advanced] タブを選択して [WLANs > Edit] ([Advanced]) ページを開きます。

図 31 : [WLANs > Edit] ([Advanced]) ページ



- ステップ 4** この WLAN 上で診断チャネルでのトラブルシューティングを有効にする場合は、[Diagnostic Channel] チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします (デフォルト値)。
(注) クライアント上で診断テストを開始するには、CLI を使用します。
- ステップ 5** [Apply] をクリックして、変更を確定します。
- ステップ 6** [Save Configuration] をクリックして、変更を保存します。

診断チャネルの設定 (CLI)

- ステップ 1** 特定の WLAN 上で診断チャネルでのトラブルシューティングを有効にするには、次のコマンドを入力します。
- ```
config wlan diag-channel {enable | disable} wlan_id
```

**ステップ 2** 変更されたかどうかを確認するには、次のコマンドを入力します。

**show wlan wlan\_id**

以下に類似した情報が表示されます。

```

WLAN Identifier..... 1
Profile Name..... employee1
Network Name (SSID)..... employee
Status..... Disabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Interface..... virtual
WLAN ACL..... unconfigured
DHCP Server..... Default
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Enabled
...

```

**ステップ 3** DHCP テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx dhcp-test client\_mac\_address**

(注) このテストでは、クライアントは診断チャンネルを使用する必要はありません。

**ステップ 4** デフォルトゲートウェイの ping テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx default-gw-ping client\_mac\_address**

(注) このテストでは、クライアントは診断チャンネルを使用する必要はありません。

**ステップ 5** DNS サーバの IP アドレスの ping テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx dns-ping client\_mac\_address**

(注) このテストでは、クライアントは診断チャンネルを使用する必要はありません。

**ステップ 6** DNS 名前解決テストを特定のホスト名に対して実行する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx dns-resolve client\_mac\_address host\_name**

(注) このテストでは、クライアントは診断チャンネルを使用する必要はありません。

**ステップ 7** アソシエーションテストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx test-association** *client\_mac\_address ssid bssid* {802.11a | 802.11b | 802.11g} *channel*

**ステップ 8** 802.1X テストを実行する要求をクライアントに送信するには、次のコマンドを入力します。  
**config client ccx test-dot1x** *client\_mac\_address profile\_id bssid* {802.11a | 802.11b | 802.11g} *channel*

**ステップ 9** プロファイルのリダイレクトテストを実行する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx test-profile** *client\_mac\_address profile\_id*

*profile\_id* には、必ずクライアントレポートが有効なクライアントプロファイルのプロファイルIDを指定します。

(注) ユーザは親の WLAN へリダイレクトされます。他のプロファイルへはリダイレクトされません。表示されるプロファイルは、ユーザの親のプロファイルのみとなります。ただし、親 WLAN のプロファイルには、診断する子 WLAN を 1 つ持つことができます。

**ステップ 10** テストを中断またはクリアする必要がある場合は、次のコマンドを使用します。

- 現在のテストを中断する要求をクライアントに送信するには、次のコマンドを入力します。

**config client ccx test-abort** *client\_mac\_address*

保留にできるテストは一度に 1 つだけのため、このコマンドは現在保留中のテストを中断します。

- コントローラ上のテスト結果をクリアするには、次のコマンドを入力します。

**config client ccx clear-results** *client\_mac\_address*

**ステップ 11** クライアントにメッセージを送信するには、次のコマンドを入力します。

例：

**config client ccx send-message** *client\_mac\_address message\_id*

*message\_id* は、次のいずれかです。

- 1 = SSID が無効です。
- 2 = ネットワーク設定が無効です。
- 3 = WLAN の信頼性に矛盾があります。
- 4 = ユーザの資格情報が正しくありません。
- 5 = サポートに問い合わせてください。
- 6 = 問題は解決されました。
- 7 = 問題は解決されていません。
- 8 = 後でもう一度試してください。
- 9 = 示された問題を修正してください。
- 10 = ネットワークによってトラブルシューティングが拒否されました。
- 11 = クライアントレポートを取得しています。
- 12 = クライアントログを取得しています。

- 13 = 取得が完了しました。
- 14 = アソシエーション テストを開始しています。
- 15 = DHCP テストを開始しています。
- 16 = ネットワーク接続テストを開始しています。
- 17 = DNS ping テストを開始しています。
- 18 = 名前解決テストを開始しています。
- 19 = 802.1X 認証テストを開始しています。
- 20 = クライアントを特定のプロファイルへリダイレクトしています。
- 21 = テストが完了しました。
- 22 = テストに合格しました。
- 23 = テストに合格しませんでした。
- 24 = 診断チャネル動作をキャンセルするか WLAN プロファイルを選択して通常の動作を再開します。
- 25 = クライアントによってログの取得が拒否されました。
- 26 = クライアントによってクライアント レポートの取得が拒否されました。
- 27 = クライアントによってテスト要求が拒否されました。
- 28 = ネットワーク (IP) 設定が無効です。
- 29 = ネットワークに関する既知の機能停止または問題があります。
- 30 = 定期的なメンテナンスの時期です。
- 31 = WLAN のセキュリティ方式が正しくありません。
- 32 = WLAN の暗号化方式が正しくありません。
- 33 = WLAN の認証方式が正しくありません。

**ステップ 12** 最新のテストのステータスを確認するには、次のコマンドを入力します。

```
show client ccx last-test-status client_mac_address
```

デフォルト ゲートウェイの ping テストに対しては、次のような情報が表示されます。

```
Test Type..... Gateway Ping Test
Test Status..... Pending/Success/Timeout

Dialog Token..... 15
Timeout..... 15000 ms
Request Time..... 1329 seconds since system boot
```

**ステップ 13** 最新のテスト応答のステータスを確認するには、次のコマンドを入力します。

```
show client ccx last-response-status client_mac_address
```

802.1X 認証テストに対しては、次のような情報が表示されます。

```
Test Status..... Success
```



```

Response Dialog Token..... 87
Response Status..... Successful
Response Test Type..... 802.1x Authentication Test
Response Time..... 3476 seconds since system boot

```

**ステップ 14** 最新の合格診断テストの結果を確認するには、次のコマンドを入力します。

```
show client ccx results client_mac_address
```

802.1X 認証テストに対しては、次のような情報が表示されます。

```

dot1x Complete..... Success
EAP Method..... *1,Host OS Login Credentials
dot1x Status..... 255

```

**ステップ 15** 前回のテストでクライアントが取得した関連データ フレームを確認するには、次のコマンドを入力します。

```
show client ccx frame-data client_mac_address
```

以下に類似した情報が表示されます。

LOG Frames:

```

Frame Number:..... 1
Last Frame Number:..... 1120
Direction:..... 1
Timestamp:..... 0d 00h 50m 39s 863954us
Frame Length:..... 197
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff ff 00 12 44 bd bd b0D...
00000010: 00 12 44 bd bd b0 f0 af 43 70 00 f2 82 01 00 00 ..D....Cp.....
00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H`
00000030: 6c 05 04 01 02 00 00 85 1e 00 00 89 00 0f 00 ff l.....
00000040: 03 19 00 41 50 32 33 2d 31 30 00 00 00 00 00 00 ...AP23-10.....
00000050: 00 00 00 00 00 00 26 96 06 00 40 96 00 ff ff dd&...@.....
00000060: 18 00 50 f2 01 01 00 00 50 f2 05 01 00 00 50 f2 ..P....P....P.
00000070: 05 01 00 00 40 96 00 28 00 dd 06 00 40 96 01 01@..(....@...

00000080: 00 dd 05 00 40 96 03 04 dd 16 00 40 96 04 00 02 ...@.....@....
00000090: 07 a4 00 00 23 a4 00 00 42 43 00 00 62 32 00 00 ...#...BC..b2..
000000a0: dd 05 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 82 ...@.....P.....
000000b0: 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f!'...BC^.b2/

```

LOG Frames:

```

Frame Number:..... 2
Last Frame Number:..... 1120
Direction:..... 1
Timestamp:..... 0d 00h 50m 39s 878289us
Frame Length:..... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff ff 00 0d ed c3 a0 22
00000010: 00 0d ed c3 a0 22 00 bd 4d 50 a5 f7 78 08 00 00".MP..x...
00000020: 64 00 01 00 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H`
00000030: 6c 05 04 01 02 00 00 85 1e 00 00 84 00 0f 00 ff l.....
00000040: 03 19 00 72 6f 67 75 65 2d 74 65 73 74 31 00 00 ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96 06 00 40 96 00 10 00 dd#...@.....
00000060: 06 00 40 96 01 01 00 dd 05 00 40 96 03 04 dd 05 ..@.....@.....
00000070: 00 40 96 0b 01 dd 18 00 50 f2 02 01 01 81 00 03 .@.....P.....

00000080: a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f 00 d2 ...!'...BC^.b2/...
00000090: b4 ab 84

```

LOG Frames:

```

Frame Number:..... 3
Last Frame Number:..... 1120

```

```

Direction:..... 1
Timestamp:..... 0d 00h 50m 39s 881513us
Frame Length:..... 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff ff ff 00 12 44 bd 80 30D..0
00000010: 00 12 44 bd 80 30 60 f7 46 c0 8b 4b d1 05 00 00 ..D..0`.F..K...
00000020: 64 00 11 08 00 01 00 01 08 8c 12 98 24 b0 48 60 d.....$.H`
00000030: 6c 05 04 00 02 00 00 85 1e 00 00 89 00 0f 00 ff l.....
00000040: 03 19 00 41 50 34 30 2d 31 37 00 00 00 00 00 00 ...AP40-17.....
00000050: 00 00 00 00 00 00 26 dd 18 00 50 f2 01 01 00 00&...P.....
00000060: 50 f2 05 01 00 00 50 f2 05 01 00 00 40 96 00 28 P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01 00 dd 05 00 40 96 03 04@.....@...

00000080: dd 16 00 40 96 04 00 05 07 a4 00 00 23 a4 00 00 ...@.....#...
00000090: 42 43 00 00 62 32 00 00 dd 05 00 40 96 0b 01 dd BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85 00 03 a4 00 00 27 a4 00 ..P.....'...
000000b0: 00 42 43 5e 00 62 32 2f 00 0b 9a 1d 6f ..BC^.b2/.....o
...

```

## クライアント レポートの設定

クライアントレポートプロトコルは、クライアント情報を交換するためにクライアントとアクセスポイントによって使用されます。クライアントレポートは、クライアントがアソシエートするときに自動で収集されます。クライアントのアソシエート後は、いつでもコントローラの GUI または CLI を使用してクライアントレポート要求を任意の CCXv5 クライアントに送信できます。クライアント レポートには次の 4 種類があります。

- **クライアント プロファイル**：クライアントの設定に関する情報を示します。
- **動作パラメータ**：クライアントの現在の動作モードの詳細を示します。
- **製造元情報**：使用されている無線 LAN クライアント アダプタに関するデータを示します。
- **クライアント機能**：クライアントの機能に関する情報を示します。

### クライアント レポートの設定 (GUI)

**ステップ 1** [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。

**ステップ 2** 目的のクライアントの MAC アドレスをクリックします。[Clients > Detail] ページが表示されます。

**ステップ 3** レポート要求をクライアントに送信するには、[Send CCXV5 Req] をクリックします。

(注) Cisco CB21AG の ACAU または CCXv5 ベンダーの同様のソフトウェアを使用して、信頼できるプロファイルを作成する必要があります。

- ステップ 4** クライアントのパラメータを表示するには、[Display] をクリックします。[Client Reporting] ページが表示されます。
- ステップ 5** 目的のクライアント プロファイルのリンクをクリックします。[Profile Details] ページには、SSID、省電力モード、無線チャネル、データ レート、802.11 セキュリティ設定などのクライアント プロファイルの詳細が表示されます。

## クライアント レポートの設定 (CLI)

- ステップ 1** クライアントプロファイルを送信する要求をクライアントに送信するには、次のコマンドを入力します。  
**config client ccx get-profiles client\_mac\_address**
- ステップ 2** 現在の動作パラメータを送信する要求をクライアントに送信するには、次のコマンドを入力します。  
**config client ccx get-operating-parameters client\_mac\_address**
- ステップ 3** 製造元の情報を送信する要求をクライアントに送信するには、次のコマンドを入力します。  
**config client ccx get-manufacturer-info client\_mac\_address**
- ステップ 4** 機能情報を送信する要求をクライアントに送信するには、次のコマンドを入力します。  
**config client ccx get-client-capability client\_mac\_address**
- ステップ 5** クライアント レポートの情報をクリアするには、次のコマンドを入力します。  
**config client ccx clear-reports client\_mac\_address**
- ステップ 6** クライアント プロファイルを表示するには、次のコマンドを入力します。  
**show client ccx profiles client\_mac\_address**
- ステップ 7** クライアントの動作パラメータを表示するには、次のコマンドを入力します。  
**show client ccx operating-parameters client\_mac\_address**
- ステップ 8** クライアントの製造元情報を表示するには、次のコマンドを入力します。  
**show client ccx manufacturer-info client\_mac\_address**
- ステップ 9** クライアントの機能情報を表示するには、次のコマンドを入力します。  
**show client ccx client-capability client\_mac\_address**

(注) このコマンドはクライアントで使用可能な機能を表示します。機能の現在の設定ではありません。

## ローミング診断とリアルタイム診断の設定

ローミングログとリアルタイムログ、および統計を使用して、システムの問題を解決できます。イベントログにより、クライアント デバイスの動作を識別および追跡できるようになります。これは、WLAN 上に存在する可能性がある問題を診断する際に特に役立ちます。 イベント ログ

はイベントのログを示し、アクセスポイントへそれらをレポートします。イベントログには次の3つのカテゴリがあります。

- **Roaming ログ**：このログは、指定されたクライアントのローミングイベントの履歴を示します。クライアントは、ローミングの失敗や成功などの直近のローミングイベントを最低5つ以上保持します。
- **Robust Security Network Association (RSNA; ロバストセキュリティネットワーク アソシエーション) ログ**：このログは、指定されたクライアントの認証イベントの履歴を示します。クライアントは、失敗や成功などの直近の認証イベントを最低5つ以上保持します。
- **Syslog**：このログは、クライアントの内部システム情報を示します。たとえば、802.11 の動作、システムの動作などに関する問題を示します。

統計レポートは、クライアントの 802.1X とセキュリティの情報を示します。クライアントのアソシエート後は、いつでもコントローラの CLI を使用してイベントログおよび統計の要求を任意の CCXv5 クライアントに送信できます。

## ローミング診断とリアルタイム診断の設定 (CLI)

**ステップ 1** ログ要求を送信するには、次のコマンドを入力します。

```
config client ccx log-request log_type client_mac_address
```

*log\_type* は、roam、rsna、または syslog です。

**ステップ 2** ログ応答を表示するには、次のコマンドを入力します。

```
show client ccx log-response log_type client_mac_address
```

*log\_type* は、roam、rsna、または syslog です。

*log\_type* が roam であるログ応答に対しては、次のような情報が表示されます。

```
Tue Jun 26 18:28:48 2007 Roaming Response LogID=133: Status=Successful
 Event Timestamp=0d 00h 00m 13s 322396us
 Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3125 (ms)
 Transition Reason: Normal roam, poor link
 Transition Result: Success
Tue Jun 26 18:28:48 2007 Roaming Response LogID=133: Status=Successful
 Event Timestamp=0d 00h 00m 16s 599006us
 Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3235 (ms)
 Transition Reason: Normal roam, poor link
 Transition Result: Success
 Event Timestamp=0d 00h 00m 19s 882921us
 Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3234 (ms)
 Transition Reason: Normal roam, poor link
 Transition Result: Success
Tue Jun 26 18:28:48 2007 Roaming Response LogID=133: Status=Successful
```

```

Event Timestamp=0d 00h 00m 08s 815477us
Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:d2, Transition
Time=3281 (ms)

Transition Reason: First association to WLAN
Transition Result: Success
Event Timestamp=0d 00h 00m 26s 637084us
Source BSSID=00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:c2, Transition
Time=3313 (ms)

```

*log\_type* が *rsna* であるログ応答に対しては、次のような情報が表示されます。

```

Tue Jun 26 18:24:09 2007 RSNA Response LogID=132: Status=Successful
Event Timestamp=0d 00h 00m 00s 246578us
Target BSSID=00:14:1b:58:86:cd
RSNA Version=1
Group Cipher Suite=00-0f-ac-02
Pairwise Cipher Suite Count = 1
 Pairwise Cipher Suite 0 = 00-0f-ac-04
AKM Suite Count = 1
 AKM Suite 0 = 00-0f-ac-01
RSN Capability = 0x0
RSNA Result: Success
Tue Jun 26 18:24:09 2007 RSNA Response LogID=132: Status=Successful
Event Timestamp=0d 00h 00m 00s 246625us
Target BSSID=00:14:1b:58:86:cd
RSNA Version=1
Group Cipher Suite=00-0f-ac-02
Pairwise Cipher Suite Count = 1
 Pairwise Cipher Suite 0 = 00-0f-ac-04
AKM Suite Count = 1
 AKM Suite 0 = 00-0f-ac-01
RSN Capability = 0x0
RSNA Result: Success
Tue Jun 26 18:24:09 2007 RSNA Response LogID=132: Status=Successful
Event Timestamp=0d 00h 00m 01s 624375us
Target BSSID=00:14:1b:58:86:cd
RSNA Version=1
Group Cipher Suite=00-0f-ac-02
Pairwise Cipher Suite Count = 1
 Pairwise Cipher Suite 0 = 00-0f-ac-04
AKM Suite Count = 1
 AKM Suite 0 = 00-0f-ac-01
RSN Capability = 0x0
RSNA Result: Success

```

*log\_type* が *syslog* であるログ応答に対しては、次のような情報が表示されます。

```

Tue Jun 26 18:07:48 2007 SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 278987us
Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory elements
missing in the OID response'
Event Timestamp=0d 00h 19m 42s 278990us
Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory elements

```

```

missing in the OID response'
Tue Jun 26 18:07:48 2007 SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 278993us
Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory elements
missing in the OID response'
Event Timestamp=0d 00h 19m 42s 278996us
Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory elements
missing in the OID response'
Tue Jun 26 18:07:48 2007 SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 279000us
Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory elements
missing in the OID response'
Event Timestamp=0d 00h 19m 42s 279003us
Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory elements
missing in the OID response'
Tue Jun 26 18:07:48 2007 SysLog Response LogID=131: Status=Successful
Event Timestamp=0d 00h 19m 42s 279009us
Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory elements
missing in the OID response'
Event Timestamp=0d 00h 19m 42s 279012us
Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory elements
missing in the OID response'

```

**ステップ 3** 統計の要求を送信するには、次のコマンドを入力します。

```
config client ccx stats-request measurement_duration stats_name client_mac_address
```

*stats\_name* は、dot11 または security です。

**ステップ 4** 統計応答を表示するには、次のコマンドを入力します。

```
show client ccx stats-report client_mac_address
```

以下に類似した情報が表示されます。

```

Measurement duration = 1

dot11TransmittedFragmentCount = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount = 3
dot11RetryCount = 4
dot11MultipleRetryCount = 5
dot11FrameDuplicateCount = 6
dot11RTSSuccessCount = 7
dot11RTSFailureCount = 8
dot11ACKFailureCount = 9
dot11ReceivedFragmentCount = 10
dot11MulticastReceivedFrameCount = 11
dot11FCSErrorCount = 12
dot11TransmittedFrameCount = 13

```

# デバッグ ファシリティの使用法

## デバッグ ファシリティの使用法について

デバッグ ファシリティにより、コントローラの CPU とやり取りするすべてのパケットを表示できるようになります。受信したパケット、送信したパケット、またはその両方に対して有効にできます。デフォルトでは、デバッグ ファシリティによって受信されたすべてのパケットが表示されます。それらを表示する前に、アクセスコントロールリスト (ACL) を定義してパケットをフィルタリングすることもできます。ACL に渡されないパケットは、表示されずに破棄されます。

各 ACL には、動作 (許可、拒否、無効化)、およびパケットの適合に使用する 1 つまたは複数のフィールドが含まれます。デバッグ ファシリティでは、次のレベルおよび値で動作する ACL が提供されます。

- ドライバ ACL
  - NPU のカプセル化の種類
  - ポート
- Ethernet header ACL
  - 宛先アドレス
  - 送信元アドレス
  - イーサネットの種類
  - VLAN ID
- IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート (該当する場合)
  - 宛先ポート (該当する場合)
- EoIP payload Ethernet header ACL
  - 宛先アドレス
  - 送信元アドレス
  - イーサネットの種類
  - VLAN ID
- EoIP payload IP header ACL

- 送信元アドレス
- 宛先アドレス
- プロトコル
- 送信元ポート (該当する場合)
- 宛先ポート (該当する場合)
- CAPWAP payload 802.11 header ACL
  - 宛先アドレス
  - 送信元アドレス
  - BSSID
  - SNAP ヘッダーの種類
- CAPWAP payload IP header ACL
  - 送信元アドレス
  - 宛先アドレス
  - プロトコル
  - 送信元ポート (該当する場合)
  - 宛先ポート (該当する場合)

各レベルにおいて、複数の ACL を定義できます。パケットと一致する最初の ACL が、選択された ACL となります。

## デバッグ ファシリティの設定 (CLI)

**ステップ 1** デバッグ ファシリティを有効にするには、次のコマンドを入力します。

• **debug packet logging enable {rx | tx | all} packet\_count display\_size**

値は次のとおりです。

- **rx** の場合は受信したすべてのパケット、**tx** の場合は送信したすべてのパケット、**all** の場合は受信と送信の両方のパケットが表示されます。
- **packet\_count** は、ログするパケットの最大数です。1 ~ 65535 の値をパケット数として入力できます。また、デフォルト値は 25 パケットです。
- **display\_size** は、パケットを印刷する際の表示バイト数です。デフォルトでは、全パケットが表示されます。



(注) デバッグ ファシリティを無効にするには、コマンド **debug packet logging disable** を入力します。

• **debug packet logging acl driver rule\_index action npu\_encap port**

値は次のとおりです。

- *rule\_index* の値は、1 ～ 6（両端の値を含む）です。
- *action* は、permit、deny、または disable です。
- *npu\_encap* では、パケットのフィルタリング方法を定める、NPU のカプセル化の種類を指定します。指定可能な値には、dhcp、dot11-mgmt、dot11-probe、dot1x、eosping、iapp、ip、lwapp、multicast、orphan-from-sta、orphan-to-sta、rbcpl、wired-guest などがあります。
- *port* は、パケットの送受信のための物理ポートです。

• パケットをログする ACL を設定するには、次のコマンドを使用します。

**debug packet logging acl eth rule\_index action dst src type vlan**

値は次のとおりです。

- *rule\_index* の値は、1 ～ 6（両端の値を含む）です。
- *action* は、permit、deny、または disable です。
- *dst* は、宛先の MAC アドレスです。
- *src* は、送信元の MAC アドレスです。
- *type* は、2 バイトのタイプコード（IP の場合は 0x800、ARP の場合は 0x806 など）です。このパラメータには、「ip」（0x800 の代わり）や「arp」（0x806 の代わり）などの一般的な文字列値も使用できます。
- *vlan* は、2 バイトの VLAN ID です。

• **debug packet logging acl ip rule\_index action src dst proto src\_port dst\_port**

値は次のとおりです。

- *proto* は、数値、または getprotobyname() で認識される任意の文字列です。サポートされる文字列は、ip、icmp、igmp、ggp、ipencap、st、tcp、egp、pup、udp、hmp、xns-idp、rdp、iso-tp4、xtp、ddp、idpr-cmtp、rspf、vmtp、ospf、ipip、および encap です。
- *src\_port* は、2 バイトの UDP/TCP 送信元ポート（telnet、23 など）または「any」です。コントローラには、数値、または getservbyname() によって認識される任意の文字列を指定できます。サポートされる文字列は、tcpmux、echo、discard、systat、daytime、netstat、qotd、msp、chargen、ftp-data、ftp、fsp、ssh、telnet、smtp、time、rtp、nameserver、whois、re-mail-ck、domain、mtp、bootps、bootpc、tftp、gopher、rje、finger、www、link、kerberos、supdup、hostnames、iso-tsap、csnet-ns、3com-tsmux、rtelnet、pop-2、pop-3、sunrpc、auth、sftp、uucp-path、nntp、ntp、netbios-ns、netbios-dgm、netbios-ssn、imap2、snmp、snmp-trap、cmip-man、cmip-agent、xdmcp、

nextstep、bgp、prospero、irc、smux、at-rtmp、at-nbp、at-echo、at-zis、qmtmp、z3950、ipx、imap3、ulistserv、https、snpp、saft、npmp-local、npmp-gui、および hmmp-ind です。

° *dst\_port* は、2 バイトの UDP/TCP 宛先ポート (telnet、23 など) または「any」です。コントローラには、数値、または getservbyname() によって認識される任意の文字列を指定できます。サポートされる文字列は、*src\_port* と同じです。

- **debug packet logging acl eoip-eth rule\_index action dst src type vlan**
  - **debug packet logging acl eoip-ip rule\_index action src dst proto src\_port dst\_port**
  - **debug packet logging acl lwapp-dot11 rule\_index action dst src bssid snap\_type**
- 値は次のとおりです。

° *bssid* は、Basic Service Set Identifier (BSSID; 基本サービス セット ID) です。

° *snap\_type* は、イーサネットの種類です。

- **debug packet logging acl lwapp-ip rule\_index action src dst proto src\_port dst\_port**

(注) 設定済みの ACL をすべて削除するには、コマンド **debug packet logging acl clear-all** を入力します。

**ステップ 2** デバッグ出力の形式を設定するには、次のコマンドを入力します。

**debug packet logging format {hex2pcap | text2pcap}**

デバッグ ファシリティでは、hex2pcap と text2pcap という 2 つの出力形式がサポートされています。IOS によって使用される標準の形式では hex2pcap の使用がサポートされており、HTML フロントエンドを使用してデコードできます。text2pcap オプションは、一連のパケットを同一のコンソール ログ ファイルからデコードできるようにするために用意されています。

次の図に、hex2pcap の出力例を示します。

図 32 : Hex2pcap の出力例

```
tx len=118, encap=n/a, port=1
[0000]: 000c316E 7F80000B 854008c0 08004500 ..1n....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.....
[0030]: 00000000 00000000 00000000 00001C1D
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253 NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@.....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.....
[0030]: 00000000 00000000 00000000 00001C1D
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253 NOPQRS
```

212235

次の図に、text2pcap の出力例を示します。

図 33: Text2pcap の出力例

```

tx len=118, encap=n/a, port=1
0000 00 0c 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..in....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@.>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 l....Ye.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53 NOPQRS

rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..in....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 l....Ye.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53 NOPQRS

```

23/2343

**ステップ 3** パケットが表示されない理由を判断するには、次のコマンドを入力します。

**debug packet error {enable | disable}**

**ステップ 4** パケットのデバッグのステータスを表示するには、次のコマンドを入力します。

**show debug packet**

以下に類似した情報が表示されます。

```

Status..... disabled
Number of packets to display..... 25
Bytes/packet to display..... 0
Packet display format..... text2pcap

Driver ACL:
 [1]: disabled
 [2]: disabled
 [3]: disabled
 [4]: disabled
 [5]: disabled
 [6]: disabled
Ethernet ACL:
 [1]: disabled
 [2]: disabled
 [3]: disabled
 [4]: disabled
 [5]: disabled
 [6]: disabled
IP ACL:
 [1]: disabled
 [2]: disabled
 [3]: disabled
 [4]: disabled
 [5]: disabled
 [6]: disabled
EoIP-Ethernet ACL:
 [1]: disabled
 [2]: disabled
 [3]: disabled
 [4]: disabled

```

```
[5]: disabled
[6]: disabled
EoIP-IP ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
LWAPP-Dot11 ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled
LWAPP-IP ACL:
[1]: disabled
[2]: disabled
[3]: disabled
[4]: disabled
[5]: disabled
[6]: disabled?
```

## 無線スニファの設定

### 無線スニファについて

コントローラには、アクセスポイントの1つをネットワーク「スニファ」として設定する機能があります。スニファは、特定のチャンネル上のパケットをすべてキャプチャして、パケットアナライザソフトウェアを実行しているリモートマシンに転送します。これらのパケットには、タイムスタンプ、信号強度、パケットサイズなどの情報が含まれます。スニファを使用すると、ネットワークアクティビティを監視して記録し、問題を検出できます。

### 無線スニファの必須条件

無線スニファを実行するには、次のハードウェアとソフトウェアが必要です。

- 専用アクセスポイント：スニファとして設定されたアクセスポイントは、そのネットワーク上で無線アクセスサービスを同時に提供できません。カバレッジの中断を回避するには、既存のワイヤレスネットワークの一部ではないアクセスポイントを使用します。
- リモート監視デバイス：アナライザソフトウェアを実行できるコンピュータ。
- Windows XPまたはLinuxオペレーティングシステム：コントローラは、Windows XPとLinuxのいずれのマシンでもスニファをサポートしています。
- ソフトウェアおよび関連ファイル、プラグイン、またはアダプタ：アナライザソフトウェアによっては、有効にするために特殊なファイルが必要となる場合があります。

## 無線スニファの制約事項

- サポートされているサードパーティ製のネットワーク アナライザ ソフトウェア アプリケーションは、次のとおりです。
  - Wildpackets Omnipeek または Airoppeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- Wireshark の最新バージョンでは、Analyze モードでパケットをデコードできます。[decode as] を選択し、UDP5555 を AIROPEEK としてデコードするように切り替えます。
- アクセスポイントが Cisco 5500 シリーズコントローラに join されている場合、スニファモードでアクセスポイントを使用するには IP-MAC アドレス バインディングを無効にする必要があります。IP-MAC アドレスバインディングを無効にするには、コントローラ CLI で **config network ip-mac-binding disable** コマンドを入力します。
- アクセスポイントが Cisco 5500 シリーズコントローラに join されている場合、スニファモードでアクセスポイントを使用するには WLAN 1 を有効にする必要があります。WLAN 1 が無効の場合は、アクセスポイントはパケットを送信できません。

無線スニファの必須条件

## アクセスポイントのスニファの設定 (GUI)

- 
- ステップ 1** [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2** スニファとして設定するアクセスポイントの名前をクリックします。[All APs > Details for] ページが表示されます。
- ステップ 3** [AP Mode] ドロップダウンリストから [Sniffer] 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** アクセスポイントをリポートするプロンプトが表示されたら、[OK] をクリックします。
- ステップ 6** [Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して [/ac802.11a/n (または 802.11b/g/n) Radios] ページを開きます。
- ステップ 7** カーソルを目的のアクセスポイントの青いドロップダウン矢印の上に置いて [Configure] を選択します。[802.11a/n/ac (または 802.11b/g/n) Cisco APs > Configure] ページが表示されます。
- ステップ 8** [Sniff] チェックボックスをオンにして、このアクセスポイントのスニファを有効にします。オンにしなければ、スニファは無効になります。デフォルトではオフになっています。
- ステップ 9** ステップ 8 でスニファを有効にした場合は、次の手順に従ってください。
- a) [Channel] ドロップダウンリストから、アクセスポイントがパケットに対してスニファするチャンネルを選択します。

- b) [Server IP Address] テキスト ボックスに、Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスを入力します。

ステップ 10 [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

---

## アクセス ポイントのスニファの設定 (CLI)

---

ステップ 1 次のコマンドを入力して、アクセス ポイントをスニファとして設定します。

```
config ap mode sniffer Cisco_AP
```

*Cisco\_AP* はスニファとして設定されるアクセス ポイントです。

ステップ 2 アクセス ポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。アクセス ポイントはスニファ モードでリブートします。

ステップ 3 次のコマンドを入力して、アクセス ポイントでスニファを有効にします。

```
config ap sniff {802.11a | 802.11b} enable channel server_IP_address Cisco_AP
```

値は次のとおりです。

- *channel* はアクセス ポイントがパケットに対してスニファする無線チャンネルです。デフォルト値は 36 (802.11a/n/ac) と 1 (802.11b/g/n) です。
- *server\_IP\_address* は Omnippeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレスです。
- *Cisco\_AP* はスニファとして設定されるアクセス ポイントです。

(注) アクセス ポイントでスニファを無効にするには、**config ap sniff {802.11a | 802.11b} disable Cisco\_AP** コマンドを入力します。

ステップ 4 次のコマンドを入力して、変更を保存します。

```
save config
```

ステップ 5 次のコマンドを入力して、アクセス ポイントのスニファの設定を表示します。

```
show ap config {802.11a | 802.11b} Cisco_AP
```

---

## Telnet または SSH\_old を使用したアクセスポイントのトラブルシューティング

コントローラは、Telnet プロトコルおよび Secure Shell (SSH) プロトコルを使用した Lightweight アクセスポイントのトラブルシューティングをサポートしています。これらのプロトコルを使用すると、特にアクセスポイントがコントローラに接続できない場合に、デバッグを簡単に行うことができます。

- 潜在的な競合やネットワークセキュリティの脅威を避けるために、Telnet または SSH のセッションを有効にしている間は **config terminal**、**telnet**、**ssh**、**rsh**、**ping**、**traceroute**、**clear**、**clock**、**crypto**、**delete**、**fsck**、**lwapp**、**mkdir**、**radius**、**release**、**reload**、**rename**、**renew**、**rmdir**、**save**、**set**、**test**、**upgrade** のコマンドを使用できないようになっています。
- Telnet または SSH のセッション中に使用できる主なコマンドは、**debug**、**disable**、**enable**、**help**、**led**、**login**、**logout**、**more**、**no debug**、**show**、**systat**、**undebug**、**where** です。



(注) コントローラ上で Telnet または SSH のセッションを設定する手順については、「[Telnet および Secure Shell セッションの設定](#)」セクションを参照してください。

### Telnet または SSH を使用したアクセスポイントのトラブルシューティングについて

コントローラは、Telnet プロトコルおよび Secure Shell (SSH) プロトコルを使用した Lightweight アクセスポイントのトラブルシューティングをサポートしています。これらのプロトコルを使用すると、特にアクセスポイントがコントローラに接続できない場合に、デバッグを簡単に行うことができます。

- 潜在的な競合やネットワークセキュリティの脅威を避けるために、Telnet または SSH のセッションを有効にしている間は **config terminal**、**telnet**、**ssh**、**rsh**、**ping**、**traceroute**、**clear**、**clock**、**crypto**、**delete**、**fsck**、**lwapp**、**mkdir**、**radius**、**release**、**reload**、**rename**、**renew**、**rmdir**、**save**、**set**、**test**、**upgrade** のコマンドを使用できないようになっています。
- Telnet または SSH のセッション中に使用できる主なコマンドは、**debug**、**disable**、**enable**、**help**、**led**、**login**、**logout**、**more**、**no debug**、**show**、**systat**、**undebug**、**where** です。



(注) コントローラ上で Telnet または SSH のセッションを設定する手順については、「[Telnet および Secure Shell セッションの設定](#)」の項を参照してください。

Telnet または SSH を設定するには、ソフトウェアリリース 5.0 以降のリリースのコントローラ CLI を使用するか、ソフトウェアリリース 6.0 以降のリリースのコントローラ GUI を使用します。

## Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (GUI)

- 
- ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2 Telnet または SSH を有効にするアクセス ポイントの名前をクリックします。
- ステップ 3 [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。
- ステップ 4 [Telnet] チェックボックスをオンにして、このアクセス ポイント上の Telnet 接続を有効にします。デフォルトではオフになっています。
- ステップ 5 [SSH] チェックボックスをオンにして、このアクセス ポイント上の SSH 接続を有効にします。デフォルトではオフになっています。
- ステップ 6 [Apply] をクリックします。
- ステップ 7 [Save Configuration] をクリックします。
- 

## Telnet または SSH を使用したアクセス ポイントのトラブルシューティング (CLI)

- 
- ステップ 1 次のコマンドを入力して、アクセス ポイントで Telnet または SSH の接続を有効にします。  
**config ap {telnet | ssh} enable Cisco\_AP**  
 デフォルト値はディセーブルです。  
 (注) 次のコマンドを入力して、アクセス ポイントで Telnet または SSH の接続を無効にします。 **config ap {telnet | ssh} disable Cisco\_AP**
- ステップ 2 次のコマンドを入力して、変更を保存します。  
**save config**
- ステップ 3 次のコマンドを入力して、Telnet または SSH がアクセス ポイント上で有効かどうかを確認します。  
**show ap config general Cisco\_AP**  
 以下に類似した情報が表示されます。

```

Cisco AP Identifier..... 5
Cisco AP Name..... AP33
Country code..... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country..... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number 2
MAC Address..... 00:19:2f:11:16:7a
IP Address Configuration..... Static IP assigned
IP Address..... 10.22.8.133
IP NetMask..... 255.255.248.0
Gateway IP Addr..... 10.22.8.1

```



```

Domain.....
Name Server.....
Telnet State..... Enabled
Ssh State..... Enabled
...

```

## アクセス ポイント監視サービスのデバッグ

### アクセス ポイント監視サービスのデバッグについて

コントローラから Cisco 3300 シリーズ モビリティ サービス エンジン (MSE; Mobility Services Engine) にアクセスポイントステータス情報を送信するときに、アクセスポイント監視サービスが使用されます。

MSE は、サービス サブスクリプションおよびアクセス ポイント監視サービス要求を送信して、その時点でコントローラが認識しているすべてのアクセスポイントのステータスを取得します。アクセスポイントのステータスが変更されると、MSE に通知が送信されます。

### アクセス ポイント監視サービスの問題のデバッグ (CLI)

アクセス ポイント監視サービスの問題が発生した場合は、次のコマンドを入力します。

```
debug service ap-monitor {all | error | event | nmosp | packet} {enable | disable}
```

値は次のとおりです。

- **all** : すべてのアクセス ポイント ステータス メッセージのデバッグを行います。
- **error** : アクセス ポイント監視エラー イベントのデバッグを行います。
- **event** : アクセス ポイント監視イベントのデバッグを行います。
- **nmosp** : アクセス ポイント監視 NMSP イベントのデバッグを行います。
- **packet** : アクセス ポイント監視パケットのデバッグを行います。
- **enable** : debug service ap-monitor モードを有効にします。
- **disable** : debug service ap-monitor モードを無効にします。

# OfficeExtend アクセスポイントのトラブルシューティング

## OfficeExtend アクセスポイントのトラブルシューティングについて

この項では、OfficeExtend アクセスポイントの問題が発生した場合のトラブルシューティング情報を示します。

### OfficeExtend の LED の解釈

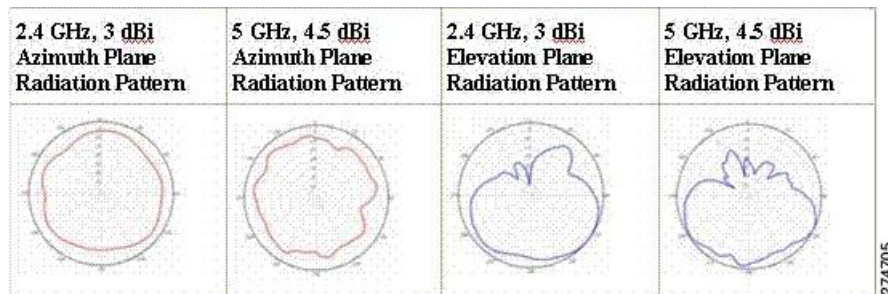
LED パターンは、OfficeExtend アクセスポイントが 1130 シリーズか 1140 シリーズかによって異なります。LED パターンの説明については、『Cisco OfficeExtend Access Point Quick Start Guide』を参照してください。このガイドには、次の URL からアクセスできます。

<http://www.cisco.com/en/US/products/hw/wireless/index.html>

### RF カバレッジが最適になるように OfficeExtend アクセスポイントを配置する

OfficeExtend アクセスポイントの位置を決めるときは、アクセスポイントの RF 信号がアクセスポイントの LED 側から円すい形に広がるように発信されることを考慮してください。アクセスポイントを取り付けるときは、背面の金属プレートの背後を空気が通るようにして、アクセスポイントの過熱を防いでください。

図 34 : OfficeExtend アクセスポイントの放射パターン



## 一般的な問題のトラブルシューティング

OfficeExtend アクセスポイントに関する問題のほとんどは、次のいずれかです。

- ネットワークまたはファイアウォールの問題が原因で、アクセスポイントがコントローラに join できない。

**解決方法：**「アクセスポイントの join 情報の表示」の項の指示に従って、OfficeExtend アクセスポイントの join 統計情報を表示します。または、アクセスポイントのパブリック IP アドレスを見つけて、パケットサイズを変えながら ping を社内から実行します。

- アクセスポイントが join しても何度も切断される。この動作が発生するのは一般に、ネットワークの問題があるときや、タイムアウト時間が短いためにネットワーク アドレス変換 (NAT) またはファイアウォールポートが閉じたときです。

**解決方法**：テレワーカーに LED の状態を確認してもらいます。

- NAT の問題が原因でクライアントがアソシエートできない。

**解決方法**：テレワーカーに速度テストと ping テストを実行してもらいます。サーバによっては、パケットのサイズが大きいと ping を実行しても応答が返されません。

- クライアントがデータを廃棄し続ける。この動作が発生するのは一般に、タイムアウト時間が短いためにホーム ルータがポートを閉じたときです。

**解決方法**：クライアントのトラブルシューティングを Cisco Prime Infrastructure で実行し、問題が OfficeExtend アクセスポイントとクライアントのどちらに関連するものかを判断します。

- アクセスポイントがエンタープライズ WLAN をブロードキャストしていない。

**解決方法**：テレワーカーにケーブル、電源、および LED の状態を確認してもらいます。それでも問題を特定できない場合は、テレワーカーに次のことを試してもらいます。

- PC をホーム ルータに直接接続して、<http://www.cisco.com/> などのインターネット Web サイトに接続できるかどうかを調べます。PC がインターネットに接続できない場合は、ルータまたはモデムを調べます。PC がインターネットに接続できる場合は、ホーム ルータの設定を調べます。アクセスポイントからインターネットへの到達をブロックするような、ファイアウォールまたは MAC に基づくフィルタが有効になっているかどうかを調べてください。
- ホーム ルータにログインして、アクセスポイントが IP アドレスを取得済みかどうか調べます。取得済みならば、アクセスポイントの LED は通常はオレンジ色で点滅します。

- アクセスポイントがコントローラに join できず、問題を特定できない。

**解決方法**：ホームルータに問題がある可能性があります。テレワーカーに、ルータのマニュアルを調べて次のことを試してもらいます。

- アクセスポイントの MAC アドレスに基づいて、アクセスポイントに固定 IP アドレスを割り当てます。
- アクセスポイントを非武装地帯 (DMZ) に置きます。DMZ とは、会社のプライベートネットワークと外部のパブリックネットワークとの間に中立地帯として挿入される、小さなネットワークです。DMZ を設置すると、会社のデータが格納されているサーバに外部のユーザが直接アクセスすることはできなくなります。
- それでも問題が解決されない場合は、会社の IT 部門に連絡して支援を受けてください。

- テレワーカーがアクセスポイント上で個人 SSID の設定を行っているときに問題が発生する。

**解決方法**：アクセスポイント GUI で [Clear Config] をクリックするか、clear ap config Cisco\_AP コマンドを入力することにより、アクセスポイントの設定をクリアして工場出荷時のデフォ

ルト設定に戻します。その後、OfficeExtend アクセス ポイントで個人 SSID を設定します。それでも問題が解決されない場合は、会社の IT 部門に連絡して支援を受けてください。

- ホーム ネットワークをリブートする必要がある。

**解決方法：**テレワーカーに次の手順を実行してもらいます。

すべてのデバイスがネットワークに接続されたままの状態、すべてのデバイスの電源を切ります。

ケーブルまたは DSL のモデムの電源を入れて、2 分間待機します。（LED の状態を確認してください）。

ホーム ルータの電源を入れて、2 分間待機します。（LED の状態を確認してください）。

アクセスポイントの電源を入れて、5 分間待機します。（LED の状態を確認してください）。

クライアントの電源を入れます。



## 第 II 部

# ポートとインターフェイスの設定

- [ポートとインターフェイスの概要, 345 ページ](#)
- [管理インターフェイスの設定, 353 ページ](#)
- [AP マネージャ インターフェイスの設定, 357 ページ](#)
- [仮想インターフェイスの設定, 363 ページ](#)
- [サービス ポート インターフェイスの設定, 367 ページ](#)
- [動的インターフェイスの設定, 369 ページ](#)
- [ポートの設定, 375 ページ](#)
- [リンク集約の設定, 377 ページ](#)
- [複数の AP マネージャ インターフェイスの設定, 383 ページ](#)
- [VLAN Select の設定, 387 ページ](#)
- [インターフェイス グループの設定, 393 ページ](#)
- [マルチキャストの最適化の設定, 397 ページ](#)
- [ハイアベイラビリティの設定, 399 ページ](#)





# 第 28 章

## ポートとインターフェイスの概要

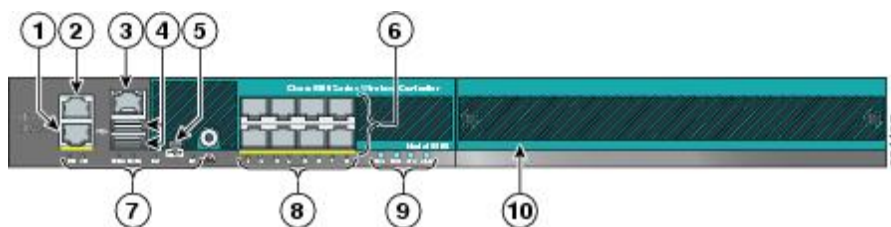
コントローラと無線ネットワーク ポートの接続方法を理解するカギとなるのは、ポート、インターフェイス、および WLAN の 3 つの概念です。

- [ポートについて](#), 345 ページ
- [ディストリビューションシステム ポートについて](#), 346 ページ
- [インターフェイスに関する情報](#), 348 ページ
- [動的 AP 管理について](#), 349 ページ
- [WLAN について](#), 350 ページ

### ポートについて

ポートは、コントローラプラットフォーム上に存在し、接続に使用される物理的実体です。コントローラには、ディストリビューションシステム ポートと、サービス ポートの 2 種類があります。

図 35: Cisco 5500 シリーズ Wireless LAN Controller のポート



|   |                  |   |                               |
|---|------------------|---|-------------------------------|
| 1 | 冗長ポート (RJ-45)    | 6 | SFP ディストリビューションシステム ポート 1 ~ 8 |
| 2 | サービス ポート (RJ-45) | 7 | 管理ポートの LED                    |

|   |                                                                                                            |    |                                                       |
|---|------------------------------------------------------------------------------------------------------------|----|-------------------------------------------------------|
| 3 | コンソールポート (RJ-45)                                                                                           | 8  | SFP ディストリビューションポートのリンク LED とアクティビティ LED               |
| 4 | USB ポート 0 および 1 (タイプ A)                                                                                    | 9  | 電源 (PS1 および PS2) LED、システム (SYS) LED、およびアラーム (ALM) LED |
| 5 | コンソールポート (ミニ USB タイプ B)<br>(注) 1つのコンソールポートのみを使用できます (RJ-45 または ミニ USB)。1つのコンソールポートに接続すると、もう一方のポートは無効になります。 | 10 | 拡張モジュール スロット                                          |

## ディストリビューションシステムポートについて

ディストリビューションシステムポートは近接スイッチとコントローラを接続し、これら2つのデバイス間のデータパスとして動作します。

### ディストリビューションシステムポートの設定に関する制限

- Cisco 5508 コントローラには、8個のギガビットイーサネットディストリビューションシステムポートが搭載されていて、これらのポートを通じて複数のアクセスポイントを管理できます。5508-12モデル、5508-25モデル、5508-50モデル、5508-100モデル、および5508-250モデルでは、合計12台、25台、50台、100台、または250台のアクセスポイントをコントローラに join できます。Cisco 5508 コントローラでは、1つのポートに対するアクセスポイント数の制限はありません。ただし、リンク集約 (LAG) を使用するか、ギガビットイーサネットポートで動的 AP マネージャ インターフェイスを設定して、ロードバランシングを自動的に行うことをお勧めします。100台を超えるアクセスポイントを Cisco 5500 シリーズ コントローラに接続する場合、複数のギガビットイーサネット インターフェイスをアップストリーム スイッチに接続するようにしてください。





(注) Cisco 5508 コントローラのギガビットイーサネットポートは、次の SX/LC/T Small Form-Factor Plug-in (SFP) モジュールに対応します。- 1000BASE-SX SFP モジュール。LC 物理コネクタを使用した 850nm (SX) 光ファイバリンクで 1000 Mbps の有線接続をネットワークに提供します。- 1000BASE-LX SFP モジュール。LC 物理コネクタを使用した 1300nm (LX/LH) 光ファイバリンクで 1000 Mbps の有線接続をネットワークに提供します。- 1000BASE-T SFP モジュール。RJ-45 物理コネクタを使用した銅線リンクで 1000 Mbps の有線接続をネットワークに提供します。

- GLC-SX-MM (1000BASE-SX コネクタ) を最適に機能させるには、自動ネゴシエーションモードにする必要があります。これは、LC 物理コネクタを使用するすべての SFP モジュールが正常に動作するために Cisco 5508 シリーズ コントローラで自動ネゴシエーションモードに設定される必要があるからです。ただし、Cisco ASR がファイバポートを使用して接続されている場合、Cisco ASR が正常に機能するには固定モードのコネクタが必要であるため、GLC-SX-MM は、Cisco ASR と Cisco 5508 間では機能しません。
- デフォルトでは、各ディストリビューションシステムポートは 802.1Q VLAN トランクポートです。ポートの VLAN トランク特性は設定できません。



(注) 一部のコントローラは、コントローラのすべてのディストリビューションシステムポートを1つの 802.3ad ポートチャネルにまとめるリンク集約 (LAG) をサポートしています。Cisco 5500 シリーズ コントローラは LAG をサポートします。LAG は Cisco WiSM2 内のコントローラで自動的に有効になります。

- アクセスモードの Cisco WLC 設定はサポートされていません。スイッチで Cisco WLC ポートを設定する場合、Cisco WLC をトランクモードに設定することをお勧めします。
- Cisco FLEX 7500 および 8500 シリーズ コントローラの場合
  - 5秒間のソーク期間後にポートが応答しない場合は、ポートがプライマリおよびアクティブポートであるすべてのインターフェイスが、バックアップが設定されていて正常に稼働している場合はバックアップポートにフェールオーバーされます。同様に、応答しないポートがバックアップポートの場合は、プライマリポートが正常に稼働している場合はすべてのインターフェイスがプライマリポートにフェールオーバーします。
  - 応答しないポートが復元されると、60秒のソーク期間が取られ、その後ポートが引き続き正常に動作していれば、プライマリポートだったこのポートにすべてのインターフェイスがフォールバックされます。このポートがバックアップポートであった場合は、変更は行われません。

## サービスポートについて

Cisco 5500 シリーズ コントローラは、10/100/1000 銅線イーサネット サービスポートも装備しています。このサービスポートは、サービスポートインターフェイスにより制御され、コントローラの帯域外管理と、ネットワーク障害時のシステム復旧とメンテナンスのために割り当てられています。また、これは、コントローラがブートモードのときにアクティブな唯一のポートです。このサービスポートは 802.1Q タグに対応していないので、近接スイッチ上のアクセスポートに接続する必要があります。サービスポートの使用は任意です。



(注) サービスポートには自動認識機能が備わっていません。サービスポートと通信するには、適切なストレートまたはクロスイーサネットケーブルを使用する必要があります。



注意 ネットワークのコントローラのサービスポートの同じ VLAN またはサブネットに有線クライアントを設定しないでください。サービスポートと同じサブネットまたは VLAN に有線クライアントを設定すると、コントローラの管理インターフェイスにアクセスできなくなります。

## インターフェイスに関する情報

インターフェイスはコントローラ上の論理実体です。インターフェイスには、IP アドレス、デフォルトゲートウェイ (IP サブネット用)、プライマリ物理ポート、セカンダリ物理ポート、VLAN 識別子、DHCP サーバなど、複数のパラメータが関連付けられています。

次の 5 種類のインターフェイスをコントローラで使用できます。これらのうち 4 種類は固定で、セットアップ時に設定されます。

- 管理インターフェイス (固定でセットアップ時に設定。必須)
- AP マネージャ インターフェイス (固定でセットアップ時に設定。必須)



(注) Cisco 5500 シリーズ コントローラでは AP マネージャ インターフェイスを設定する必要はありません。

- 仮想インターフェイス (固定でセットアップ時に設定。必須)
- サービスポート インターフェイス (固定でセットアップ時に設定。任意)
- 動的インターフェイス (ユーザ定義)



- (注) 通常、管理、AP マネージャ、仮想、およびサービスポートの各インターフェイスパラメータを定義するには、スタートアップ ウィザードを使用します。ただし、コントローラが実行されている場合は、GUI または CLI のどちらかを介して、インターフェイスパラメータを表示し、設定できます。

LAG が無効な場合、各インターフェイスは少なくとも1つのプライマリポートにマッピングされます。一部のインターフェイス（管理および動的）は、オプションのセカンダリ（または、バックアップ）ポートにマッピングできます。あるインターフェイスのプライマリポートに障害が発生すると、このインターフェイスは自動的にバックアップポートに移動します。また、複数のインターフェイスを1つのコントローラポートにマッピングできます。



- (注) 隔離されたインターフェイスは、[Controller > Interfaces] ページには表示されません。たとえば、6 個のインターフェイスがあり、これらの1つが隔離された場合、隔離されたインターフェイスは表示されず、他の5 個のインターフェイスの詳細が GUI に表示されます。GUI の右上隅に表示される番号から、隔離されたインターフェイスを含むインターフェイスの総数がわかります。

## インターフェイスの設定に関する注意事項

- ワイヤレスコントローラの各物理ポートには、AP マネージャを1つだけ設定できます。Cisco 5500 シリーズコントローラの場合、AP 管理が有効になっている管理インターフェイスは、管理またはダイナミック VLAN インターフェイスの AP マネージャのプライマリであるバックアップポートにフェールオーバーすることはできません。
- Cisco 5500 シリーズコントローラは、インターフェイスで断片化された ping をサポートしません。

## 動的 AP 管理について

動的インターフェイスはデフォルトでは WLAN インターフェイスとして作成されます。ただし、動的インターフェイスは、AP マネージャインターフェイスとして設定できます。物理ポートごとに許可される AP マネージャインターフェイスは1つです。動的 AP 管理オプションを有効にした動的インターフェイスは、コントローラからアクセスポイントへのパケットのトンネル発信元、およびアクセスポイントからコントローラへの CAPWAP パケットの宛先として使用されます。AP 管理の動的インターフェイスには固有の IP アドレスが必要で、通常は管理インターフェイスとして同じサブネットに設定されます。



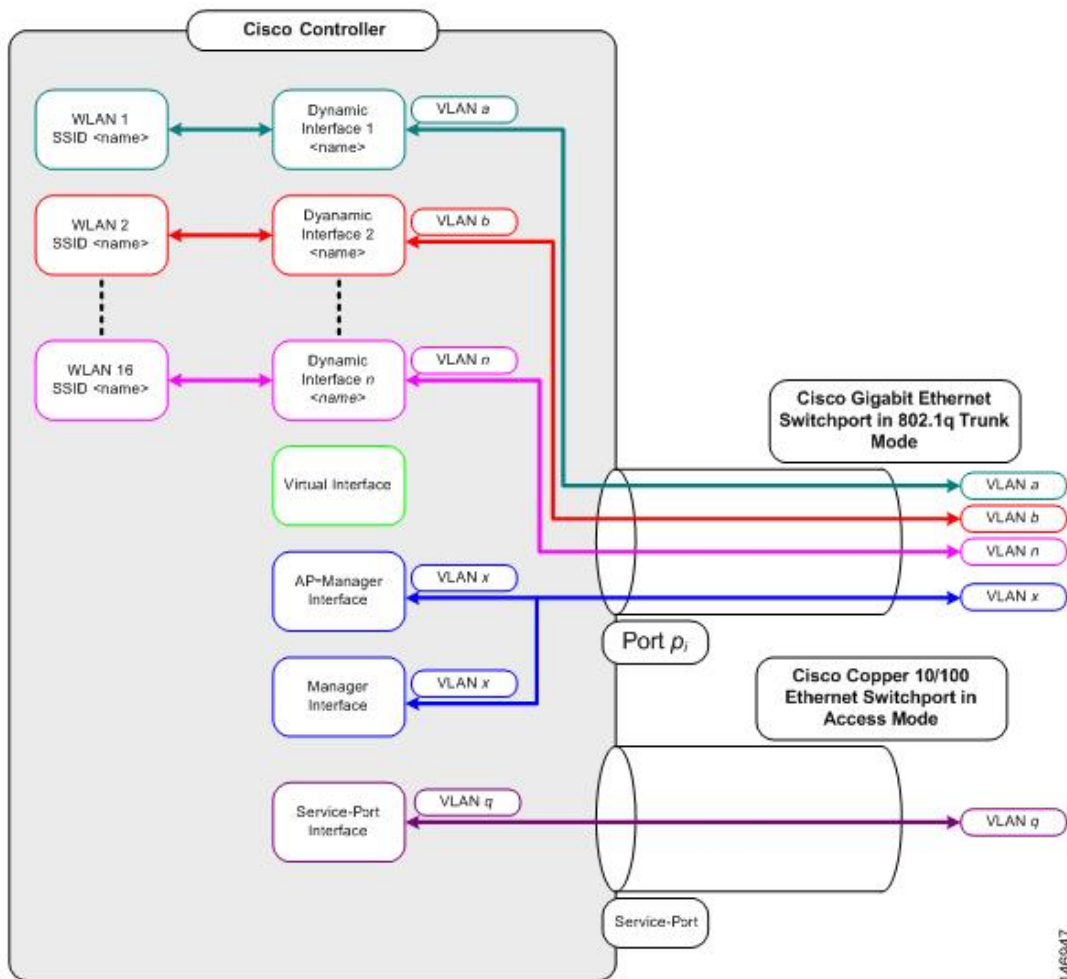
(注) リンク集約 (LAG) が有効化されているときは、AP マネージャ インターフェイスは1つだけ設定することができます。

コントローラ ポートごとに別々の動的 AP マネージャ インターフェイスを設定することをお勧めします。

## WLAN について

WLAN は、サービスセット ID (SSID) をインターフェイスまたはインターフェイス グループにアソシエートします。これは、セキュリティ、Quality of Service (QoS)、無線ポリシーなどその他の無線ネットワーク パラメータを使って設定されます。コントローラ 1 つあたり、最大 512 台の WLAN を設定できます。

図 36: ポート、インターフェイス、および WLAN の関係



各コントローラポートの接続は 802.1Q トランクであり、隣接スイッチでもこのように設定する必要があります。Cisco スイッチでは、802.1Q トランクのネイティブ VLAN にはタグは付いていません。隣接する Cisco スイッチでネイティブ VLAN を使用するためにインターフェイスを設定するには、タグなしになるように、コントローラのインターフェイスを設定する必要があります。



---

(注) VLAN 識別子の値が 0 の場合 ([Controller > Interfaces] ページ)、インターフェイスにタグが付けられていないことを表します。

---

Cisco スイッチにおいて、デフォルト (タグなし) のネイティブ VLAN は VLAN 1 です。コントローラインターフェイスがタグ付きとして設定されている (つまり、VLAN 識別子に 0 以外の値が設定されている) 場合、ネイティブのタグなし VLAN ではなく、近接スイッチの 802.1Q トランク設定で VLAN を許可する必要があります。

コントローラでは、タグ付き VLAN を使用することをお勧めします。また、近接スイッチからコントローラポートへの 802.1Q トランク接続では、関連する VLAN のみを許可するようにしてください。その他の VLAN はすべて、スイッチポート トランク設定で無効にするか、プルーニングする必要があります。コントローラのパフォーマンスを最適化するには、この慣例はきわめて重要です。



---

(注) コントローラが VLAN トラフィックを正常にルーティングできるよう、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。

---





## 第 29 章

# 管理インターフェイスの設定

- [管理インターフェイスについて](#), 353 ページ
- [管理インターフェイスの設定 \(GUI\)](#), 354 ページ
- [管理インターフェイスの設定 \(CLI\)](#), 355 ページ

## 管理インターフェイスについて

管理インターフェイスは、コントローラのインバンド管理や、AAA サーバなどのエンタープライズ サービスへの接続に使用されるデフォルト インターフェイスです。また、コントローラとアクセス ポイント間の通信にも使用されます。管理インターフェイスには、唯一常時「ping 可能」な、コントローラのインバンド インターフェイス IP アドレスが設定されています。コントローラの GUI にアクセスするには、Internet Explorer または Mozilla Firefox ブラウザのアドレス フィールドに、コントローラの管理インターフェイスの IP アドレスを入力します。

CAPWAP の場合、ポートの数に関係なく、このコントローラには、コントローラ間の全通信を制御する管理インターフェイスが 1 つと、コントローラとアクセス ポイント間の全通信を制御する AP マネージャ インターフェイスが 1 つ必要です。



(注) 有線または無線クライアントによる（無線クライアントの動的インターフェイスまたは VLAN からの）コントローラの管理ネットワークへのアクセスを拒否またはブロックするには、許可されたクライアントだけが適切な CPU ACL によって管理ネットワークへのアクセス権を持つように、またはクライアントの動的インターフェイスと管理ネットワーク間のファイアウォールを使用するように、ネットワーク管理者が設定する必要があります。



注意

ゲスト WLAN を管理インターフェイスにマッピングしないでください。EoIP トンネルが切断すると、クライアントが IP を取得し、管理サブネット内に配置されてしまう可能性があります。



注意

ネットワークのコントローラのサービス ポートの同じ VLAN またはサブネットに有線クライアントを設定しないでください。サービス ポートと同じサブネットまたは VLAN に有線クライアントを設定すると、コントローラの管理インターフェイスにアクセスできなくなります。

## 管理インターフェイスの設定 (GUI)

**ステップ 1** [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

**ステップ 2** [management] リンクをクリックします。  
[Interfaces > Edit] ページが表示されます。

**ステップ 3** 管理インターフェイスのパラメータを設定します。

(注) 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューションシステム MAC アドレスが使用されます。

- 該当する場合、隔離および隔離 VLAN ID

(注) [Quarantine] チェックボックスは、この VLAN を正常に動作していない VLAN として設定する場合、またはネットワークアクセスコントロール (NAC) アウトオブバンドを設定する場合にオンにします。このように設定すると、この VLAN に割り当てられているあらゆるクライアントのデータトラフィックがコントローラを通るようになります。

- NAT アドレス (Cisco 2500 シリーズ コントローラと Cisco 5500 シリーズ コントローラのみが動的 AP 管理用に設定されます)

(注) 1 対 1 のネットワーク アドレス変換 (NAT) を使用するルータまたは他のゲートウェイ デバイスの背後に Cisco 2500 シリーズ コントローラまたは Cisco 5500 シリーズ コントローラを展開できるようにする場合は、[Enable NAT Address] チェックボックスをオンにして、外部 NAT IP アドレスを入力します。NAT を使用すると、ルータなどのデバイスがインターネット (パブリック) とローカルネットワーク (プライベート) 間のエージェントとして動作します。この場合、コントローラのイントラネット IP アドレスは対応する外部アドレスにマッピングされます。コントローラが discovery response で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの動的 AP マネージャ インターフェイスを設定する必要があります。

(注) Cisco 2500 シリーズ コントローラまたは Cisco 5500 シリーズ コントローラの管理インターフェイスに外部 NAT IP アドレスが設定されている場合、ローカルモードの AP はコントローラにアソシエートできません。この問題を回避するには、グローバルに有効な IP アドレスが管理インターフェイスに設定されるようにするか、外部 NAT IP アドレスをローカル AP に対して内部的に有効なものにします。



(注) NAT パラメータの使用は、1 対 1 のマッピングの NAT を使用する場合にだけサポートされています。これにより、各プライベートクライアントはグローバルアドレスに直接かつ固定的にマッピングされます。NAT パラメータでは、クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートしていません。

- VLAN 識別子

(注) タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を入力します。管理インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ

- 動的 AP 管理 (Cisco 2500 シリーズ コントローラ または Cisco 5500 シリーズ コントローラ に対してのみ)

(注) Cisco 5500 シリーズ コントローラ の場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。必要に応じて、管理インターフェイスを AP マネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。

- 物理ポートの割り当て (Cisco 2500 シリーズ コントローラ または Cisco 5500 シリーズ コントローラ を除くすべてのコントローラ)

- プライマリ および セカンダリの DHCP サーバ

- 必要に応じて、アクセス コントロール リスト (ACL) の設定

ステップ 4 [Save Configuration] をクリックします。

ステップ 5 管理インターフェイスまたは仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

## 管理インターフェイスの設定 (CLI)

ステップ 1 **show interface detailed management** コマンドを入力し、現在の管理インターフェイスの設定を表示します。

(注) 管理インターフェイスでは、工場出荷時にコントローラに設定されたディストリビューションシステム MAC アドレスが使用されます。

ステップ 2 **config wlan disable wlan-number** コマンドを入力して、ディストリビューションシステム通信用に管理インターフェイスを使用する各 WLAN を無効にします。

ステップ 3 次のコマンドを入力し、管理インターフェイスを定義します。

- **config interface address management ip-addr ip-netmask gateway**

- **config interface quarantine vlan management *vlan\_id***
  - (注) 隔離 VLAN を管理インターフェイスに設定するには、**config interface quarantine vlan management *vlan\_id*** コマンドを使用します。
- **config interface vlan management {*vlan-id* | 0}**
  - (注) タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を入力します。管理インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。
- **config interface ap-manager management {enable | disable}** (Cisco 5500 シリーズ コントローラの場合のみ)
  - (注) 管理インターフェイスに対して動的 AP 管理を有効または無効にするには、**config interface ap-manager management {enable | disable}** コマンドを使用します。Cisco 5500 シリーズ コントローラの場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。必要に応じて、管理インターフェイスを AP マネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。
- **config interface port management *physical-ds-port-number*** (5500 シリーズを除くすべてのコントローラ)
- **config interface dhcp management *ip-address-of-primary-dhcp-server* [*ip-address-of-secondary-dhcp-server*]**
- **config interface acl management *access-control-list-name***

**ステップ 4** 1 対 1 のネットワーク アドレス変換 (NAT) を使用するルータまたは他のゲートウェイ デバイスの背後に Cisco 5500 シリーズ コントローラを展開できるようにする場合は、次のコマンドを入力します。

- **config interface nat-address management {enable | disable}**
- **config interface nat-address management set *public\_IP\_address***

NAT を使用すると、ルータなどのデバイスがインターネット (パブリック) とローカルネットワーク (プライベート) 間のエージェントとして動作します。この場合、コントローラのイントラネット IP アドレスは対応する外部アドレスにマッピングされます。コントローラが **discovery response** で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの動的 AP マネージャ インターフェイスを設定する必要があります。

- (注) これらのコマンドは、1 対 1 マッピング NAT での使用に対してだけサポートされています。各プライベートクライアントはグローバルアドレスに対して直接的かつ固定的にマッピングされます。これらのコマンドでは、クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートされません。

**ステップ 5** **save config** コマンドを入力します。

**ステップ 6** **show interface detailed management** コマンドを入力して、変更内容が保存されていることを確認します。

**ステップ 7** 管理インターフェイスに何らかの変更を行った場合に、変更を有効にするためにコントローラをリブートするには、**reset system** と入力します。



# 第 30 章

## AP マネージャ インターフェイスの設定

- AP マネージャ インターフェイスについて, 357 ページ
- AP マネージャ インターフェイス設定の制約事項, 358 ページ
- AP マネージャ インターフェイスの設定 (GUI), 358 ページ
- AP マネージャ インターフェイスの設定 (CLI), 359 ページ
- 設定例 : Cisco 5500 シリーズ コントローラでの AP マネージャの設定, 360 ページ

### AP マネージャ インターフェイスについて

1つのコントローラに1つ以上のAPマネージャインターフェイスがあります。このインターフェイスは、Lightweightアクセスポイントがコントローラにjoinした後でコントローラとアクセスポイントの間で行われるすべてのレイヤ3通信に使用されます。APマネージャのIPアドレスは、コントローラからアクセスポイントへのCAPWAPパケットのトンネル発信元、およびアクセスポイントからコントローラへのCAPWAPパケットの宛先として使用されます。



(注) コントローラはジャンボフレームの送信をサポートしていません。フラグメンテーションおよび再構成を必要とするAPにコントローラからCAPWAPパケットが送信されないようにするには、クライアント側でMTU/MSSを減らします。

APマネージャインターフェイスは、どのディストリビューションシステムポートを介して通信するときも、できる限り多くのLightweightアクセスポイントのアソシエーションおよび通信を行うために、レイヤ3ネットワーク全体のアクセスポイントのCAPWAPまたはLWAPP joinメッセージを受信します。

## AP マネージャ インターフェイス設定の制約事項

- 管理インターフェイスおよび AP マネージャのインターフェイスの MAC アドレスは、ベース LAG MAC アドレスと同じです。
- 使用可能なディストリビューションシステムポートが1つだけの場合は、ディストリビューションシステム ポート 1 を使用してください。
- 
- AP マネージャ インターフェイスを設定する必要はありません。管理インターフェイスはデフォルトで、AP マネージャ インターフェイスのように動作するので、アクセス ポイントはこのインターフェイスで join できます。
- リンク集約 (LAG) が有効化されているときは、AP マネージャ インターフェイスは1つだけ設定することができます。ただし、LAG が無効の場合は、1つ以上の AP マネージャ インターフェイスを作成できます。通常は1つの物理ポートにつき1つです。
- AP マネージャ インターフェイスに対するポート冗長化はサポートされません。AP マネージャ インターフェイスをバックアップ ポートにマッピングすることはできません。

## AP マネージャ インターフェイスの設定 (GUI)

**ステップ 1** [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

**ステップ 2** AP マネージャ インターフェイスをクリックします。  
[Interface > Edit] ページが表示されます。

**ステップ 3** AP-Manager Interface パラメータを設定します。

(注) Cisco 5500 シリーズコントローラの場合は、AP マネージャ インターフェイスを設定する必要はありません。管理インターフェイスは、デフォルトで AP マネージャ インターフェイスとして動作します。

- 物理ポートの割り当て
- VLAN 識別子

(注) タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を入力します。  
AP マネージャ インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ
- プライマリおよびセカンダリの DHCP サーバ
- 必要な場合は、アクセス コントロール リスト (ACL) 名

**ステップ 4** [Save Configuration] をクリックして、変更を保存します。

**ステップ 5** 管理インターフェイスまたは仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

## AP マネージャ インターフェイスの設定 (CLI)

### はじめる前に

Cisco 5500 シリーズ コントローラの場合は、AP マネージャ インターフェイスを設定する必要はありません。管理インターフェイスは、デフォルトで AP マネージャ インターフェイスとして動作します。

- ステップ 1** **show interface summary** コマンドを入力して、現在のインターフェイスを表示します。  
 (注) システムがレイヤ2モードで動作している場合は、AP マネージャ インターフェイスは出力に表示されません。
- ステップ 2** **show interface detailed ap-manager** コマンドを入力して、現在の AP マネージャ インターフェイスの設定を表示します。
- ステップ 3** **config wlan disable wlan-number** コマンドを入力して、ディストリビューション システム通信用に AP マネージャ インターフェイスを使用する各 WLAN を無効にします。
- ステップ 4** 次のコマンドを入力し、AP マネージャ インターフェイスを定義します。
- **config interface address ap-manager ip-addr ip-netmask gateway**
  - **config interface vlan ap-manager {vlan-id | 0}**  
 (注) タグなし VLAN については 0、タグ付き VLAN についてはゼロ以外の値を入力します。  
 AP マネージャ インターフェイスでは、タグ付きの VLAN を使用することをお勧めします。
  - **config interface port ap-manager physical-ds-port-number**
  - **config interface dhcp ap-manager ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]**
  - **config interface acl ap-manager access-control-list-name**
- ステップ 5** **save config** コマンドを入力して、変更を保存します。
- ステップ 6** **show interface detailed ap-manager** コマンドを入力して、変更内容が保存されていることを確認します。

## 設定例 : Cisco 5500 シリーズ コントローラでの AP マネージャの設定

Cisco 5500 シリーズ コントローラでは、LAG を使用しない場合、8 つの動的 AP マネージャ インターフェイスをコントローラの 8 つのギガビットポートに関連付けることをお勧めします。管理 インターフェイス（デフォルトで AP マネージャ インターフェイスのように機能する）を使用している場合、さらに動的 AP マネージャ インターフェイスを 7 つ作成し、残りの 7 つのギガビットポートに関連付ける必要があります。

次の図は、動的 AP マネージャ インターフェイスとして有効であり、ポート番号 2 に関連付けられている動的インターフェイスを表しています。

図 37 : 動的 AP 管理を使用した動的インターフェイスの例

The screenshot shows the configuration page for a dynamic interface named 'dyn-1' on a Cisco Wireless Controller. The page is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes sections like General, Inventory, Interfaces, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main configuration area is titled 'Interfaces > Edit' and contains several sections: 'General Information' (Interface Name: dyn-1, MAC Address: 00:21:1b:fc:29:c1), 'NAT Address' (Enable NAT Address: unchecked), 'Physical Information' (Port Number: 2, Backup Port: 0, Active Port: 2, Enable Dynamic AP Management: checked), 'Interface Address' (VLAN Identifier: 99, IP Address: 209.165.200.225, Netmask: 255.255.255.0, Gateway: 10.10.99.1), and 'DHCP Information' (Primary DHCP Server: 10.10.99.1, Secondary DHCP Server: empty).

| General Information |                   |
|---------------------|-------------------|
| Interface Name      | dyn-1             |
| MAC Address         | 00:21:1b:fc:29:c1 |

| NAT Address        |                          |
|--------------------|--------------------------|
| Enable NAT Address | <input type="checkbox"/> |

| Physical Information         |                                     |
|------------------------------|-------------------------------------|
| Port Number                  | 2                                   |
| Backup Port                  | 0                                   |
| Active Port                  | 2                                   |
| Enable Dynamic AP Management | <input checked="" type="checkbox"/> |

| Interface Address |                 |
|-------------------|-----------------|
| VLAN Identifier   | 99              |
| IP Address        | 209.165.200.225 |
| Netmask           | 255.255.255.0   |
| Gateway           | 10.10.99.1      |

| DHCP Information      |            |
|-----------------------|------------|
| Primary DHCP Server   | 10.10.99.1 |
| Secondary DHCP Server |            |

274694

次の図は、LAGが無効になっている Cisco 5500 シリーズ コントローラを表しています。管理インターフェイスは1つの動的 AP マネージャ インターフェイスとして使用され、他の7つの動的 AP マネージャ インターフェイスはそれぞれ異なるギガビット ポートにマッピングされています。

図 38 : Cisco 5500 シリーズのコントローラ インターフェイスの設定例

| Interface Name               | VLAN Identifier | IP Address      | Interface Type | Dynamic AP Management |
|------------------------------|-----------------|-----------------|----------------|-----------------------|
| <a href="#">dyn-1</a>        | 99              | 209.165.200.225 | Dynamic        | Enabled               |
| <a href="#">dyn-2</a>        | 99              | 209.165.200.226 | Dynamic        | Enabled               |
| <a href="#">dyn-3</a>        | 99              | 209.165.200.227 | Dynamic        | Enabled               |
| <a href="#">dyn-4</a>        | 99              | 209.165.200.228 | Dynamic        | Enabled               |
| <a href="#">dyn-5</a>        | 99              | 209.165.200.229 | Dynamic        | Enabled               |
| <a href="#">dyn-6</a>        | 99              | 209.165.200.230 | Dynamic        | Enabled               |
| <a href="#">dyn-7</a>        | 99              | 209.165.200.231 | Dynamic        | Enabled               |
| <a href="#">management</a>   | untagged        | 209.165.200.232 | Static         | Enabled               |
| <a href="#">service-port</a> | N/A             | 209.165.200.233 | Static         | Not Supported         |
| <a href="#">virtual</a>      | N/A             | 209.165.200.234 | Static         | Not Supported         |

274695







## 第 31 章

# 仮想インターフェイスの設定

- [仮想インターフェイスについて](#), 363 ページ
- [仮想インターフェイスの設定 \(GUI\)](#), 364 ページ
- [仮想インターフェイスの設定 \(CLI\)](#), 364 ページ

## 仮想インターフェイスについて

仮想インターフェイスは、モビリティ管理、Dynamic Host Configuration Protocol (DHCP) リレー、およびゲスト Web 認証や VPN 終端などのレイヤ 3 の組み込みセキュリティをサポートするために使用されます。また、レイヤ 3 Web 許可が有効な場合に証明書のソースを確認するために、レイヤ 3 Security Manager と Mobility Manager で使用されるドメイン ネーム システム (DNS) ゲートウェイのホスト名も管理します。

具体的には、仮想インターフェイスは主に次の 2 つの役割を果たします。

- ワイヤレス クライアントの IP アドレスを DHCP サーバから取得する、ワイヤレス クライアントの代理 DHCP サーバの役割。
- Web 認証ログイン ページのリダイレクトアドレスの役割。

仮想インターフェイスの IP アドレスは、コントローラと無線クライアントの間の通信でのみ使用されます。ディストリビューションシステム ポートから出て、スイッチド ネットワークに入るパケットの発信元アドレスや、宛先アドレスとなることは決してありません。システムを正常に動作させるには、仮想インターフェイスの IP アドレスを設定する必要がありますが (0.0.0.0 は設定できません)、ネットワーク上の他のデバイスは、この仮想インターフェイスと同じアドレスを使用できません。したがって、仮想インターフェイスは、割り当てられず、使用もされない ゲートウェイ IP アドレスを使って設定する必要があります。仮想インターフェイスの IP アドレスは ping できませんし、ネットワーク上のいかなるルーティングテーブルにも存在してはいけません。また、仮想インターフェイスを物理ポートにマッピングすることもできません。



- (注) 同一のモビリティグループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。設定しなかった場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

## 仮想インターフェイスの設定 (GUI)

ステップ 1 [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

ステップ 2 [Virtual] をクリックします。  
[Interfaces > Edit] ページが表示されます。

ステップ 3 次のパラメータを入力します。

- 架空の未割り当てで未使用のゲートウェイ IP アドレス
- DNS ゲートウェイ ホスト名

(注) 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスの DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

ステップ 4 [Save Configuration] をクリックします。

ステップ 5 管理インターフェイスまたは仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

## 仮想インターフェイスの設定 (CLI)

ステップ 1 **show interface detailed virtual** コマンドを入力し、現在の仮想インターフェイスの設定を表示します。

ステップ 2 **config wlan disable wlan-number** コマンドを入力して、ディストリビューションシステム通信用に仮想インターフェイスを使用する各 WLAN を無効にします。

ステップ 3 次のコマンドを入力し、仮想インターフェイスを定義します。

- **config interface address virtual ip-address**

(注) *ip-address* には、架空の未割り当てで未使用のゲートウェイ IP アドレスを入力します。

- **config interface hostname virtual** *dns-host-name*

**ステップ 4** **reset system** コマンドを入力します。NVRAM に設定変更を保存するには、確認のプロンプトで Y と入力します。コントローラがリブートします。

**ステップ 5** **show interface detailed virtual** コマンドを入力して、変更内容が保存されていることを確認します。

---





## 第 32 章

# サービスポート インターフェイスの設定

- サービスポート インターフェイスについて, 367 ページ
- サービスポート インターフェイスの設定に関する制限, 367 ページ
- サービスポート インターフェイスの設定 (GUI), 367 ページ
- サービスポート インターフェイスの設定 (CLI), 368 ページ

## サービスポート インターフェイスについて

サービスポート インターフェイスはサービスポートを介した通信を制御し、サービスポートに対して静的にマッピングされます。サービスポートは DHCP を使用して IP アドレスを取得したり、固定 IP アドレスを割り当てたりすることはできますが、サービスポート インターフェイスにデフォルト ゲートウェイを割り当てることはできません。サービスポートへのリモートネットワーク アクセスに使用される静的なルートはコントローラを通じて定義できます。

## サービスポート インターフェイスの設定に関する制限

- Cisco 7500 シリーズ コントローラと Cisco 5500 シリーズ コントローラにのみ、外部ネットワークから到達可能な物理サービスポート インターフェイスがあります。

## サービスポート インターフェイスの設定 (GUI)

- ステップ 1** [Controller]> [Interfaces] の順に選択して、[Interfaces] ページを開きます。
- ステップ 2** サービスポート リンクをクリックして、[Interfaces > Edit] ページを開きます。
- ステップ 3** 次の Service-Port Interface パラメータを入力します。
  - (注) サービスポート インターフェイスでは、工場出荷時にコントローラに設定されたサービスポートの MAC アドレスが使用されます。

- DHCP プロトコル (有効)
- DHCP プロトコル (無効) および IP アドレスと IP ネットマスク

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

ステップ 5 管理インターフェイスまたは仮想インターフェイスに何らかの変更を行ったときに変更を有効にするには、コントローラをリブートします。

---

## サービスポートインターフェイスの設定 (CLI)

ステップ 1 次のコマンドを入力して、現在のサービスポートインターフェイスの設定を表示します。

**show interface detailed service-port**

(注) サービスポートインターフェイスでは、工場出荷時にコントローラに設定されたサービスポートの MAC アドレスが使用されます。

ステップ 2 次のコマンドを入力し、サービスポートインターフェイスを定義します。

- DHCP サーバを設定するには、次のコマンドを入力します。

**config interface dhcp service-port enable**

- DHCP サーバを無効にするには、次のコマンドを入力します。

**config interface dhcp service-port disable**

- IP アドレスを設定するには、次のコマンドを入力します。

**config interface address service-port ip-addr ip-netmask**

ステップ 3 このサービスポートは、コントローラの帯域外管理に使用されます。管理ワークステーションがリモートサブネットにある場合、このリモートワークステーションからコントローラを管理するには、コントローラにルートを追加する必要があります。そのためには、次のコマンドを入力します。

**config route add network-ip-addr ip-netmask gateway**

ステップ 4 **save config** コマンドを入力して、変更を保存します。

ステップ 5 **show interface detailed service-port** コマンドを入力して、変更内容が保存されていることを確認します。

---



## 第 33 章

# 動的インターフェイスの設定

- [動的インターフェイスについて, 369 ページ](#)
- [動的インターフェイス設定の前提条件, 370 ページ](#)
- [動的インターフェイスの設定に関する制約事項, 370 ページ](#)
- [動的インターフェイスの設定 \(GUI\) , 371 ページ](#)
- [動的インターフェイスの設定 \(CLI\) , 372 ページ](#)

## 動的インターフェイスについて

動的インターフェイスは VLAN インターフェイスとも呼ばれ、ユーザによって作成され、無線 LAN クライアントの VLAN に相当する設計になっています。1つのコントローラで最大 512 個の動的インターフェイス (VLAN) をサポートできます。動的インターフェイスはそれぞれ、個別に設定され、コントローラの任意またはすべてのディストリビューションシステムポートに独立した通信ストリームを設定できます。各ダイナミックインターフェイスでは、VLAN およびコントローラとその他のすべてのネットワーク デバイスとの間の通信が制御されます。また、インターフェイスにマップされた WLAN に接続するワイヤレス クライアントに対して、それぞれが DHCP リレーとして機能します。動的インターフェイスは、ディストリビューションシステムポート、WLAN、レイヤ 2 管理インターフェイス、およびレイヤ 3 AP マネージャ インターフェイスに割り当てることができます。また、動的インターフェイスをバックアップポートにマップすることもできます。

1つ、または複数の動的インターフェイスをディストリビューションシステムポートに設定できます。また、1つも設定しなくても問題ありません。ただし、動的インターフェイスはすべて、そのポートに設定された他のインターフェイスとは異なる VLAN または IP サブネットに設定する必要があります。ポートにタグが付いていない場合は、動的インターフェイスはすべて、そのポートに設定されている他のインターフェイスとは異なる IP サブネットに設定する必要があります。

次の表に、各種コントローラ プラットフォームでサポートされている VLAN の最大数を示します。

表 7: Cisco シスコ ワイヤレス コントローラでサポートされている VLAN の最大数

| 無線コントローラ                                            | VLAN の最大数 |
|-----------------------------------------------------|-----------|
| Cisco 仮想ワイヤレス コントローラ                                | 512       |
| Cisco Wireless Controller Module for ISR G2         | 16        |
| Cisco 2500 シリーズ ワイヤレス コントローラ                        | 16        |
| Cisco 5500 シリーズ ワイヤレス コントローラ                        | 512       |
| Cisco Catalyst 6500 シリーズ ワイヤレス サービス モジュール 2 (WiSM2) | 512       |
| Cisco Flex 7500 シリーズ Cloud Controller               | 4,096     |
| Cisco 8500 シリーズ コントローラ                              | 4,096     |

## 動的インターフェイス設定の前提条件

コントローラの動的インターフェイスを設定する際は、次の内容を確認する必要があります。

- 
- 動的インターフェイスでは、タグ付きの VLAN を使用する必要があります。

## 動的インターフェイスの設定に関する制約事項

次の制限は、コントローラに動的インターフェイスを設定するときに適用されます。

- コントローラ CPU から到達可能なサーバ (RADIUS サーバなど) と同じサブネットワーク内に動的インターフェイスを設定しないでください。設定すると、非対称ルーティングの問題が発生する可能性があります。
- 動的 AP 管理がダイナミック VLAN で有効になると、有線クライアントは AP マネージャ インターフェイスの IP アドレスを使用して、Cisco WLC 2500 シリーズの管理インターフェイスにアクセスすることはできません。
- 
- 動的インターフェイスとして設定されたサブネットワークから送信される SNMP 要求の場合、コントローラは応答しますが、その応答は会話を開始したデバイスに到達しません。



- DHCP プロキシまたは RADIUS 送信元インターフェイスを使用している場合は、動的インターフェイスに有効なルーティング可能アドレスがあることを確認します。コントローラインターフェイス間で重複するアドレスはサポートされていません。

## 動的インターフェイスの設定 (GUI)

**ステップ 1** [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

**ステップ 2** 次のいずれかの操作を行います。

- 新たに動的インターフェイスを作成するには、[New] をクリックします。[Interfaces > New] ページが表示されます。ステップ 3 に進みます。
- 既存の動的インターフェイスの設定を変更するには、インターフェイスの名前をクリックします。そのインターフェイスの [Interfaces > Edit] ページが表示されます。ステップ 5 に進みます。
- 既存の動的インターフェイスを削除するには、そのインターフェイスの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

**ステップ 3** 上の図に示すように、インターフェイス名と VLAN 識別子を入力します。

**ステップ 4** [Apply] をクリックして、変更を確定します。[Interfaces > Edit] ページが表示されます。

**ステップ 5** 次のパラメータを設定します。

- 該当する場合、ゲスト LAN
- 該当する場合、隔離および隔離 VLAN ID
  - (注) [Quarantine] チェックボックスは、この VLAN を正常に動作していない VLAN として設定する場合、またはネットワークアクセスコントロール (NAC) アウトオブバンドを設定する場合にオンにします。このように設定すると、この VLAN に割り当てられているあらゆるクライアントのデータトラフィックがコントローラを通るようになります。
- 物理ポートの割り当て (5500 シリーズを除くすべてのコントローラ)
- NAT アドレス (動的 AP 管理用に設定された Cisco 5500 シリーズコントローラの場合のみ)
  - (注) 1 対 1 のネットワークアドレス変換 (NAT) を使用するルータまたは他のゲートウェイデバイスの背後に Cisco 5500 シリーズコントローラを展開できるようにする場合は、[Enable NAT Address] チェックボックスをオンにして、外部 NAT IP アドレスを入力します。NAT を使用すると、ルータなどのデバイスがインターネット (パブリック) とローカルネットワーク (プライベート) 間のエージェントとして動作します。この場合、コントローラのイントラネット IP アドレスは対応する外部アドレスにマッピングされます。コントローラが discovery response で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの動的 AP マネージャインターフェイスを設定する必要があります。

(注) NAT パラメータの使用は、1 対 1 のマッピングの NAT を使用する場合にだけサポートされています。これにより、各プライベートクライアントはグローバルアドレスに直接かつ固定的にマッピングされます。NAT パラメータでは、クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートしていません。

- 動的 AP 管理

(注) この機能を有効にすると、この動的インターフェイスは AP マネージャ インターフェイスとして設定されます (物理ポートごとに許可される AP マネージャ インターフェイスは 1 つです)。AP マネージャ インターフェイスとして指定された動的インターフェイスは WLAN インターフェイスとして使用できません。

(注) コントローラに設定されている動的インターフェイスとは異なる VLAN に AP を設定します。動的インターフェイスと同じ VLAN 内に存在する AP は、コントローラに登録されず、「LWAPP discovery rejected」エラーと「Layer 3 discovery request not received on management VLAN」エラーがコントローラ上のログに記録されます。

- VLAN 識別子

- 固定 IP アドレス、IP ネットマスク、およびデフォルト ゲートウェイ
- プライマリおよびセカンダリの DHCP サーバ
- 必要な場合は、アクセス コントロール リスト (ACL) 名

(注) 適切に動作させるには、Port Number パラメータおよび Primary DHCP Server パラメータを設定する必要があります。

**ステップ 6** [Save Configuration] をクリックして、変更を保存します。

**ステップ 7** 作成または編集する動的インターフェイスごとにこの手順を繰り返します。

## 動的インターフェイスの設定 (CLI)

**ステップ 1** `show interface summary` コマンドを入力して、現在の動的インターフェイスを表示します。

**ステップ 2** 次のコマンドを入力して、特定の動的インターフェイスの詳細を表示します。

`show interface detailed operator_defined_interface_name`

(注) インターフェイス名にスペースが含まれる場合は、二重引用符で囲む必要があります。例：

`config interface create "vlan 25"`

**ステップ 3** `config wlan disable wlan_id` コマンドを入力して、ディストリビューションシステム通信用に動的インターフェイスを使用する各 WLAN を無効にします。

**ステップ 4** 次のコマンドを入力し、動的インターフェイスを設定します。

- `config interface create operator_defined_interface_name {vlan_id | x}`

- **config interface address interface** *ip\_addr ip\_netmask* [*gateway*]
- **config interface vlan operator\_defined\_interface\_name** {*vlan\_id* | *o*}
- **config interface port operator\_defined\_interface\_name** *physical\_ds\_port\_number*
- **config interface ap-manager operator\_defined\_interface\_name** {**enable** | **disable**}

(注) 動的 AP 管理を有効または無効にするには、**config interface ap-manager operator\_defined\_interface\_name {enable|disable}** コマンドを使用します。この機能を有効にすると、この動的インターフェイスは AP マネージャ インターフェイスとして設定されます (物理ポートごとに許可される AP マネージャ インターフェイスは 1 つです)。AP マネージャ インターフェイスとして指定された動的インターフェイスは WLAN インターフェイスとして使用できません。

- **config interface dhcp operator\_defined\_interface\_name** *ip\_address\_of\_primary\_dhcp\_server* [*ip\_address\_of\_secondary\_dhcp\_server*]
- **config interface quarantine vlan interface\_name** *vlan\_id*
- (注) 任意のインターフェイスに隔離 VLAN を設定するには、**config interface quarantine vlan interface\_name vlan\_id** コマンドを使用します。
- **config interface acl operator\_defined\_interface\_name** *access\_control\_list\_name*

**ステップ 5** 1 対 1 のネットワーク アドレス変換 (NAT) を使用するルータまたは他のゲートウェイ デバイスの背後に Cisco 5500 シリーズ コントローラを展開できるようにする場合は、次のコマンドを入力します。

- **config interface nat-address dynamic-interface operator\_defined\_interface\_name** {**enable** | **disable**}
- **config interface nat-address dynamic-interface operator\_defined\_interface\_name** **set public\_IP\_address**

NAT を使用すると、ルータなどのデバイスがインターネット (パブリック) とローカルネットワーク (プライベート) 間のエージェントとして動作します。この場合、コントローラのイントラネット IP アドレスは対応する外部アドレスにマッピングされます。コントローラが **discovery response** で適切な IP アドレスを送信できるように、外部 NAT IP アドレスを使用してコントローラの動的 AP マネージャ インターフェイスを設定する必要があります。

(注) これらのコマンドは、1 対 1 マッピング NAT での使用に対してだけサポートされています。各プライベートクライアントはグローバルアドレスに対して直接的かつ固定的にマッピングされます。これらのコマンドでは、クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートされません。

**ステップ 6** **config wlan enable** *wlan\_id* コマンドを入力して、ディストリビューション システム通信に動的インターフェイスを使用する各 WLAN を再度有効にします。

**ステップ 7** **save config** コマンドを入力して、変更を保存します。

**ステップ 8** **show interface detailed operator\_defined\_interface\_name** command and **show interface summary** コマンドを入力し、変更内容が保存されていることを確認します。

(注) 動的インターフェイスを削除する必要がある場合は、**config interface delete operator\_defined\_interface\_name** コマンドを入力します。





# 第 34 章

## ポートの設定

- [ポートの設定 \(GUI\)](#) , 375 ページ

### ポートの設定 (GUI)

コントローラのポートは、工場出荷時にデフォルト設定が行われていて、追加設定しなくても動作する設計になっています。しかし、必要に応じて、コントローラのポートのステータスを表示し、設定パラメータを編集できます。

**ステップ 1** [Controller] > [Ports] を選択して [Ports] ページを開きます。

このページには、コントローラのポート別に現在の設定が表示されます。

特定のポートの設定を変更するには、そのポートの番号をクリックします。[Port > Configure] ページが表示されます。

(注) 管理インターフェイスおよび AP マネージャ インターフェイスが同じポートにマップされており、いずれも同じ VLAN のメンバである場合は、WLAN を無効にしてから、ポートマッピングをいずれかのインターフェイスに変更する必要があります。管理インターフェイスと AP マネージャ インターフェイスが別々の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

(注) [Port > Configure] ページで使用できるパラメータの数は、使用しているコントローラの種類によって異なります。

ポートの現在のステータスには、次のものがあります。

- [Port Number] : 現在のポートの番号。
- [Admin Status] : ポートの現在の状態。 値 : [Enable] または [Disable]
- [Physical Mode] : ポートの物理インターフェイスの設定。 モードは、コントローラの種類によって異なります。

- [Physical Status] : ポートで使用されているデータ レート。使用可能なデータ レートは、コントローラの種類によって異なります。
  - 2500 シリーズ 1 Gbps 全二重
  - WiSM2 - 10 Gbps 全二重
  - 7500 シリーズ - 10 Gbps 全二重
- [Link Status] : ポートのリンクステータス。値 : [Link Up]、または [Link Down]
- [Link Trap] : リンク ステータスが変更されたときにトラップを送信するようにポートが設定されているかどうかを示します。値 : [Enable] または [Disable]
- [Power over Ethernet (PoE)] : 接続デバイスにイーサネット ケーブル経由で受電する機能がある場合は、-48VDC を供給します。値 : [Enable] または [Disable]
  - (注) 古い Cisco アクセス ポイントの中には、コントローラ ポートで有効になっていても、PoE を受電しないものがあります。このような場合は、Cisco Technical Assistance Center (TAC) にお問い合わせください。

次に、ポートの設定可能なパラメータのリストを示します。

- 1 [Admin Status] : ポートを経由するトラフィックのフローを有効、または無効にします。オプション : [Enable] または [Disable]、デフォルト : [Enable]。
  - (注) プライマリ ポートリンクがダウンした場合、メッセージは内部のログにのみ記録され、syslog サーバにはポストされません。syslog サーバへのロギングが回復するまでに、最大で 40 秒の時間がかかる可能性があります。
- 2 [Physical Mode] : ポートのデータ レートが自動的に設定されるか、ユーザによって指定されるかを表します。サポートされているデータ レートは、コントローラの種類によって異なります。デフォルト : [Auto]
- 3 [Link Trap] : ポートのリンク ステータスが変化したときにポートからトラップが送信されるようにします。オプション : [Enable] または [Disable]、デフォルト : [Enable]。

**ステップ 2** [Apply] をクリックします。

**ステップ 3** [Save Configuration] をクリックします。

**ステップ 4** [Ports] ページに戻り、変更内容を確認するには、[Back] をクリックします。

**ステップ 5** 設定するポートそれぞれについて、この手順を繰り返します。



# 第 35 章

## リンク集約の設定

---

- [リンク集約について](#), 377 ページ
- [リンク集約の制約事項](#), 378 ページ
- [リンク集約の有効化 \(GUI\)](#), 380 ページ
- [リンク集約の有効化 \(CLI\)](#), 380 ページ
- [リンク集約の設定の確認 \(CLI\)](#), 380 ページ
- [リンク集約をサポートするための隣接デバイスの設定](#), 381 ページ
- [リンク集約と複数の AP マネージャ インターフェイス間の選択](#), 381 ページ

### リンク集約について

リンク集約 (LAG) は、802.3ad ポート集約標準の部分的な実装です。コントローラのすべてのディストリビューションシステムポートが1つの802.3adポートチャンネルにまとめられるので、コントローラのポートの設定に必要なIPアドレスの数を減らすことができます。LAGが有効である場合、ポートの冗長性は動的に管理され、アクセスポイントはユーザからは透過的にロードバランシングされます。

LAGを使用すれば、インターフェイスごとにプライマリポートとセカンダリポートを設定する必要がないので、コントローラ設定も簡単に行えるようになります。いずれかのコントローラポートに障害が発生した場合は、他のポートへトラフィックが自動的に移行します。少なくとも1つのコントローラポートが機能している限り、システムは継続して動作し、アクセスポイントはネットワークに接続されたままとなります。また、ワイヤレスクライアントは引き続きデータを送受信します。

Cisco WLC は、LAG のインターフェイスで CDP アドバタイズメントを送信しません。



---

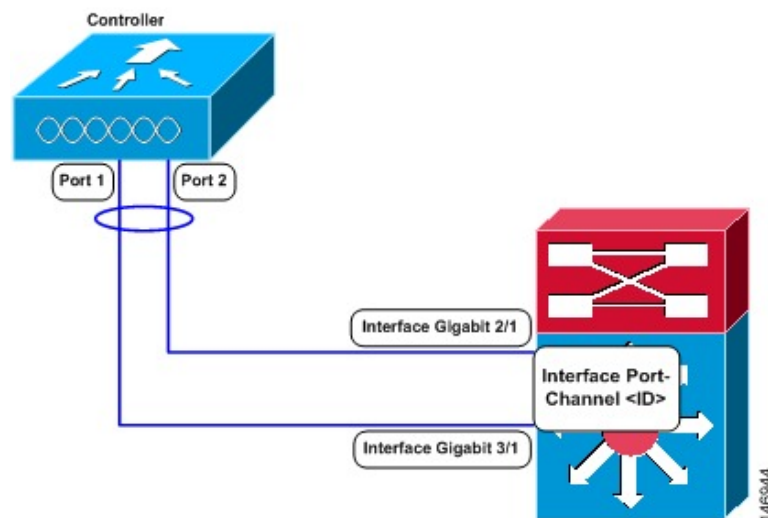
(注) LAG はスイッチ全体でサポートされます。

---

## リンク集約の制約事項

- Cisco 5508 コントローラ上の 8 個すべてのポートを 1 本のリンクにまとめることができます。
- 単一の Catalyst 6500 シリーズ スイッチの中の 2 つのモジュールで終端することによって冗長化されるので、一方のモジュールに障害が発生してもスイッチとコントローラとの接続は維持されます。コントローラのポート 1 は Catalyst 6500 シリーズ スイッチのギガビット インターフェイス 3/1 に接続されており、コントローラのポート 2 はギガビット インターフェイス 2/1 に接続されています。どちらのスイッチ ポートも、同じチャンネルグループに割り当てられています。
- LAG を行うには、コントローラと Catalyst スイッチの両方で EtherChannel が on モードに設定されている必要があります。
- リンクの両端で EtherChannel を on に設定した後は、Catalyst スイッチを Link Aggregation Control Protocol (LACP) あるいは Cisco 独自のポート集約プロトコル (PAgP) に設定することはできません。無条件に LAG に設定されます。コントローラとスイッチの間のチャンネルネゴシエーションは行われなため、スイッチで LAG のダイナミック フォームが設定されている場合は、コントローラはネゴシエーション フレームに回答せず、LAG は構成されません。また、LACP と PAgP はコントローラではサポートされません。
- 推奨されるロードバランシング方法を Catalyst スイッチ上で設定できない場合は、LAG 接続を単一メンバリンクとして設定するか、コントローラで LAG を行わないように設定します。

図 39: Catalyst 6500 シリーズ近接スイッチを使用したリンク集約



- 1 つのコントローラの複数のポートを別々の LAG グループに設定することはできません。1 つのコントローラがサポートする LAG グループは 1 つのみです。したがって、LAG モードのコントローラ 1 つを接続できる隣接デバイスは 1 つのみです。



- LAG を有効化したときや、LAG の設定に変更を加えたときは、ただちにコントローラをリブートしてください。
- LAG を有効にした場合、必要な論理ポートは1つだけなので、AP マネージャ インターフェイスを1つだけ設定できます。LAG を使用する場合は、複数の AP マネージャ インターフェイスのサポートに関する要件はなくなります。
- LAG を有効にした場合、動的 AP マネージャ インターフェイス、およびタグの付いていないインターフェイスはすべて削除されます。同時に、WLAN がすべて無効になり、管理インターフェイスにマッピングされます。また、管理インターフェイス、スタティック AP マネージャ インターフェイス、および VLAN タグ付き動的インターフェイスは、LAG ポートに移されます。
- 複数のタグなしインターフェイスを同じポートに割り当てることはできません。
- LAG を有効にした場合、29 以外のプライマリ ポートを使用してインターフェイスを作成することはできません。
- LAG を有効にした場合、デフォルトでは、すべてのポートが LAG に加わります。近接スイッチにある接続されたポートすべてについて、LAG を設定する必要があります。
- LAG が有効化されているときは、リンクのいずれかがダウンした場合にトラフィックは別のリンクに移されます。
- LAG が有効化されているときは、物理ポートが1つでも機能していればコントローラはクライアントトラフィックを伝送することができます。
- LAG が有効化されているときは、LAG モードの変更をアクティブにするためにコントローラをリポートするまで、アクセスポイントはスイッチに接続されたままになります。また、ユーザに対するデータ サービスが中断されることはありません。
- LAG が有効化されているときは、各インターフェイスに対してプライマリとセカンダリのポートを設定する必要はなくなります。
- LAG が有効化されているときは、コントローラがパケットを受信したポートと同じポートからパケットが送信されます。アクセスポイントからの CAPWAP パケットがコントローラの物理ポート 1 に入ると、コントローラによって CAPWAP ラッパーが除去され、パケットが処理され、物理ポート 1 からネットワークに転送されます。LAG が無効化されている場合は、このようにはならないことがあります。
- LAG を無効化すると、管理、スタティック AP マネージャ、および動的の各インターフェイスはポート 1 に移されます。
- LAG を無効にする場合、すべてのインターフェイスについて、プライマリ ポートとセカンダリ ポートを設定する必要があります。
- LAG を無効にする場合、コントローラ上の各ポートに AP マネージャ インターフェイスを割り当てる必要があります。そうしない場合、アクセスポイントは join できません。
- Cisco 5500 シリーズ コントローラでは、静的リンク集約バンドルが1つだけサポートされません。

- 通常、LAG はスタートアップ ウィザードを使って設定されますが、GUI または CLI を使用して、必要なときに有効または無効にすることができます。
- 直接接続アクセス ポイントがアソシエートしている Cisco 2500 シリーズ コントローラで LAG を有効にした場合、ダイレクト コネクト アクセス ポイントは、LAG の有効化が移行状態であるため、切断されます。LAG を有効にした直後に、コントローラをリブートする必要があります。

## リンク集約の有効化 (GUI)

- 
- ステップ 1 [Controller] > [General] の順に選択して、[General] ページを開きます。
  - ステップ 2 [LAG Mode on Next Reboot] パラメータを [Enabled] に設定します。
  - ステップ 3 [Apply] をクリックして、変更を確定します。
  - ステップ 4 [Save Configuration] をクリックして、変更を保存します。
  - ステップ 5 コントローラをリブートします。
  - ステップ 6 WLAN を適切な VLAN に割り当てます。
- 

## リンク集約の有効化 (CLI)

- 
- ステップ 1 LAG を有効にするには、**config lag enable** コマンドを入力します。  
(注) LAG を無効にするには、**config lag disable** コマンドを入力します。
  - ステップ 2 **save config** コマンドを入力して、設定を保存します。
  - ステップ 3 コントローラをリブートします。
- 

## リンク集約の設定の確認 (CLI)

LAG の設定を確認するには、次のコマンドを入力します。

**show lag summary**

以下に類似した情報が表示されます。

```
LAG Enabled
```

## リンク集約をサポートするための隣接デバイスの設定

コントローラの隣接デバイスも、LAG をサポートするように適切に設定する必要があります。

- コントローラが接続されている隣接ポートはそれぞれ、次のように設定します。

```
interface GigabitEthernet <interface id>
 switchport
 channel-group <id> mode on
 no shutdown
```

- 近接スイッチのポート チャンネルは、次のように設定します。

```
interface port-channel <id>
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk native vlan <native vlan id>
 switchport trunk allowed vlan <allowed vlans>
 switchport mode trunk
 no shutdown
```

## リンク集約と複数の AP マネージャ インターフェイス間の選択

Cisco 5500 シリーズ コントローラにはポートあたりのアクセス ポイント数の制限はありませんが、LAG を使用するか、各ギガビットイーサネットポートで複数の動的 AP マネージャ インターフェイスを使用して、ロード バランシングを自動的に行うことをお勧めします。

コントローラがレイヤ 3 での操作用に設定されている場合、どちらの方法を使用すべきかを判断するポイントは次のとおりです。

- LAG では、コントローラのポートはすべて、同一の近接スイッチに接続されている必要があります。近接スイッチがダウンすると、コントローラの接続は失われます。
- 複数の AP マネージャ インターフェイスを使用する場合、ポートをさまざまな隣接デバイスへ接続できます。近接スイッチの 1 つがダウンしても、コントローラの接続は失われません。ただし、ポートの冗長性に不安がある場合、複数の AP マネージャ インターフェイスの使用には、多少の問題があります。





## 第 36 章

# 複数の AP マネージャ インターフェイスの設定

- [複数の AP マネージャ インターフェイスについて, 383 ページ](#)
- [複数の AP マネージャ インターフェイス設定の制約事項, 384 ページ](#)
- [複数の AP マネージャ インターフェイスの作成 \(GUI\) , 384 ページ](#)
- [複数の AP マネージャ インターフェイスの作成 \(CLI\) , 385 ページ](#)

## 複数の AP マネージャ インターフェイスについて

複数の AP マネージャ インターフェイスを作成すると、インターフェイスはそれぞれ異なるポートにマッピングされます。AP マネージャ インターフェイス 2 がポート 2、AP マネージャ インターフェイス 3 がポート 3、AP マネージャ インターフェイス 4 がポート 4 となるように、ポートが順番に設定されている必要があります。

アクセス ポイントはコントローラに join する前に、discovery request を送信します。アクセス ポイントは、受信した discovery response から、コントローラにある AP マネージャ インターフェイスの数と、各 AP マネージャ インターフェイスにあるアクセス ポイントの数を判断します。アクセス ポイントは、通常、最もアクセス ポイント数の少ない AP マネージャに join します。この方法により、アクセス ポイントの負荷は、複数の AP マネージャ インターフェイスに対して動的に分散されます。



(注) アクセス ポイントは AP マネージャ インターフェイス全体に、均等に分散されるわけではありませんが、ある程度のロード バランシングは行われます。

## 複数の AP マネージャ インターフェイス設定の制約事項

次の制限は、コントローラに複数の AP マネージャ インターフェイスを設定するときに適用されます。

- コントローラ上の各ポートに、AP マネージャ インターフェイスを割り当てる必要があります。
- 複数の AP マネージャ インターフェイスを実装する前に、それらがコントローラのポート冗長性に与える影響を考慮する必要があります。
- 複数の AP マネージャ インターフェイスを使用できるのは、Cisco 5500 シリーズ コントローラだけです。
- すべての AP マネージャ インターフェイスが同じ VLAN または同じ IP サブネット上になくてもかまいません。また、管理インターフェイスと同じ VLAN または IP サブネットになくても問題はありません。ただし、すべての AP マネージャ インターフェイスが同一の VLAN または IP サブネット上に存在するように設定することをお勧めします。
- いずれかの AP マネージャ インターフェイスのポートで障害が発生した場合は、コントローラによってアクセスポイントの状態がクリアされるので、通常のコントローラ join プロセスを使用してコントローラとの通信を再確立するために、アクセスポイントのリポートが必要になります。この後、コントローラからの CAPWAP または LWAPP ディスカバリ応答には、障害を起こした AP マネージャ インターフェイスは含まれなくなります。アクセスポイントは再度コントローラに join し、アクセスポイントの負荷は使用可能な AP マネージャ インターフェイス間に分散されます。

## 複数の AP マネージャ インターフェイスの作成 (GUI)

**ステップ 1** [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。

**ステップ 2** [New] をクリックします。  
[Interfaces > New] ページが表示されます。

**ステップ 3** AP マネージャ インターフェイスの名前と VLAN 識別子を入力します。

**ステップ 4** [Apply] をクリックして、変更を確定します。[Interfaces > Edit] ページが表示されます。

**ステップ 5** 適切なインターフェイス パラメータを入力します。

(注) すべてのインターフェイスは、次の場合を除き、プライマリおよびバックアップポートをサポートします。

- 動的インターフェイスは、ポート設定のバックアップをサポートしない AP マネージャに変換されます。
- AP マネージャが管理インターフェイスで有効であり、管理インターフェイスがプライマリポート障害のためにバックアップポートに移動した場合、AP マネージャ インターフェイスは無効になります。

**ステップ 6** このインターフェイスを AP マネージャ インターフェイスにするには、[Enable Dynamic AP Management] チェックボックスをオンにします。

(注) 1つの物理ポートにつき、AP マネージャ インターフェイスは1つのみ許可されます。AP マネージャ インターフェイスとして指定された動的インターフェイスはWLAN インターフェイスとして使用できません。

**ステップ 7** [Save Configuration] をクリックして設定を保存します。

**ステップ 8** 作成する AP マネージャ インターフェイスそれぞれについて、この手順を繰り返します。

## 複数の AP マネージャ インターフェイスの作成 (CLI)

**ステップ 1** 次のコマンドを入力し、新しいインターフェイスを作成します。

- **config interface create** *operator\_defined\_interface\_name* {*vlan\_id* | *x*}
- **config interface address** *operator\_defined\_interface\_name* *ip\_addr* *ip\_netmask* [*gateway*]
- **config interface vlan** *operator\_defined\_interface\_name* {*vlan\_id* | *o*}
- **config interface port** *operator\_defined\_interface\_name* *physical\_ds* *port\_number*
- **config interface dhcp** *operator\_defined\_interface\_name* *ip\_address\_of\_primary\_dhcp\_server* [*ip\_address\_of\_secondary\_dhcp\_server*]
- **config interface quarantine vlan** *interface\_name* *vlan\_id*

(注) このコマンドを使用して、任意のインターフェイスに対して隔離 VLAN を設定します。
- **config interface acl** *operator\_defined\_interface\_name* *access\_control\_list\_name*

**ステップ 2** このインターフェイスを AP マネージャ インターフェイスにするには、次のコマンドを入力します。  
{**config interface ap-manager** *operator\_defined\_interface\_name* **enable** | **disable**}

(注) 1つの物理ポートにつき、AP マネージャ インターフェイスは1つのみ許可されます。AP マネージャ インターフェイスとして指定された動的インターフェイスはWLAN インターフェイスとして使用できません。

**ステップ 3** `save config` コマンドを入力して、変更を保存します。

**ステップ 4** 作成する AP マネージャ インターフェイスそれぞれについて、この手順を繰り返します。

---





# 第 37 章

## VLAN Select の設定

- [VLAN Select](#) について, 387 ページ
- [VLAN 選択の設定に関する制限](#), 388 ページ
- [インターフェイス グループの設定](#), 388 ページ

### VLAN Select について

無線クライアントが無線ネットワーク (WLAN) に接続すると、クライアントは、WLAN に関連付けられている VLAN に配置されます。講堂、競技場、会議場などといった大規模な会場では、大量の無線クライアントが使用される可能性があり、単一の WLAN だけで多数のクライアントに対応することは困難な場合があります。

VLAN Select 機能を使用すると、複数の VLAN をサポート可能な単一の WLAN を使用できるようになります。クライアントは、設定されている VLAN の 1 つに割り当てることができます。この機能を使用すれば、インターフェイス グループを使用して 1 つまたは複数のインターフェイスの VLAN に WLAN をマッピングすることができます。WLAN との関連付けを行うワイヤレスクライアントは、インターフェイスで特定されるサブネットのプールから IP アドレスを取得します。IP アドレスは、ワイヤレスクライアントの MAC アドレスをベースにしたアルゴリズムで生成されます。この機能は、現行の AP グループアーキテクチャも拡張しており、WLAN がマッピングされているインターフェイスまたはインターフェイスグループ (インターフェイスグループを使用した複数のインターフェイス) よりも AP グループを優先させることができます。さらにこの機能では、自動アンカー制限に対するソリューションも提供されており、外部ロケーションにいる無線ゲストユーザが、同じアンカーコントローラから、自分の外部ロケーションまたは外部コントローラに基づいて複数のサブネットのうちの 1 つの IP アドレスを取得できます。

クライアントがあるコントローラから別のコントローラにローミングすると、外部コントローラから、モビリティアナウンスメッセージの一部として VLAN 情報が送信されます。アンカーは、受信した VLAN 情報に基づいて、アンカーコントローラと外部コントローラ間でトンネルを構築する必要があるかどうかを決定します。外部コントローラで同一の VLAN を使用できる場合は、アンカーからクライアントコンテキストがすべて削除され、外部コントローラがクライアントに対する新しいアンカーコントローラとなります。

あるサブネットにあるインターフェイス (int-1) があるコントローラ (VLAN ID 0) にタグが付けられておらず、同じサブネットにあるインターフェイス (int-2) が他のコントローラ (Vlan ID 1) にタグ付けされている場合、VLAN Select を使用すると、このインターフェイスによって 1 台目のコントローラに join しているクライアントは、2 番目のコントローラに移動する間に L2 ローミングを受けることはありません。したがって、VLAN Select で 2 つのコントローラ間の L2 ローミングを発生させるには、同じサブネット内のすべてのインターフェイスがタグ付きまたはタグなしのいずれかに統一されている必要があります。

VLAN Select 機能の一部として、モビリティ アナウンス メッセージは追加のベンダー ペイロードを運びます。このペイロードには、外部コントローラの WLAN にマッピングされたインターフェイス グループ内の VLAN インターフェイスのリストが格納されています。アンカーは、この VLAN リストを使用して、ローカル間のハンドオフとローカルから外部へのハンドオフを区別できます。

## VLAN 選択の設定に関する制限

- VLAN Select 機能を使用すると、複数の VLAN をサポート可能な単一の WLAN を使用できるようにになります。

## インターフェイス グループの設定

### インターフェイス グループについて

インターフェイス グループは、インターフェイスの論理的なグループです。インターフェイス グループを使用すると、同じインターフェイス グループを複数の WLAN で設定するユーザ設定や、AP グループごとに WLAN インターフェイスを上書きすることが容易になります。インターフェイス グループには隔離済みまたは隔離済みでないインターフェイスを排他的に含めることができます。1 つのインターフェイスを複数のインターフェイス グループに含めることができます。

WLAN は、インターフェイスまたはインターフェイス グループに関連付けることができます。インターフェイス グループの名前とインターフェイスの名前を同じにすることはできません。

この機能を使用すると、クライアントを特定のサブネットに、そのサブネットが接続している外部コントローラに基づいて関連付けることができます。必要に応じて、外部コントローラの MAC と特定のインターフェイスまたはインターフェイス グループ (外部マップ) との間のマッピングを維持するように、アンカー コントローラ WLAN を設定できます。このマッピングが設定されていない場合は、その外部コントローラ上のクライアントは、WLAN に設定されているインターフェイス グループからラウンドロビン方式で VLAN を割り当てられます。

インターフェイス グループには AAA Override を設定することもできます。この機能では、現行のアクセス ポイント グループと AAA Override アーキテクチャが拡張され、アクセス ポイント グループと AAA Override が、インターフェイスがマッピングされているインターフェイス グループ WLAN よりも優先されるように設定できます。これは、インターフェイス グループを使用した複数のインターフェイスに対して行われます。

この機能により、ネットワーク管理者はゲストアンカー制限を設定できます。それにより、外部ロケーションにいる無線ゲストユーザは、同じアンカーコントローラ内から、外部ロケーションとコントローラ上の複数のサブネットのうちの1つのIPアドレスを取得できます。

## インターフェイスグループの設定に関する制限

- WALNにVLANインターフェイス選択を設定するときの優先順位は、次のようになります。
  - AAA Override
  - AP グループ
  - DHCP サーバのオーバーライド
  - インターフェイス グループ

## インターフェイスグループの作成 (GUI)

- 
- ステップ 1** [Controller] > [Interface Groups] を選択します。  
[Interface Groups] ページが表示され、すでに作成されているインターフェイスグループのリストが表示されます。
- (注) インターフェイスグループを削除するには、青のドロップダウンアイコンの上にマウスポインタを移動し、[Remove] を選択します。
- ステップ 2** [Add Group] をクリックします。  
[Add New Interface Group] ページが表示されます。
- ステップ 3** インターフェイスグループの詳細を入力します。
- [Interface Group Name] : インターフェイスグループの名前を指定します。
  - [Description] : インターフェイスグループの簡単な説明を入力します。
- ステップ 4** [Add] をクリックします。
- 

## インターフェイスグループの作成 (CLI)

- **config interface group {create | delete} interface\_group\_name** : インターフェイスグループを作成または削除します。
- **config interface group description interface\_group\_name description** : インターフェイスグループに説明を追加します。

## インターフェイスグループへのインターフェイスの追加（GUI）

- 
- ステップ 1** [Controller] > [Interface Groups] を選択します。  
[Interface Groups] ページが表示され、すべてのインターフェイスグループのリストが示されます。
- ステップ 2** インターフェイスを追加するインターフェイスグループの名前をクリックします。  
[Interface Groups > Edit] ページが表示されます。
- ステップ 3** このインターフェイスグループに追加するインターフェイスの名前を [Interface Name] ドロップダウンリストから選択します。
- ステップ 4** [Add Interface] をクリックして、インターフェイスをインターフェイスグループに追加します。
- ステップ 5** このインターフェイスグループに複数のインターフェイスを追加する場合は、ステップ 2～3 を繰り返します。  
(注) インターフェイスグループからインターフェイスを削除するには、青のドロップダウン矢印の上にマウスポインタを移動し、[Remove] を選択します。
- 

## インターフェイスグループへのインターフェイスの追加（CLI）

インターフェイスをインターフェイスグループに追加するには、**config interface group interface add interface\_group interface\_name** コマンドを使用します。

## インターフェイスグループ内の VLAN の表示（CLI）

インターフェイスグループ内の VLAN のリストを表示するには、**show interface group detailed interface-group-name** コマンドを使用します。

## WLAN へのインターフェイスグループの追加（GUI）

- 
- ステップ 1** [WLAN] タブを選択します。  
[WLANs] ページが表示され、使用可能な WLAN のリストが示されます。
- ステップ 2** インターフェイスグループを追加する WLAN の WLAN ID をクリックします。
- ステップ 3** [General] タブで、[Interface/Interface Group (G)] ドロップダウンリストからインターフェイスグループを選択します。
- ステップ 4** [Apply] をクリックします。

- (注) ユーザが WLAN に追加したインターフェイスグループで、RADIUS サーバ オーバーライドインターフェイスが有効になっているとします。この場合、クライアントが認証を要求すると、コントローラは RADIUS サーバとしてインターフェイスグループから最初の IP アドレスを選択します。
- 

## WLAN へのインターフェイスグループの追加 (CLI)

WLAN にインターフェイスグループを追加するには、**config wlan interface *wlan\_id* *interface\_group\_name*** コマンドを入力します。





## 第 38 章

# インターフェイス グループの設定

- [インターフェイス グループについて, 393 ページ](#)
- [インターフェイス グループの設定に関する制限, 394 ページ](#)
- [インターフェイス グループの作成 \(GUI\) , 394 ページ](#)
- [インターフェイス グループの作成 \(CLI\) , 395 ページ](#)
- [インターフェイス グループへのインターフェイスの追加 \(GUI\) , 395 ページ](#)
- [インターフェイス グループへのインターフェイスの追加 \(CLI\) , 395 ページ](#)
- [インターフェイス グループ内の VLAN の表示 \(CLI\) , 395 ページ](#)
- [WLAN へのインターフェイス グループの追加 \(GUI\) , 396 ページ](#)
- [WLAN へのインターフェイス グループの追加 \(CLI\) , 396 ページ](#)

## インターフェイス グループについて

インターフェイス グループは、インターフェイスの論理的なグループです。インターフェイス グループを使用すると、同じインターフェイス グループを複数の WLAN で設定するユーザ設定や、AP グループごとに WLAN インターフェイスを上書きすることが容易になります。インターフェイス グループには隔離済みまたは隔離済みでないインターフェイスを排他的に含めることができます。1つのインターフェイスを複数のインターフェイス グループに含めることができます。

WLAN は、インターフェイスまたはインターフェイス グループに関連付けることができます。インターフェイス グループの名前とインターフェイスの名前を同じにすることはできません。

この機能を使用すると、クライアントを特定のサブネットに、そのサブネットが接続している外部コントローラに基づいて関連付けることができます。必要に応じて、外部コントローラの MAC と特定のインターフェイスまたはインターフェイス グループ (外部マップ) との間のマッピングを維持するように、アンカー コントローラ WLAN を設定できます。このマッピングが設定されていない場合は、その外部コントローラ上のクライアントは、WLAN に設定されているインターフェイス グループからラウンドロビン方式で VLAN を割り当てられます。

インターフェイスグループには AAA Override を設定することもできます。この機能では、現行のアクセスポイントグループと AAA Override アーキテクチャが拡張され、アクセスポイントグループと AAA Override が、インターフェイスがマッピングされているインターフェイスグループ WLAN よりも優先されるように設定できます。これは、インターフェイスグループを使用した複数のインターフェイスに対して行われます。

この機能により、ネットワーク管理者はゲストアンカー制限を設定できます。それにより、外部ロケーションにいる無線ゲストユーザは、同じアンカーコントローラ内から、外部ロケーションとコントローラ上の複数のサブネットのうちの 1 つの IP アドレスを取得できます。

## インターフェイスグループの設定に関する制限

- WLAN に VLAN インターフェイス選択を設定するときの優先順位は、次のようになります。
  - AAA Override
  - AP グループ
  - DHCP サーバのオーバーライド
  - インターフェイスグループ

## インターフェイスグループの作成 (GUI)

**ステップ 1** [Controller] > [Interface Groups] を選択します。  
[Interface Groups] ページが表示され、すでに作成されているインターフェイスグループのリストが示されます。

(注) インターフェイスグループを削除するには、青のドロップダウンアイコンの上にマウスポインタを移動し、[Remove] を選択します。

**ステップ 2** [Add Group] をクリックします。  
[Add New Interface Group] ページが表示されます。

**ステップ 3** インターフェイスグループの詳細を入力します。

- [Interface Group Name] : インターフェイスグループの名前を指定します。
- [Description] : インターフェイスグループの簡単な説明を入力します。

**ステップ 4** [Add] をクリックします。



## インターフェイスグループの作成 (CLI)

- **config interface group {create | delete} interface\_group\_name** : インターフェイスグループを作成または削除します。
- **config interface group description interface\_group\_name description** : インターフェイスグループに説明を追加します。

## インターフェイスグループへのインターフェイスの追加 (GUI)

- 
- ステップ 1** [Controller] > [Interface Groups] を選択します。  
[Interface Groups] ページが表示され、すべてのインターフェイスグループのリストが示されます。
- ステップ 2** インターフェイスを追加するインターフェイスグループの名前をクリックします。  
[Interface Groups > Edit] ページが表示されます。
- ステップ 3** このインターフェイスグループに追加するインターフェイスの名前を [Interface Name] ドロップダウンリストから選択します。
- ステップ 4** [Add Interface] をクリックして、インターフェイスをインターフェイスグループに追加します。
- ステップ 5** このインターフェイスグループに複数のインターフェイスを追加する場合は、ステップ 2～3 を繰り返します。  
(注) インターフェイスグループからインターフェイスを削除するには、青のドロップダウン矢印の上にマウスポインタを移動し、[Remove] を選択します。
- 

## インターフェイスグループへのインターフェイスの追加 (CLI)

インターフェイスをインターフェイスグループに追加するには、**config interface group interface add interface\_group interface\_name** コマンドを使用します。

## インターフェイスグループ内の VLAN の表示 (CLI)

インターフェイスグループ内の VLAN のリストを表示するには、**show interface group detailed interface-group-name** コマンドを使用します。

## WLAN へのインターフェイス グループの追加 (GUI)

---

- ステップ 1 [WLAN] タブを選択します。  
[WLANs] ページが表示され、使用可能な WLAN のリストが示されます。
- ステップ 2 インターフェイス グループを追加する WLAN の WLAN ID をクリックします。
- ステップ 3 [General] タブで、[Interface/Interface Group (G)] ドロップダウン リストからインターフェイス グループを選択します。
- ステップ 4 [Apply] をクリックします。  
(注) ユーザが WLAN に追加したインターフェイス グループで、RADIUS サーバオーバーライドインターフェイスが有効になっているとします。この場合、クライアントが認証を要求すると、コントローラは RADIUS サーバとしてインターフェイス グループから最初の IP アドレスを選択します。
- 

## WLAN へのインターフェイス グループの追加 (CLI)

WLAN にインターフェイス グループを追加するには、**config wlan interface wlan\_id interface\_group\_name** コマンドを入力します。



## 第 39 章

# マルチキャストの最適化の設定

- [マルチキャスト最適化について, 397 ページ](#)
- [マルチキャスト VLAN の設定 \(GUI\) , 398 ページ](#)
- [マルチキャスト VLAN の設定 \(CLI\) , 398 ページ](#)

## マルチキャスト最適化について

7.0.116.0 よりも前のリリースでは、マルチキャストは、マルチキャストアドレスと VLAN を 1 つのエンティティ (MGID) としてグループ化することを基本としていました。VLAN Select と VLAN プーリングが使用されると、重複パケットが増加する可能性があります。VLAN Select 機能では、すべてのクライアントがそれぞれ異なる VLAN 上でマルチキャストストリームをリッスンします。そのため、コントローラは、マルチキャストアドレスと VLAN の組み合わせごとに異なる MGID を作成します。その結果、アップストリームルータは VLAN ごとにコピーを 1 つ送信し、最悪の場合、プール内に存在する VLAN の数だけコピーが作成されます。WLAN はすべてのクライアントに対して同じままなので、マルチキャストパケットの複数のコピーが無線で送信されます。無線メディア上およびコントローラとアクセスポイントの間に発生する重複したマルチキャストストリームを抑制するには、マルチキャスト最適化機能を使用できます。

マルチキャスト最適化では、マルチキャストトラフィック用に使用可能なマルチキャスト VLAN を作成できます。WLAN の VLAN の 1 つを、マルチキャストグループが登録されるマルチキャスト VLAN として設定できます。クライアントは、マルチキャスト VLAN 上でマルチキャストストリームをリッスンできます。MGID は、マルチキャスト VLAN とマルチキャスト IP アドレスを使用して生成されます。同じ WLAN の VLAN プール上にある複数のクライアントが単一のマルチキャスト IP アドレスをリッスンしている場合、単一の MGID が生成されます。コントローラは、この VLAN プール上のクライアントからのすべてのマルチキャストストリームが常にマルチキャスト VLAN 上に送られるようにして、その VLAN プールのすべての VLAN に対し、アップストリームルータに登録されるエントリが 1 つになるようにします。クライアントが異なる VLAN 上にあっても、1 つのマルチキャストストリームだけが VLAN プールにヒットします。したがって、無線で送信されるマルチキャストパケットは、1 つのストリームだけになります。

## マルチキャスト VLAN の設定 (GUI)

---

- ステップ1 [WLANs] > [WLAN ID] を選択します。 [WLAN > Edit] ページが表示されます。
- ステップ2 [General] タブで [Multicast VLAN feature] チェックボックスを選択して、WLAN に対してマルチキャスト VLAN を有効にします。  
[Multicast Interface] ドロップダウン リストが表示されます。
- ステップ3 [Multicast Interface] ドロップダウン リストから VLAN を選択します。
- ステップ4 [Apply] をクリックします。
- 

## マルチキャスト VLAN の設定 (CLI)

`config wlan multicast interface wlan_id enable interface_name` コマンドを使用して、マルチキャスト VLAN 機能を設定します。



## 第 40 章

# ハイアベイラビリティの設定

- [ハイアベイラビリティに関する情報, 399 ページ](#)
- [ハイアベイラビリティの制約事項, 403 ページ](#)
- [ハイアベイラビリティ \(GUI\) の設定, 407 ページ](#)
- [ハイアベイラビリティ \(CLI\) の設定, 408 ページ](#)

## ハイアベイラビリティに関する情報

コントローラのハイアベイラビリティ (HA) によって、コントローラのフェールオーバーで生じる無線ネットワークのダウンタイムを短縮することができます。

1:1 (アクティブ : スタンバイホット) のアクセスポイントステートフルスイッチオーバー (AP SSO) がサポートされています。HA アーキテクチャでは、1 台のコントローラはプライマリ コントローラとして、別のコントローラはセカンダリ コントローラとして設定されています。

HA を有効にした後、プライマリおよびセカンダリ コントローラがリブートされます。ブートプロセス中に、プライマリコントローラのロールはアクティブとして、セカンダリコントローラのロールはスタンバイホットとしてネゴシエートされます。スイッチオーバー後、セカンダリ コントローラは、アクティブ コントローラになり、プライマリ コントローラがスタンバイホット コントローラになります。それ以降の切り替えの後、ロールは、プライマリおよびセカンダリ コントローラ間で交換されます。スイッチオーバーの原因は、手動トリガー、またはコントローラやネットワークの障害のいずれかです。

APSSO 中に、すべての AP セッションはステートフルにスイッチオーバーして、FlexConnect モードでローカルに切り替えられたクライアントを除くすべてのクライアントは認証解除され、新しいアクティブ コントローラに再アソシエートされます。

スタンバイホットコントローラは、専用のリダンダンシーポートに有線で直接接続したアクティブコントローラの状態を連続してモニタします。両方のコントローラは管理インターフェイスの IP アドレスを含め、同じ設定を共有します。

HA を有効にする前に、両方のコントローラがイーサネット ケーブルを使用して、冗長ポート経由で物理的に接続されていることを確認します。また、アップリンクがインフラストラクチャスイッチに接続され、ゲートウェイが両方のコントローラから到達可能であることを確認します。

HA アーキテクチャでは、リダンダンシー ポートおよびリダンダンシー マネジメント インターフェイスが新しく導入されました。

アクティブコントローラからスタンバイコントローラへのクライアントのシームレスな移行もサポートされます。実行状態にないクライアントはスイッチオーバー後に削除されます。クライアントのステートフルスイッチオーバー中（クライアント SSO）に、クライアントがコントローラに関連付けられている、または設定されている場合、クライアントの情報がスタンバイ コントローラと同期されます。完全に認証されたクライアント、つまり、実行状態にあるクライアントはピアコントローラと同期されます。クライアントのデータ構造は、クライアントの状態に基づいて同期されます。過渡状態にあるクライアントは、スイッチオーバー後にアソシエーションが解除されます。

次に、ハイ アベイラビリティに関する注意事項を示します。

- 異なるハードウェア モデルの 2 台のコントローラを組み合わせないことを推奨します。それらを組み合わせると、より優先順位が高いコントローラ モデルはアクティブ コントローラになり、他のコントローラはメンテナンス モードになります。
- コントローラ ソフトウェア リリースの異なる 2 台のコントローラを組み合わせないことを推奨します。それらを組み合わせると、優先順位のより低いリダンダンシー マネジメント アドレスを持つコントローラは、アクティブコントローラになり、他のコントローラはメンテナンス モードになります。
- イメージ、設定、Web 認証バンドル、およびシグニチャ ファイルなど、ダウンロードしたファイルタイプはすべて、アクティブ コントローラで最初にダウンロードされてから、スタンバイホット コントローラにプッシュされます。
- 組み合わせる前に、証明書を各コントローラに個別にダウンロードする必要があります。
- アクティブ コントローラの GUI または CLI を使用して、設定、イベント ログ、クラッシュ ファイルなどの、ファイルタイプをスタンバイホット コントローラからアップロードできます。また、ファイル名にアップロードされたファイルを識別するサフィックスを指定できます。
- ピアアップロードを実行するには、サービスポートを使用します。管理ネットワークでは、管理 VLAN と同様に、リダンダンシー ポートまたは RMI VLAN、もしくはその両方にマッピングされたリダンダンシー マネジメント インターフェイス（RMI）を使用することもできます。RMI および RP が 2 つの異なる L2 VLAN にあることに注意してください。これは必須設定です。
- コントローラが冗長ポートおよび RMI を介して相互に接続できない場合、プライマリ コントローラがアクティブになり、スタンバイホット コントローラはメンテナンス モードになります。



(注) 2つの Cisco WiSM2 プラットフォーム間の HA を実現するには、複数のシャーシ間で仮想スイッチング システム (VSS) を使用してリダンダンシー VLAN を拡張することで、コントローラを単一シャーシまたは複数のシャーシで展開する必要があります。



(注) リダンダンシー VLAN は非ルーティング VLAN にする必要があります。その場合、レイヤ 3 インターフェイスは VLAN に作成するべきではなく、複数のシャーシ間の HA 設定を展開するように、インターフェイスがトランク ポートで許可できるようにします。リダンダンシー VLAN は、他のデータ VLAN 同様に Cisco IOS ベースのスイッチング ソフトウェアで作成する必要があります。リダンダンシー VLAN は、バックプレーン経由でシスコ WiSM2 の冗長ポートに接続されます。IP アドレスが自動的に生成されるため、リダンダンシー VLAN の IP アドレスを設定する必要はありません。また、リダンダンシー VLAN が管理 VLAN と同じではないことを確認します。



(注) 組み合わせている 2 台のコントローラの RMI (同じ VLAN にマッピングされ、同じレイヤ 3 スイッチに接続されている) が動作を停止すると、スタンバイコントローラが再起動されます。

- HA が有効な場合、スタンバイ コントローラは常にリダンダンシー マネジメント インターフェイス (RMI) を使用します。他のすべてのインターフェイス (ダイナミック、および管理) は無効です。ping は発信元としてリダンダンシー マネジメント インターフェイス (RMI) のみを受理する必要があり、その他のインターフェイスは受け取りません。
- HA が有効な場合、バックアップされたイメージを使用しないでください。このイメージが使用されると、HA 機能が想定どおりに機能しない可能性があります。
  - SSO をイネーブルにすると、設定されているサービス ポートとルート情報が失われます。SSO をイネーブルにした後は、サービス ポートとルート情報を再設定する必要があります。peer-service-port および peer-route コマンドを使用して、スタンバイホットコントローラのサービス ポートとルート情報を設定できます。
  - Cisco WiSM2 については、冗長性をイネーブルにした後、サービスポートの再設定が必要です。そうしないと、Cisco WiSM2 はスーパーバイザと通信できない場合があります。冗長性をイネーブルにする前に、サービス ポートで DHCP を有効にすることを推奨します。
  - スタンバイホット コントローラで reset コマンドを直接使用しないことを推奨します。これを使用すると、保存されていない設定は失われます。
- インフラストラクチャ スイッチのポート チャネルをイネーブルにする前に、コントローラのリンク集約 (LAG) の設定をイネーブルにすることを推奨します。

- アクティブコントローラのリブートが必要なすべての設定により、結果として、スタンバイホットコントローラがリブートされます
- [Ignore AP] リストでは、アクティブコントローラからスタンバイホットコントローラに同期されません。リストは、スタンバイホットコントローラがアクティブになると、Cisco Prime Infrastructure の SNMP メッセージを通じて再学習されます。
- クライアント SSO 関連の注意事項
  - スタンバイコントローラは2つのクライアントリストを保持します。実行状態のクライアントのリストおよび他のすべての状態である一時的なクライアントのリストです。
  - 実行状態にあるクライアントのみがフェールオーバー中に保持されます。ローミング、802.1X キーの再生成、Web 認証のログアウトなどの過渡状態にあるクライアントのアソシエーションは解除されます。
  - AP SSO と同様に、クライアント SSO は WLAN でのみサポートされます。コントローラは、同じサブネット内にある必要があります。L3 接続はサポートされません。
- リリース 7.3.x では AP SSO はサポートされますが、クライアント SSO はサポートされていないため、リリース 7.3.x を使用する HA セットアップでスイッチオーバーが発生した後で、Cisco WLC に関連付けられているすべてのクライアントは認証解除され、再アソシエーションを要求されます。
- ピアコントローラにリリース 7.2 以前のコントローラソフトウェアリリースがある場合、スイッチオーバー後のアクティブコントローラにモビリティ MAC アドレスを設定する必要があります。

### リダンダンシー マネジメント インターフェイス

アクティブおよびスタンバイホットコントローラでは、リダンダンシー マネジメント インターフェイスを使用して、ネットワーク インフラストラクチャを介して管理インターフェイスのピアコントローラおよびデフォルトゲートウェイの健全性をチェックします。

また、障害が発生または手動でリセットした場合に、リダンダンシー マネジメント インターフェイスがアクティブコントローラからスタンバイホットコントローラに通知を送信するために使用されます。スタンバイホットコントローラは、Syslog、NTP、FTP および TFTP サーバと通信するためにリダンダンシー マネジメント インターフェイスを使用します。

プライマリコントローラおよびセカンダリコントローラの両方で同じサブネット内のリダンダンシー マネジメント インターフェイスおよび管理インターフェイスの IP アドレスを設定する必要があります。

### リダンダンシー ポート

リダンダンシーポートは、設定、動作データの同期、プライマリおよびセカンダリコントローラ間のロールネゴシエーションに使用されます。

リダンダンシーポートは、スタンバイホットコントローラからアクティブコントローラに 100 ミリ秒ごとに（デフォルトの頻度）UDP キープアライブメッセージを送信することによってピア



の到達可能性を確認します。アクティブコントローラの障害が発生した場合、リダンダンシーポートがスタンバイホットコントローラを通知するために使用されます。

NTPサーバが設定されていない場合、リダンダンシーポートがアクティブコントローラからスタンバイホットコントローラに時刻同期を行います。

Cisco WiSM2 では、利用可能な物理リダンダンシーポートがないため、リダンダンシー VLAN を Cisco Catalyst 6000 スーパーバイザ エンジンで設定する必要があります。

Cisco WiSM2 のリダンダンシーポートおよびリダンダンシー VLAN には、最後の 2 オクテットがリダンダンシー マネジメント インターフェイスの最後の 2 オクテットから取得され、自動的に生成された IP アドレスが割り当てられます。最初の 2 オクテットは常に 169.254 です。たとえば、リダンダンシー マネジメント インターフェイスの IP アドレスが 209.165.200.225 の場合、リダンダンシーポートの IP アドレスは 169.254.200.225 です。

リダンダンシーポートは L2 スイッチを介して接続できます。リダンダンシーポートのラウンドトリップ時間は、キープアライブ タイマーがデフォルトの 100 ミリ秒に設定されている場合は 80 ミリ秒未満、キープアライブ タイマーが 100 ミリ秒～400 ミリ秒の範囲に設定されている場合はキープアライブ タイマーの 80% にしてください。たとえば、キープアライブ タイマーが 100 ミリ秒に設定されている場合、障害検出時間は次のように計算されます： $3 * 100 = 300 + 60 = 360 +$ ジッタ (12 ミリ秒) = ～400 ミリ秒。リダンダンシーポート間の帯域幅が 60 Mbps 以上であることを確認します。最大伝送単位 (MTU) が 1500 バイト以上であることを確認します。

### 暗号化のサポート

アクティブおよびスタンバイコントローラ間の HA 関連メッセージの暗号化は、Data Transport Layer Security (DTLS) の使用でサポートされています。暗号化は、デフォルトで無効になっています。暗号化は、設定、AP とクライアントの同期化でサポートされています。

暗号化は、アクティブおよびスタンバイコントローラが管理ポートのリダンダンシー インターフェイス経由で通信する場合にのみサポートされます。暗号化は、リダンダンシーポートがアクティブコントローラとスタンバイコントローラ間の通信に使用される場合はサポートされません。ただし、リダンダンシーポートにマッピングされたリダンダンシー マネジメント インターフェイスはデフォルトのオプションです。リダンダンシー マネジメント インターフェイスがリダンダンシーポートにマッピングされていない場合、HA 情報がネットワークに送信されるので、暗号化が有効になります。

暗号化が 1 台のコントローラで有効になっており、他方で無効の場合、コントローラはペアになりますが、冗長リンクによるデータ同期は暗号化されません。暗号化は、設定および AP とクライアントの同期化でサポートされています。ロールネゴシエーションとキープアライブメッセージは暗号化されません。

## ハイアベイラビリティの制約事項

- HA SSO 用にコントローラを設定した場合、Cisco 600 シリーズ OfficeExtend アクセス ポイントはサポートされません。
- HA 環境で FlexConnect のローカルにスイッチされるクライアントを使用すると、クライアント情報にユーザ名が表示されない場合があります。クライアントの詳細を取得するには、ク

クライアントのMACアドレスを使用する必要があります。この制限は、FlexConnectの中央でスイッチされるクライアントまたは中央（ローカル）モードのクライアントには適用されません。

- HA を有効にしている場合は、サービス インターフェイスを介して Cisco WiSM-2 GUI にアクセスすることはできません。回避策は、HA が確立された後に、サービス ポート インターフェイスを再作成することです。
- HA 環境では、LDPE イメージから LDPE 以外のイメージへのアップグレードはサポートされていません。
- 2 台のプライマリ コントローラまたは 2 台のセカンダリ コントローラを組み合わせることはできません。
- スタンバイ コントローラは AP に接続されたスイッチ ポートでは利用できません。
- 評価ライセンスを持つ HA-SKU コントローラをスタンバイ コントローラにすることはできません。ただし、ゼロ ライセンスを持つ HA-SKU コントローラはスタンバイ コントローラにすることができます。
- HA モードから HA 以外のモード、またはその逆に移行すると、サービス VLAN 設定が失われます。再度サービス IP アドレスを手動で設定する必要があります。
- プライマリ コントローラの管理アドレスとリダンダンシー マネジメント アドレスが同じ VLAN 上であって、プライマリ コントローラと同じ VLAN 上にセカンダリ コントローラの管理アドレスがあり、別の VLAN にそのリダンダンシー マネジメント アドレスがあるというシナリオはサポートされていません。
- 次に、ソフトウェア アップグレードのシナリオの一覧を示します。
  - アクティブ コントローラのソフトウェア アップグレードでは、スタンバイホット コントローラのアップグレードを確認します。
  - インサーブアップグレードはサポートされません。このため、HA 環境でコントローラをアップグレードする前に、ネットワークのダウン タイムを計画する必要があります。
  - ソフトウェア アップグレード後のアクティブ コントローラをリブートすると、スタンバイホット コントローラもリブートします。
  - アクティブおよびスタンバイ ホット コントローラの両方のバックアップに異なるソフトウェア リリースがある場合、アクティブ コントローラで **config boot backup** コマンドを入力すると、両方のコントローラがそれぞれのバックアップ イメージでリブートされて、ソフトウェアの不一致により HA ペアが切断されます。
  - スケジュール リセットが HA 環境の両方のコントローラに適用されます。アクティブ コントローラで期限切れになるスケジュール時刻の 1 分前にピア コントローラがリブートします。
  - リセットがスケジュールされていない場合、**reset peer-system** コマンドを入力して、アクティブ コントローラからスタンバイホット コントローラをリブートできます。このコマンドでスタンバイホット コントローラのみをリセットすると、スタンバイホット

コントローラの未保存の設定はすべて失われます。そのため、スタンバイホットコントローラをリセットする前に、アクティブコントローラ上で設定を保存する必要があります。

- プリイメージダウンロードは、SSO がイメージの転送時にトリガーされると再起動されます。
- **debug** コマンドおよび **show** コマンドだけが、スタンバイホットコントローラで許可されます。
- スイッチオーバー後、ピアコントローラにリリース7.5以前のコントローラソフトウェアリリースがある場合、すべてのモビリティクライアントが認証解除されます。
- コントローラ GUI、Cisco Prime Infrastructure、または Telnet 経由でスタンバイホットコントローラにアクセスすることはできません。コンソールでのみスタンバイホットコントローラにアクセスできます。
- フェールオーバーが発生時した場合、正常なスイッチオーバーのために、SSO では、スタンバイコントローラはスタンバイホット状態、冗長ポートはターミナル状態である必要があります。
- LAG を有効または無効にするには、HA を無効にする必要があります。



(注) LAG が無効になっていて、プライマリおよびバックアップポートの両方が管理インターフェイスに接続されている場合、プライマリポートが動作不能になると、デフォルトゲートウェイに到達できずにバックアップポートのフェールオーバーが 12 秒を超える可能性があるため、スイッチオーバーが発生することがあります。

- HA SSO 設定で LAG が有効になっており、2つのポートがプライマリおよびセカンダリコントローラの両方に接続されている場合、アクティブコントローラで1つのスイッチポートが動作不能になると、スイッチオーバーが発生します。リダンダンシーマネジメントインターフェイスが DP にマッピングされている場合に、いずれかのポートの動作不能が 300 ミリ秒を超えると、SSO が発生します。これは、LAG のコンバージェンスが約 5 秒かかるためです。
- フェールオーバーが発生し、スタンバイコントローラが新しいアクティブコントローラになる場合、2台のコントローラ間のデータベースの同期 (AP、クライアントおよびマルチキャスト) に約 15 ~ 20 分かかります。新たにフェールオーバーがこの時間内に発生した場合、HA の構造が同期されることはありません。したがって、AP およびクライアントを再アソシエートして、個別に再認証する必要があります。
- Pairwise Master Key (PMK) キャッシュの同期は FlexConnect のローカル認証クライアントではサポートされません。
- クライアント SSO の制限
  - 新しいモビリティはサポートされていません。

- ポスチャおよびネットワーク アドミッション コントロールアウトオブバンドは、クライアントが実行状態にないため、サポートされません。
- 次の内容は、アクティブ コントローラとスタンバイ コントローラの間で同期されません。
  - Cisco Compatible Extensions ベースのアプリケーション
  - クライアントの統計
  - プロキシ モバイル IPv6、Application Visibility and Control、セッション開始プロトコル (SIP)、およびスタティック コール アドミッション制御 (CAC) ツリー
  - ワークグループブリッジおよびその関連クライアント
  - Cisco 600 シリーズ OfficeExtend アクセス ポイントに関連付けられたクライアント
  - パッシブ クライアント
- 暗号化はサポートされています。
- 暗号化は、アクティブおよびスタンバイのコントローラが管理ポートのリダンダンシー管理インターフェイス経由で通信する場合のみサポートされます。暗号化は、リダンダンシーポートがアクティブ コントローラとスタンバイ コントローラ間の通信に使用される場合はサポートされません。
- コントローラがリダンダンシー モードの場合、管理インターフェイスの NAT アドレスの設定は変更できません。管理インターフェイスで NAT アドレス設定を有効にするには、最初に冗長構成を削除する必要があります。プライマリ コントローラで必要な変更を行ってから、同じコントローラで冗長構成を再度有効にします。
- Cisco WiSM2 および Cisco Catalyst 6500 シリーズ Supervisor Engine 2T では、HA が有効になっている場合、スイッチオーバー後に AP は接続を解除して WiSM2 コントローラと再アソシエートする可能性があります。この問題の発生を防ぐために、HA を設定する前に、ポートチャンネルでアクティブおよびスタンバイの両方の Cisco WiSM2 コントローラの詳細（ポートが同じ順序に保たれていて、ポートチャンネルハッシュ分散で固定アルゴリズムが使用されている）を確認することをお勧めします。これらが適切でない場合、ポートチャンネル分散を訂正し、Cisco Catalyst 6500 シリーズ Supervisor Engine 2T から Cisco WiSM2 をリセットする必要があります。
- SSO を有効にしてから、スタンバイおよびアクティブの両方のコントローラにアクセスするには、次を使用します。
  - コンソール接続
  - サービス ポートの SSH 機能
  - リダンダンシー マネジメント インターフェイスの SSH 機能



(注) SSO が有効な場合、Web UI/Telnet 機能を使用しても、サービスポートの Cisco Prime Infrastructure/Prime NCS を使用しても、スタンバイおよびアクティブの両方のコントローラにアクセスすることはできません。

- コントローラのスイッチオーバー後に、子メッシュ アクセス ポイント (MAP) とともに、クライアントは接続を解除されて新しいアクティブ コントローラに再 join されます。メッシュ ツリー全体が再構築されます。ルート アクセス ポイント (RAP) のクライアントも接続を解除されますが、RAP はコントローラと共にそのまま残ります。

## ハイアベイラビリティ (GUI) の設定

### はじめる前に

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。  
[Controllers]>[Interfaces] を選択し、管理インターフェイスの IP アドレスを表示して、両方のコントローラの GUI でこれを確認できます。

- ステップ 1** 両方のコントローラの GUI で、[Controller]>[Redundancy]>[Global Configuration] を選択します。  
[Global Configuration] ページが表示されます。
- ステップ 2** [Redundant Management IP] および [Peer Redundant Management IP] テキスト ボックスに両方のコントローラのアドレスを入力します。  
1 台のコントローラのリダンダンシー マネジメント インターフェイス IP アドレスがピア コントローラのリダンダンシー マネジメント インターフェイス IP アドレスと同じであることを確認します。
- ステップ 3** [Redundant Unit] ドロップダウン リストで、コントローラの 1 つをプライマリとして、他のコントローラをセカンダリとして選択します。
- ステップ 4** 両方のコントローラの GUI で、[SSO] を Enabled 状態に設定します。  
SSO をイネーブルにすると、サービスポートのピア IP アドレス、およびサービスポートのネットマスクが設定ページに表示されます。HA ピアが使用可能で稼働している場合、サービスポートのピア IP アドレスとネットマスクがピアのみにプッシュできることに注意してください。HA をイネーブルにすると、サービスポートのピア IP アドレスおよびサービスポートのネットマスク パラメータを設定する必要はありません。HA ピアが使用可能で稼働している場合、パラメータを設定する必要があります。SSO をイネーブルにした後、両方のコントローラがリブートされます。リブートプロセス中に、コントローラは設定に基づいて冗長ポートを介して冗長ロールをネゴシエートします。プライマリ コントローラは、アクティブ コントローラになり、セカンダリ コントローラがスタンバイ コントローラになります。
- ステップ 5** (任意) HA ペアが使用可能および動作可能になると、サービスポートがスタティックに設定されている場合にピアサービスポートの IP アドレスおよびネットマスクを設定できます。サービスポートの DHCP をイネーブルにすると、[Global Configuration] ページで次のパラメータを設定する必要はありません。
- Service Port Peer IP : ピア コントローラのサービスポートの IP アドレス。

- **Service Port Peer Netmask** : ピア コントローラのサービス ポートのネットマスク。
- **Mobility MAC Address** : モビリティ プロトコルで使用されるアクティブ コントローラとスタンバイ コントローラの共通 MAC アドレス。 HA ペアをモビリティ グループのモビリティ メンバとして追加する場合は、モビリティ MAC アドレスを (アクティブまたはスタンバイ コントローラのシステム MAC アドレスの代わりに) 使用する必要があります。通常、モビリティ MAC アドレスはアクティブ コントローラの MAC アドレスとして選択されるため、手動で設定する必要はありません。
- **Keep Alive Timer** : スタンバイ コントローラがアクティブ コントローラにハートビート キープアライブ メッセージを送信する頻度を制御するタイマー。有効範囲は 100 ~ 400 ミリ秒の 50 の倍数です。
- **Peer Search Timer** : アクティブ コントローラがスタンバイ コントローラにピア検索メッセージを送信する頻度を制御するタイマー。有効な範囲は 60 ~ 180 秒です。

HA をイネーブルにし、コントローラを組み合わせると、管理ポートを通じて HA ペアを管理する統合 GUI が 1 種類のみになります。サービスポートを通過する GUI へのアクセスは、アクティブ コントローラとスタンバイ コントローラのいずれでも実行できません。スタンバイ コントローラは、コンソールまたはサービスポートを介してのみ、管理できます。

Telnet および SSH セッションだけが、アクティブ コントローラとスタンバイ コントローラのサービスポート経由で許可されます。

**ステップ 6** [Apply] をクリックします。

**ステップ 7** [Save Configuration] をクリックします。

**ステップ 8** [Monitor] > [Redundancy] > [Summary] を選択し、HA ペアの冗長ステータスを表示します。  
[Redundancy Summary] ページが表示されます。

**ステップ 9** 次の手順に従って、ピア ネットワーク ルートを設定します。

- a) [Controller] > [Redundancy] > [Peer Network Route] を選択します。  
[Network Routes Peer] ページが表示されます。

このページでは、異なるサブネット上のネットワークまたは要素管理システムへの、ピア コントローラの既存のサービスポート ネットワーク ルートの概要を示します。IP アドレス、IP ネットマスク、またはゲートウェイ IP アドレスを表示できます。

- b) 新しいピア ネットワーク ルートを作成するには、[New] をクリックします。
- c) ルートの IP アドレス、IP ネットマスク、およびゲートウェイ IP アドレスを入力します。
- d) [Apply] をクリックします。

## ハイアベイラビリティ (CLI) の設定

はじめる前に

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。

- 次のコマンドを入力して、ローカルリダンダンシー IP アドレスおよびピアリダンダンシー マネジメント IP アドレスを設定します。  
**config interface address redundancy-management ip-addr1 peer-redundancy-management ip-addr2**
- 次のコマンドを入力して、コントローラのロールを設定します。  
**config redundancy unit {primary | secondary}**
- 次のコマンドを入力して、冗長モードを設定します。  
**config redundancy mode {sso | none}**  
両方のコントローラはリブートし、次にアクティブおよびスタンバイホットコントローラのロールをネゴシエートします。
- 次のコマンドを入力して、冗長性を設定します。  
**config redundancy mode {sso {ap | client} | disable}**  
AP SSO とクライアント SSO を選択できます。
- 次のコマンドを入力して、スタンバイコントローラのルート設定を設定します。  
**config redundancy peer-route {add network-ip-addr ip-mask | delete network-ip-addr}**  
このコマンドは HA ピアコントローラが使用可能であり、正常に動作している場合だけ実行できます。
- 次のコマンドを入力して、モビリティの MAC アドレスを設定します。  
**config redundancy mobilitymac mac-addr**  
このコマンドは、SSO が無効になっている場合にだけ実行できます。
- 次のコマンドを入力して、スタンバイピアコントローラのピアサービスポートの IP アドレスとネットマスクを設定します。  
**config redundancy interface address peer-service-port ip-address netmask**  
このコマンドは HA ピアコントローラが使用可能であり、正常に動作している場合だけ実行できます。
- 次のコマンドを入力して、手動スイッチオーバーを開始します。  
**config redundancy force-switchover**  
手動スイッチオーバーが必要な場合のみこのコマンドを実行します。
- 次のコマンドを入力して、リダンダンシータイマーを設定します。  
**config redundancy timer {keep-alive-timer time-in-milliseconds | peer-search-timer time-in-seconds}**
- 次のコマンドを入力して、コントローラ間の通信の暗号化を設定します。  
**config redundancy link-encryption {enable | disable}**
- 次のコマンドを入力して、ハッシュ分散を固定に設定します。  
トラブルシューティングのヒント  
**config port-channel hash-distribution fixed**
- 次のコマンドを入力して、ポートチャネルメンバーの順序および負荷値を確認します。  
トラブルシューティングのヒント  
**show etherchannel port-channel**
- 次のコマンドを入力して、冗長ステータスを表示します。

**show redundancy summary**

- 次のコマンドを入力して、リダンダンシー マネジメント インターフェイスに関する情報を表示します。

**show interface detailed redundancy-management**

- 次のコマンドを入力して、リダンダンシー ポートに関する情報を表示します。

**show interface detailed redundancy-port**

- 次のコマンドを入力して、ピア コントローラをリブートします。

**reset peer-system**

- アクティブ コントローラで次のコマンドを入力して、スタンバイホット コントローラから、設定、イベント ログ、クラッシュ ファイルなどのファイル タイプのアップロードを開始します。

**transfer upload peer-start**

- 次のコマンドを入力して、リダンダンシー マネージャのコマンドをデバッグします。

**debug rmgr {packet | events | errors | detail}**

- 次のコマンドを入力して、リダンダンシー 同期マネージャのコマンドをデバッグします。

**debug rsyncmgr {packet | events | errors | detail}**

- 次のコマンドを入力して、リダンダンシー ファシリテータのコマンドをデバッグします。

**debug rfrac {packet | events | errors | detail}**





第 **III** 部

## VideoStream の設定

- [VideoStream の設定, 413 ページ](#)





## 第 41 章

# VideoStream の設定

---

- [VideoStream について](#), 413 ページ
- [VideoStream の前提条件](#), 413 ページ
- [VideoStream の設定に関する制限](#), 414 ページ
- [VideoStream の設定 \(GUI\)](#), 414 ページ
- [VideoStream の設定 \(CLI\)](#), 418 ページ
- [メディア ストリームの表示とデバッグ](#), 419 ページ

## VideoStream について

IEEE 802.11 ワイヤレスマルチキャスト配信メカニズムには、パケットの消失や破損を認識するための、信頼できる方法がありません。結果として、無線配信中にマルチキャストパケットが消失しても再送されないため、IP マルチキャスト ストリームが表示できなくなることがあります。

VideoStream 機能では、無線でマルチキャストフレームをユニキャスト ストリームに無線で変換することで、IP マルチキャスト ストリームの無線配信を信頼できるものにします。VideoStream クライアントは、それぞれビデオ IP マルチキャスト ストリームの受信を認識します。

## VideoStream の前提条件

マルチキャスト機能が有効であることを確認します。コントローラ上の IP マルチキャストは `multicast-multicast` モードで設定することをお勧めします。

クライアントマシン上の IP アドレスを確認します。マシンには、それぞれの VLAN の IP アドレスが必要です。

アクセス ポイントがコントローラに join していることを確認します。

クライアントが 802.11n の速度で設定された WLAN に関連づけられることを確認します。

## VideoStream の設定に関する制限

VideoStream は、7.0.98.0 以降のコントローラ ソフトウェア リリースでサポートされます。

VideoStream は、Cisco Aironet 3600、3500、1260、1250、1240、1140、1130、および 1040 のアクセス ポイントでサポートされています。

## VideoStream の設定 (GUI)

**ステップ 1** 次の手順に従って、マルチキャスト機能を設定します。

- a) [Wireless] > [MediaStream] > [General] を選択します。
- b) [Multicast Direct feature] チェックボックスをオンまたはオフにします。デフォルト値はディセーブルです。  
(注) マルチキャストダイレクト機能を有効にすると、既存のクライアントの状態が自動的にリセットされません。コントローラでマルチキャストダイレクト機能を有効にした後、ワイヤレスクライアントはマルチキャストストリームに再 join する必要があります。
- c) [Session Message Config] 領域で、[Session announcement State] チェックボックスをオンにしてセッション通知メカニズムを有効にします。セッション通知の状態が有効の場合、コントローラがクライアントにマルチキャストダイレクトデータを提供できない場合は常にクライアントに通知されます。
- d) [Session announcement URL] テキストボックスには、マルチキャストメディアストリーム伝送中にエラーが発生した場合にクライアントが詳細情報を見つけられる URL を入力します。
- e) [Session announcement e-mail] テキストボックスには、連絡が可能な人物の電子メールアドレスを入力します。
- f) [Session announcement Phone] テキストボックスには、連絡が可能な人物の電話番号を入力します。
- g) [Session announcement Note] テキストボックスには、特定のクライアントにマルチキャストメディアを提供できない理由を入力します。
- h) [Apply] をクリックします。

**ステップ 2** 次の手順に従って、メディアストリームを追加します。

- a) [Wireless] > [Media Stream] > [Streams] を選択して [Media Stream] ページを開きます。
- b) 新しいメディアストリームを設定するには、[Add New] をクリックします。[Media Stream > New] ページが表示されます。  
(注) [Stream Name]、[Multicast Destination Start IP Address (IPv4 or IPv6)]、および [Multicast Destination End IP Address (IPv4 or IPv6)] テキストボックスは必須です。これらのテキストボックスに情報を入力する必要があります。
- c) [Stream Name] テキストボックスに、メディアストリーム名を入力します。ストリーム名には最大 64 文字を使用できます。
- d) [Multicast Destination Start IP Address (IPv4 or IPv6)] テキストボックスに、マルチキャストメディアストリームの開始 (IPv4 または IPv6) アドレスを入力します。

- e) [Multicast Destination End IP Address (IPv4 or IPv6)] テキスト ボックスに、マルチキャスト メディア ストリームの終了 (IPv4 または IPv6) アドレスを入力します。
- (注) マルチキャスト宛先の開始 IP と終了 IP のアドレスが同じタイプであることを確認します。つまり、両方のアドレスが IPv4 または IPv6 タイプのいずれかである必要があります。
- f) [Maximum Expected Bandwidth] テキスト ボックスに、メディア ストリームに割り当てる最大期待帯域幅を入力します。値は 1 ~ 35000 kbps の範囲で指定できます。
- (注) コントローラにメディア ストリームを追加するには、テンプレートを使用することをお勧めします。
- g) [Resource Reservation Control (RRC) Parameters] の下の [Select from Predefined Templates] ドロップダウン リストから、次のいずれかのオプションを選択して、リソース予約制御の詳細を指定します。
- Very Coarse (300 kbps 以下)
  - Coarse (500 kbps 以下)
  - Ordinary (750 kbps 以下)
  - Low (1 Mbps 以下)
  - Medium (3 Mbps 以下)
  - High (5 Mbps 以下)
- (注) ドロップダウン リストから事前定義済みのテンプレートを選択すると、[Resource Reservation Control (RRC) Parameters] の下の次のテキスト ボックスにテンプレートで割り当てるデフォルト値がリスト表示されます。
- [Average Packet Size (100-1500 bytes)] : 平均パケットサイズを指定します。値の範囲は 100 ~ 1500 バイトです。デフォルト値は 1200 です。
  - [RRC Periodic update] : RRC (Resource Reservation Control Check) の定期的な更新を有効にします。デフォルトで、このオプションは有効になっています。RRC は正しいチャネルロードに従って許可されたストリームのアドミSSION決定を定期的に更新します。結果として、特定の優先順位の低い許可されたストリームの要求が拒否される場合があります。
  - [RRC Priority (1-8)] : メディア ストリーム内の優先順位ビットを指定します。優先順位は 1 ~ 8 の間の任意の数値に設定できます。値が大きくなるほど、優先順位が高くなります。たとえば、1 が最低値で、8 が最高値です。デフォルトのプライオリティは 4 です。優先順位の低いストリームは RRC 定期更新で拒否される場合があります。
  - [Traffic Profile Violation] : 再 RRC 後に違反した場合に実行される動作を指定します。ドロップダウン リストから動作を選択します。表示される値は次のとおりです。
    - [Drop] : 定期的な再評価でストリームがドロップされるように指定します。
    - [Fallback] : 定期的な再評価でストリームがベスト エフォート クラスに降格されるよう指定します。
 デフォルト値は [Drop] です。

h) [Apply] をクリックします。

**ステップ 3** 次の手順に従って、メディア ストリームのマルチキャストダイレクトを有効にします。

- a) [WLANs] > [WLAN ID] の順に選択して、[WLANs > Edit] ページを開きます。
- b) [QoS] タブをクリックして [Quality of Service (QoS)] ドロップダウンリストから [Gold (Video)] を選択します。
- c) [Apply] をクリックします。

**ステップ 4** 次の手順に従って、EDCA パラメータを設定して、音声とビデオを最適化します (任意)。

- a) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [EDCA Parameters] の順に選択します。
- b) [EDCA Profile] ドロップダウンリストで、[Voice and Video Optimized] オプションを選択します。
- c) [Apply] をクリックします。

**ステップ 5** 次の手順に従って、ビデオの帯域でアドミッション コントロールを有効にします (任意)。

(注) パフォーマンスを上げるために、音声の帯域割り当ては最低のままにしてください。

- a) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Media] の順に選択して、[802.11a/n (5 GHz) (または 802.11b/g/n) > Media] ページを開きます。
- b) [Video] タブをクリックします。
- c) この無線帯域で帯域幅ベースの CAC を有効にするには、[Admission Control (ACM)] チェックボックスをオンにします。デフォルト値はディセーブルです。
- d) [Apply] をクリックします。

**ステップ 6** 次の手順に従って、ビデオ帯域幅を設定します。

(注) メディアストリームに対して設定するテンプレート帯域幅は、メディアストリームのソースの帯域幅より大きくする必要があります。

(注) 音声の設定はオプションです。パフォーマンスを上げるために、音声の帯域割り当ては最低のままにしてください。

- a) すべての WMM WLAN を無効にします。
- b) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Media] の順に選択して、[802.11a/n/ac (5 GHz) (または 802.11b/g/n) > Media] ページを開きます。
- c) [Video] タブをクリックします。
- d) この無線帯域でビデオの CAC を有効にするには、[Admission Control (ACM)] チェックボックスをオンにします。デフォルト値はディセーブルです。
- e) [Max RF Bandwidth] フィールドに、この無線帯域でビデオ アプリケーション用にクライアントに割り当てられる最大帯域幅の割合を入力します。指定された値に達すると、アクセスポイントはこの無線帯域での新しい要求を拒否します。
- f) 範囲は 5 ~ 85 % です。
- g) デフォルト値は 9 % です。
- h) [Apply] をクリックします。
- i) すべての WMM WLAN を有効にし、[Apply] をクリックします。

**ステップ 7** 次の手順に従って、メディア帯域幅を設定します。

- a) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Media] の順に選択して、[802.11a (または 802.11b) > Media > Parameters] ページを開きます。
- b) [Media] タブをクリックして、[Media] ページを開きます。
- c) [Unicast Video Redirect] チェックボックスをオンにして、ユニキャストビデオリダイレクトを有効にします。デフォルト値はディセーブルです。
- d) [Maximum Media Bandwidth (0-85%)] テキストボックスに、この無線帯域でメディアアプリケーション用に割り当てられる最大帯域幅の割合を入力します。クライアントが指定値に達すると、この無線帯域上での新しいコールはアクセスポイントで拒否されます。
- e) デフォルト値は 85 % です。有効な値は 0 ~ 85 % です。
- f) [Client Minimum Phy Rate] テキストボックスに、クライアントへの最小伝送データレートをを入力します。伝送データレートが PHY レートを下回ると、ビデオが開始されないか、クライアントが不良クライアントとして分類される場合があります。不良クライアントビデオは、より良いエフォートの QoS のために降格されたり、拒否される可能性があります。
- g) [Maximum Retry Percent (0-100%)] テキストボックスに、許可される最大再試行の割合を入力します。デフォルト値は 80 です。80 を超えると、ビデオが開始されないか、クライアントが不良クライアントとして分類される場合があります。不良クライアントビデオは、より良いエフォートの QoS のために降格されたり、拒否される可能性があります。
- h) [Multicast Direct Enable] フィールドを有効にするには、[Multicast Direct Enable] チェックボックスをオンにします。デフォルト値はイネーブルです。
- i) [Max Streams per Radio] ドロップダウンリストで無線ごとに許可されるストリームの最大数を 0 ~ 20 の範囲から選択します。デフォルト値は [No-limit] に設定されています。[No-limit] を選択した場合、クライアントサブスクリプションの数に制限はありません。
- j) [Max Streams per Client] ドロップダウンリストでクライアントごとに許可されるストリームの最大数を 0 ~ 20 の範囲から選択します。デフォルト値は [No-limit] に設定されています。[No-limit] を選択した場合、クライアントサブスクリプションの数に制限はありません。
- k) ベストエフォート Quality Of Service アドミッションを有効にするには、[Best Effort QoS Admission] チェックボックスをオンにします。
- l) [Apply] をクリックします。

**ステップ 8** 次の手順に従って、WLAN を有効にします。

- a) [WLANS] > [WLAN ID] を選択します。[WLANS > Edit] ページが表示されます。
- b) [Status] チェックボックスをオンにします。
- c) [Apply] をクリックします。

**ステップ 9** 次の手順に従って、802.11a/n/ac または 802.11b/g/n ネットワークを有効にします。

- a) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] の順に選択します。
- b) [802.11a (または 802.11b/g) Network Status] チェックボックスをオンにして、ネットワークステータスを有効にします。
- c) [Apply] をクリックします。

**ステップ 10** 次の手順に従って、クライアントがマルチキャストグループおよびグループ ID に関連付けられていることを確認します。

- a) [Monitor] > [Clients] を選択します。[Clients] ページが表示されます。

- b) 802.11a/n/ac または 802.11b/g/n ネットワーク クライアントに関連付けられたアクセス ポイントがあるかどうかを確認します。
- c) [Monitor] > [Multicast] の順に選択します。 [Multicast Groups] ページが表示されます。
- d) クライアントへの VideoStream のための [MGID] チェックボックスをオンにします。
- e) [MGID] をクリックします。 [Multicast Group Detail] ページが表示されます。 マルチキャスト ステータスの詳細を確認します。

## VideoStream の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、WLAN メディア ストリーム上でマルチキャストダイレクト機能を設定します。  
**config wlan media-stream multicast-direct** {wlan\_id | all} {enable | disable}

**ステップ 2** 次のコマンドを入力して、マルチキャスト機能を有効または無効にします。  
**config media-stream multicast-direct** {enable | disable}

**ステップ 3** 次のコマンドを入力して、さまざまなメッセージ設定パラメータを設定します。  
**config media-stream message** {state [enable | disable] | url url | email email | phone phone\_number | note note}

**ステップ 4** 次のコマンドを入力して、変更を保存します。  
**save config**

**ステップ 5** 次のコマンドを入力して、さまざまなグローバル メディア ストリーム設定を行います。  
**config media-stream add multicast-direct stream-name** media\_stream\_name start\_IP end\_IP {template {very-coarse | coarse | ordinary | low-resolution | med-resolution | high-resolution} | detail {Max\_bandwidth bandwidth | packet size packet\_size | Re-evaluation re-evaluation {periodic | initial}} video video priority {drop | fallback}}

- テンプレートに割り当てられた値に基づいて、Resource Reservation Control (RRC) パラメータが事前定義済みの値と共に割り当てられます。
- RRC パラメータをメディア ストリームに割り当てるために、次のテンプレートを使用します。
  - Very Coarse (3000 kbps 以下)
  - Coarse (500 kbps 以下)
  - Ordinary (750 kbps 以下)
  - Low Resolution (1 mbps 以下)
  - Medium Resolution (3 mbps 以下)
  - High Resolution (5 mbps 以下)

**ステップ 6** 次のコマンドを入力して、メディア ストリームを削除します。  
**config media-stream delete** media\_stream\_name



**ステップ 7** 次のコマンドを入力して、特定の Enhanced Distributed Channel Access (EDC) プロファイルを有効にします。

```
config advanced { 801.11a | 802.11b } edca-parameters optimized-video-voice
```

**ステップ 8** 次のコマンドを入力して、目的の帯域幅のアドミッション コントロールを有効にします。

- 次のコマンドを入力して、802.11a または 802.11b/g ネットワークの帯域幅ベースの音声 CAC を有効にします。

```
config {802.11a | 802.11b} cac voice acm enable
```

- 次のコマンドを入力して、802.11a または 802.11b/g ネットワーク上で音声アプリケーション用にクライアントに割り当てられた最大帯域幅の割合を設定します。

```
config {802.11a | 802.11b} cac voice max-bandwidth bandwidth
```

- 次のコマンドを入力して、802.11a または 802.11b/g ネットワーク上でローミングする音声クライアント用に予約された最大割り当て帯域幅の割合を設定します。

```
config {802.11a | 802.11b} cac voice roam-bandwidth bandwidth
```

(注) ビデオ通話用の TSpec ベースおよび SIP ベースの CAC の場合は、静的な方式のみがサポートされます。

**ステップ 9** 次のコマンドを入力して、無線および/またはクライアントごとのストリームの最大数を設定します。

- 次のコマンドを入力して、無線ごとのマルチキャスト ストリーム数の最大制限値を設定します。

```
config {802.11a | 802.11b} media-stream multicast-direct radio-maximum [value | no-limit]
```

- 次のコマンドを入力して、クライアントごとのマルチキャスト ストリームの最大数を設定します。

```
config {802.11a | 802.11b} media-stream multicast-direct client-maximum [value | no-limit]
```

**ステップ 10** 次のコマンドを入力して、変更を保存します。

```
save config
```

## メディアストリームの表示とデバッグ

- 次のコマンドを入力して、設定されたメディア ストリームを参照します。

```
show wlan wlan_id
```

- 次のコマンドを入力して、メディア ストリーム名の詳細を参照します。

```
show 802.11{a | b | h} media-stream media-stream_name
```

- 次のコマンドを入力して、メディア ストリームのクライアントを参照します。

```
show 802.11a media-stream client media-stream-name
```

- 次のコマンドを入力して、メディア ストリームとクライアント情報のサマリーを参照します。

**show media-stream group summary**

- 次のコマンドを入力して、特定のメディア ストリーム グループについての詳細を参照します。

**show media-stream group detail *media\_stream\_name***

- 次のコマンドを入力して、802.11a または 802.11b メディア リソース予約設定の詳細を参照します。

**show {802.11a | 802.11b} media-stream rrc**

- 次のコマンドを入力して、メディア ストリーム履歴のデバッグを有効にします。

**debug media-stream history {enable | disable}**



## 第 **IV** 部

# セキュリティ ソリューションの設定

- [Cisco Unified Wireless Network Solution セキュリティ, 423 ページ](#)
- [RADIUS の設定, 427 ページ](#)
- [TACACS+ の設定, 455 ページ](#)
- [FIPS 設定、CC、UCAPL, 467 ページ](#)
- [最大ローカル データベース エントリの設定, 471 ページ](#)
- [コントローラでのローカル ネットワーク ユーザの設定, 473 ページ](#)
- [パスワード ポリシーの設定, 477 ページ](#)
- [LDAP の設定, 481 ページ](#)
- [ローカル EAP の設定, 487 ページ](#)
- [SpectraLink 社の NetLink 電話用システムの設定, 501 ページ](#)
- [RADIUS NAC サポートの設定, 505 ページ](#)
- [設定の RADIUS VSA およびレルム, 509 ページ](#)
- [無線による管理機能の使用, 517 ページ](#)
- [動的インターフェイスによる管理機能, 519 ページ](#)
- [DHCP オプション 82 の設定, 521 ページ](#)
- [アクセス コントロール リストの設定と適用, 525 ページ](#)

- [管理フレーム保護の設定, 541 ページ](#)
- [クライアント除外ポリシーの設定, 547 ページ](#)
- [Identity ネットワーキングの設定, 551 ページ](#)
- [AAA Override の設定, 557 ページ](#)
- [不正なデバイスの管理, 561 ページ](#)
- [不正なアクセス ポイントの分類, 573 ページ](#)
- [Cisco TrustSec SXP の設定, 591 ページ](#)
- [ローカル ポリシーの設定, 597 ページ](#)
- [Cisco Intrusion Detection System の設定, 603 ページ](#)
- [IDS シグニチャの設定, 609 ページ](#)
- [wIPS の設定, 619 ページ](#)
- [Wi-Fi Direct クライアント ポリシーの設定, 631 ページ](#)
- [Web 認証プロキシの設定, 635 ページ](#)
- [意図的な悪用の検出, 639 ページ](#)



## 第 42 章

# Cisco Unified Wireless Network Solution セキュリティ

- [セキュリティの概要, 423 ページ](#)
- [レイヤ 1 ソリューション, 423 ページ](#)
- [レイヤ 2 ソリューション, 424 ページ](#)
- [レイヤ 3 ソリューション, 424 ページ](#)
- [統合されたセキュリティ ソリューション, 424 ページ](#)

## セキュリティの概要

Cisco Unified Wireless Network (UWN) セキュリティ ソリューションは、複雑になりがちなレイヤ 1、レイヤ 2、およびレイヤ 3 の 802.11 アクセス ポイントのセキュリティ コンポーネントを 1 つのシンプルなポリシー マネージャにまとめたもので、システム全体のセキュリティ ポリシーを WLAN 単位でカスタマイズできます。Cisco UWN セキュリティ ソリューションは、シンプルで、統一された、体系的なセキュリティ 管理ツールを提供します。

企業での WLAN 展開の最も大きな障害の 1 つが、脆弱な独立型の暗号化方式である Wired Equivalent Privacy (WEP) です。低価格のアクセス ポイントの登場も新たな問題であり、それらは企業 ネットワークに接続して man-in-the-middle 攻撃や DoS 攻撃（サービス拒絶攻撃）に利用される可能性があります。

## レイヤ 1 ソリューション

Cisco UWN セキュリティ ソリューションによって、すべてのクライアントのアクセス回数は、ユーザが設定した数値までに制限されます。制限回数内でアクセスできなかった場合、そのクライアントはユーザが設定したタイマーが切れるまで自動的に除外（アクセスをブロック）されます。オペレーティング システムでは、WLAN ごとに SSID ブロードキャストを無効にすることもできます。

## レイヤ2ソリューション

上位レベルのセキュリティと暗号化が必要な場合は、拡張認証プロトコル (EAP) や Wi-Fi Protected Access (WPA)、および WPA2 など業界標準のセキュリティソリューションを実装することもできます。Cisco UWN ソリューションの WPA 実装には、AES (Advanced Encryption Standard) ダイナミック キー、TKIP+Michael (Temporal Key Integrity Protocol+Message Integrity Code Checksum) ダイナミック キー、WEP (Wired Equivalent Privacy) スタティック キーが含まれます。無効化も使用され、ユーザが設定した回数だけ認証の試行に失敗すると、自動的にレイヤ2 アクセスがブロックされます。

どの無線セキュリティソリューションを採用した場合も、コントローラと Lightweight アクセスポイントとの間のすべてのレイヤ2 有線通信は、Control and Provisioning of Wireless Access Points (CAPWAP) トンネルを使用してデータを渡すことにより保護されます。

### レイヤ2ソリューションの制約事項

認証キー管理として WPA/WPA2 と CCKM が使用されている場合、Cisco Aironet クライアントアダプタバージョン 4.2 で認証は行われず、コントローラと AP 間に 2 秒の遅延があります。

## レイヤ3ソリューション

WEP の問題は、パススルー VPN のような業界標準のレイヤ3セキュリティソリューションを使用すると、さらに進んだ解決が可能です。

Cisco UWN ソリューションでは、ローカルおよび RADIUS MAC (Media Access Control) フィルタリングがサポートされています。このフィルタリングは、802.11 アクセスカードの MAC アドレス一覧情報が把握できている小規模のクライアントグループに適しています。

Cisco UWN ソリューションでは、ローカルおよび RADIUS ユーザおよびパスワード認証がサポートされています。この認証は、小規模から中規模のクライアントグループに適しています。

## 統合されたセキュリティソリューション

統合されたセキュリティソリューションを次に示します。

- Cisco Unified Wireless Network (UWN) ソリューションオペレーティングシステムのセキュリティは、802.1X AAA (認証、許可、アカウントリング) エンジンを中心に構築されており、ユーザは Cisco UWN ソリューション全体にわたってさまざまなセキュリティポリシーを迅速に設定および適用できます。
- コントローラおよび Lightweight アクセスポイントには、システム全体の認証および許可プロトコルがすべてのポートおよびインターフェイスに装備され、最大限のシステムセキュリティが提供されています。
- オペレーティングシステムのセキュリティポリシーは個々の WLAN に割り当てられ、Lightweight アクセスポイントは設定されたすべての WLAN (最大 16) を同時にブロードキャ

ストします。これによって追加のアクセスポイントは不要になりますが、干渉が増加し、システムスループットが低下する可能性があります。

- オペレーティングシステムセキュリティはRRM機能を使用して、干渉およびセキュリティ違反がないか継続的に空間を監視し、それらを検出したときはユーザーに通知します。
- オペレーティングシステムセキュリティは、業界標準の認証、許可、アカウントिंग（AAA）サーバで機能します。







## 第 43 章

# RADIUS の設定

- [RADIUS について](#), 427 ページ
- [ACS 上での RADIUS の設定](#), 430 ページ
- [RADIUS の設定 \(GUI\)](#), 431 ページ
- [RADIUS の設定 \(CLI\)](#), 437 ページ
- [コントローラによって送信される RADIUS 認証属性](#), 441 ページ
- [Access-Accept パケットで受け付けられる認証属性 \(Airespace\)](#), 444 ページ
- [RADIUS アカウンティング属性](#), 452 ページ

## RADIUS について

Remote Authentication Dial-In User Service (RADIUS) とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバプロトコルです。このプロトコルは、ローカル認証や TACACS+ 認証と同様に、バックエンドのデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- **認証** : コントローラにログインしようとするユーザを検証するプロセス。

コントローラで RADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。複数のデータベースを設定する場合は、バックエンドデータベースを試行する順序を指定できます。

- **アカウンティング** : ユーザによる処理と変更を記録するプロセス。

ユーザによる処理が正常に実行される度に、RADIUS アカウンティングサーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたりリモートホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。RADIUS アカウンティングサーバが接続不能になった場合、ユーザはセッションを続行できなくなります。

RADIUS では、転送にユーザ データグラム プロトコル (UDP) を使用します。RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウントング要求がリッスンされます。アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

複数の RADIUS アカウントングおよび認証サーバを設定できます。たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウントングサーバを異なる地域に配置できます。同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

管理ユーザが RADIUS サーバを使用して認証される場合、PAP プロトコルだけが使用されます。Web 認証ユーザの場合、PAP、MSCHAPv2 および MD5 セキュリティ メカニズムがサポートされます。

### RADIUS サーバのサポート

- RADIUS 認証サーバおよびアカウントング サーバは、それぞれ最大 17 台まで設定できます。
- 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。
- ワンタイムパスワード (OTP) は、RADIUS を使用しているコントローラでサポートされます。この設定では、コントローラがトランスペアレント パススルー デバイスとして動作します。コントローラは、クライアント動作をチェックせずにすべてのクライアント要求を RADIUS サーバに転送します。OTP を使用する場合は、クライアントが正しく機能するためにはコントローラへの接続を 1 つ確立する必要があります。現在、コントローラには、複数の接続を確立しようとしているクライアントを修正するチェック機能はありません。
- RADIUS サーバで読み取り専用コントローラユーザを作成するには、サービスタイプをコールバック NAS プロンプトではなく NAS プロンプトに設定します。サービスタイプをコールバック NAS プロンプトに設定すると、ユーザ認証は失敗しますが、NAS プロンプトに設定されることで、コントローラへの読み取り専用アクセスがユーザに与えられます。  
また、コールバック管理サービスタイプでは、ユーザにコントローラへのロビー アンバサダー権限が与えられます。

### Radius ACS サポート

- CiscoSecure Access Control Server (ACS) とコントローラの両方で、RADIUS を設定する必要があります。
- RADIUS は、CiscoSecure ACS バージョン 3.2 以降のリリースでサポートされます。実行しているバージョンに対応する CiscoSecure ACS のマニュアルを参照してください。

### プライマリおよびフォールバック RADIUS サーバ

プライマリ RADIUS サーバ（最も低いサーバインデックスを持つサーバ）は、コントローラの最優先サーバであるとみなされます。プライマリサーバが応答なくなると、コントローラは、次にアクティブなバックアップサーバ（低い方から2番目のサーバインデックスを持つサーバ）に切り替えます。コントローラは、プライマリ RADIUS サーバが回復して応答可能になるとそのサーバにフォールバックするように設定されているか、使用可能なバックアップサーバの中からより優先されるサーバにフォールバックするように設定されていない限り、このバックアップサーバを引き続き使用します。

### RADIUS DNS

完全修飾ドメイン名（FQDN）を使用できます。これにより、必要に応じて IP アドレスを変更できます（たとえば、ロード バランシングの更新）。サブメニューの [DNS] が [Security > AAA > RADIUS] メニューに追加されます。これを使用して、DNS から RADIUS IP 情報を取得できます。DNS クエリーはデフォルトでは無効になっています。

## ACS 上での RADIUS の設定

- ステップ1 ACS のメイン ページで、[Network Configuration] を選択します。
- ステップ2 [AAA Clients] の下の [Add Entry] を選択し、使用しているコントローラをサーバに追加します。[Add AAA Client] ページが表示されます。

図 40 : CiscoSecure ACS の [Add AAA Client] ページ

- ステップ3 [AAA Client Hostname] テキスト ボックスに、コントローラの名前を入力します。
- ステップ4 [AAA Client IP Address] テキスト ボックスに、コントローラの IP アドレスを入力します。
- ステップ5 [Shared Secret] テキスト ボックスに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。
- (注) 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

- ステップ 6 [Authenticate Using] ドロップダウン リストから [RADIUS (Cisco Airespace)] を選択します。
- ステップ 7 [Submit + Apply] をクリックして、変更内容を保存します。
- ステップ 8 ACS のメインページで、[Interface Configuration] を選択します。
- ステップ 9 [RADIUS (Cisco Aironet)] を選択します。 [RADIUS (Cisco Aironet)] ページが表示されます。
- ステップ 10 [User Group] の [Cisco-Aironet-Session-Timeout] チェックボックスをオンにします。
- ステップ 11 [Submit] をクリックして変更を保存します。
- ステップ 12 ACS のメインページで、左のナビゲーション ペインから [System Configuration] を選択します。
- ステップ 13 [Logging] を選択します。
- ステップ 14 [Logging Configuration] ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。
- ステップ 15 ACS のメインページで、左のナビゲーション ペインから [Group Setup] を選択します。
- ステップ 16 [Group] ドロップダウン リストから、以前に作成したグループを選択します。  
 (注) この手順では、ユーザが割り当てられることになるロールに基づいて、ACS のグループにすでにユーザが割り当てられていることを想定しています。
- ステップ 17 [Edit Settings] をクリックします。 [Group Setup] ページが表示されます。
- ステップ 18 [Cisco Aironet Attributes] の [Cisco-Aironet-Session-Timeout] チェックボックスをオンにし、編集ボックスにセッションタイムアウト値を入力します。
- ステップ 19 RADIUS 認証を使用したコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定します。読み取り専用アクセスが必要な場合は、Service-Type 属性 (006) を [Callback NAS Prompt] に設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] に設定してください。この属性を設定しない場合、認証プロセスはコントローラ上での許可エラーなしで正常に完了しますが、認証を再試行するようにプロンプトが表示されることがあります。  
 (注) ACS 上で Service-Type 属性を設定する場合は、必ずコントローラの GUI の [RADIUS Authentication Servers] ページ上にある [Management] チェックボックスをオンにします。
- ステップ 20 [Submit] をクリックして変更を保存します。

## RADIUS の設定 (GUI)

- ステップ 1 [Security] > [AAA] > [RADIUS] を選択します。
- ステップ 2 次のいずれかの操作を行います。
- RADIUS サーバを認証用に設定する場合は、[Authentication] を選択します。
  - RADIUS サーバをアカウントリング用に設定する場合は、[Accounting] を選択します。

(注) 認証およびアカウントिंगの設定に使用されるページでは、ほとんど同じテキストボックスが表示されます。そのため、ここでは [Authentication] ページを例にとって、設定の手順を一度だけ示します。同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

[RADIUS Authentication (または Accounting) Servers] ページが表示されます。

このページには、これまでに設定されたすべての RADIUS サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

**ステップ 3** [Acct Call Station ID Type] ドロップダウン リストから、Access-Request メッセージで RADIUS サーバに送信されるオプションを選択します。次のオプションを使用できます。

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC アドレス : SSID
- AP 名 : SSID
- AP Name
- AP グループ
- Flex グループ
- AP の場所
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

(注) AP 名 : SSID、AP 名、AP グループ、Flex グループ、AP の場所、および VLAN ID オプションは、リリース 7.4 で追加されます。

AP Ethernet MAC Address および AP Ethernet MAC Address:SSID は 7.6 リリースで追加されます。

**ステップ 4** [Auth Call Station ID Type] ドロップダウン リストから、Access-Request メッセージで RADIUS サーバに送信されるオプションを選択します。次のオプションを使用できます。

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID

- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

**ステップ 5** [Use AES Key Wrap] チェックボックスをオンにし、AES キー ラップ保護を使用して RADIUS からコントローラへのキーの転送を有効にします。デフォルト値はオフです。この機能は、FIPS を使用するユーザにとって必要です。

**ステップ 6** [Apply] をクリックします。次のいずれかの操作を行います。

- 既存の RADIUS サーバを編集するには、そのサーバのサーバインデックス番号をクリックします。[RADIUS Authentication (または Accounting) Servers > Edit] ページが表示されます。
- RADIUS サーバを追加するには、[New] をクリックします。[RADIUS Authentication (または Accounting) Servers > New] ページが表示されます。

**ステップ 7** 新しいサーバを追加している場合は、[Server Index (Priority)] ドロップダウンリストから数字を選択し、同じサービスを提供するその他の設定済みの RADIUS サーバに対してこのサーバの優先順位を指定します。

**ステップ 8** 新しいサーバを追加している場合は、[Server IP Address] テキストボックスに RADIUS サーバの IP アドレスを入力します。

**ステップ 9** [Shared Secret Format] ドロップダウンリストから [ASCII] または [Hex] を選択し、コントローラと RADIUS サーバ間で使用される共有秘密キーの形式を指定します。デフォルト値は [ASCII] です。

**ステップ 10** [Shared Secret] テキストボックスと [Confirm Shared Secret] テキストボックスに、コントローラとサーバ間で認証に使用される共有秘密キーを入力します。

(注) 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

**ステップ 11** 新しい RADIUS 認証サーバを設定して AES キー ラップを有効にすると、コントローラと RADIUS サーバ間の共有秘密の安全性を高めることができます。そのための手順は次のとおりです。

(注) AES キー ラップは、Federal Information Processing Standards (FIPS) を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。

- a) [Key Wrap] チェックボックスをオンにします。
- b) [Key Wrap Format] ドロップダウンリストから [ASCII] または [HEX] を選択して、AES キー ラップキーの形式を Key Encryption Key (KEK) または Message Authentication Code Key (MACK) に指定します。
- c) [Key Encryption Key (KEK)] テキストボックスに、16 バイトの KEK を入力します。

d) [Message Authentication Code Key (MACK)] テキスト ボックスに、20 バイトの KEK を入力します。

**ステップ 12** 新しいサーバを追加している場合は、[Port Number] テキスト ボックスに、インターフェイス プロトコルに対応する RADIUS サーバの UDP ポート番号を入力します。有効な値の範囲は 1 ~ 65535 で、認証用のデフォルト値は 1812、アカウントング用のデフォルト値は 1813 です。

**ステップ 13** [Server Status] テキスト ボックスから [Enabled] を選択してこの RADIUS サーバを有効にするか、[Disabled] を選択して無効にします。デフォルト値はイネーブルです。

**ステップ 14** 新しい RADIUS 認証サーバを設定している場合は、[Support for RFC 3576] ドロップダウン リストから [Enabled] を選択して RFC 3576 を有効にするか、[Disabled] を選択してこの機能を無効にします。RFC 3576 では、ユーザセッションの動的な変更を可能にするよう RADIUS プロトコルが拡張されています。デフォルト値は [Enabled] です。RFC 3576 では、ユーザの切断およびユーザセッションに適用される許可の変更のほか、Disconnect メッセージと Change-of-Authorization (CoA) メッセージがサポートされています。Disconnect メッセージはユーザセッションをただちに終了させ、CoA メッセージはデータ フィルタなどのセッション認証属性を変更します。

**ステップ 15** [Server Timeout] テキスト ボックスに、再送信の間隔を秒単位で入力します。有効な範囲は 2 ~ 30 秒で、デフォルト値は 2 秒です。

[Key Wrap] チェックボックスをオンにします。

(注) 再認証が繰り返し試行されたり、プライマリサーバがアクティブで接続可能なときにコントローラがバックアップサーバにフォールバックしたりする場合には、タイムアウト値を増やすことをお勧めします。

**ステップ 16** [Network User] チェックボックスをオンにしてネットワーク ユーザ認証 (またはアカウントング) を有効にするか、オフにしてこの機能を無効にします。デフォルト値はオンです。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS 認証 (アカウントング) サーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。

**ステップ 17** RADIUS 認証サーバを設定している場合は、[Management] チェックボックスをオンにして管理認証を有効にするか、オフにしてこの機能を無効にします。デフォルト値はオンです。この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。

**ステップ 18** [IPSec] チェックボックスをオンにして IP セキュリティ メカニズムを有効にするか、オフにしてこの機能を無効にします。デフォルト値はオフです。

**ステップ 19** ステップ 17 で IPSec を有効にした場合は、次の手順に従って追加の IPSec パラメータを設定します。

a) [IPSec] ドロップダウン リストから、IP セキュリティで使用される認証プロトコルとして、[HMAC MD5] または [HMAC SHA1] のいずれかのオプションを選択します。デフォルト値は [HMAC SHA1] です。Message Authentication Code (MAC; メッセージ認証コード) は、秘密キーを共有する 2 者間で送信される情報を検証するために使用されます。HMAC (Hash MAC) は暗号ハッシュ関数に基づくメカニズムです。任意の反復暗号ハッシュ関数との組み合わせで使用できます。HMAC でハッシュ関数として MD5 を使用するのが HMAC MD5 であり、SHA1 を使用するのが HMAC SHA1 です。また、HMAC では、メッセージ認証値の計算と検証に秘密キーを使用します。

b) [IPSec Encryption] ドロップダウン リストで次のオプションのいずれかを選択して、IP セキュリティ暗号化メカニズムを指定します。



- [DES] : データ暗号化規格。プライベート (秘密) キーを使用するデータ暗号化の方法です。DES では、56 ビットのキーを 64 ビットのデータブロックごとに適用します。
  - [3DES] : 連続して 3 つのキーを適用するデータ暗号化規格です。これは、デフォルト値です。
  - [AES CBC] : 高度暗号化規格。128、192、または 256 ビット長のキーを使用して 128、192、または 256 ビット長のデータブロックを暗号化します。AES 128 CBC では、暗号ブロック連鎖 (CBC) モードで 128 ビットのデータパスを使用します。
  - [256-AES] : 256 ビット長のキーを使用する高度暗号化規格。
- c) [IKE Phase 1] ドロップダウン リストから [Aggressive] または [Main] のいずれかのオプションを選択して、インターネット キー交換 (IKE) プロトコルを指定します。デフォルト値は [Aggressive] です。IKE Phase 1 は、IKE の保護方法をネゴシエートするために使用されます。Aggressive モードでは、セキュリティゲートウェイの ID をクリアで送信するだけで、わずかに高速な接続が確立され、より少ないパケットでより多くの情報が渡されます。
- d) [Lifetime] テキストボックスに値 (秒単位) を入力して、セッションのタイムアウト間隔を指定します。有効な範囲は 1800 ~ 57600 秒で、デフォルト値は 1800 秒です。
- e) [IKE Diffie Hellman Group] ドロップダウン リストから [Group 1 (768 bits)], [Group 2 (1024 bits)], または [Group 5 (1536 bits)] のいずれかのオプションを選択して、IKE Diffie Hellman グループを指定します。デフォルト値は [Group 1 (768 bits)] です。  
Diffie Hellman 技術を 2 つのデバイスで使用して共通キーを生成します。このキーを使用すると、値を公開された状態で交換して、同じ共通キーを生成することができます。3 つのグループのすべてで従来の攻撃に対するセキュリティが確保されますが、キーのサイズが大きいことから、Group 5 の安全性がより高くなります。ただし、Group 1 および Group 2 のキーを使用した計算は、素数サイズがより小さいために、多少高速に実行される可能性があります。
- (注) IPsec の共有秘密が設定されていない場合、デフォルトの RADIUS 共有秘密が使用されます。認証方式が PSK の場合、IPsec 共有秘密を使用するために WLANCC を有効にする必要があります。無効の場合はデフォルト値が使用されます。[Controller] > [Inventory] で WLANCC および UCAPL の前提条件モードの状態を表示できます。

**ステップ 20** [Apply] をクリックします。

**ステップ 21** [Save Configuration] をクリックします。

**ステップ 22** 同じサーバ上または追加の RADIUS サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

**ステップ 23** 次の手順を実行して、RADIUS サーバフォールバックの動作を指定します。

- a) [Security] > [AAA] > [RADIUS] > [Fallback to open the RADIUS] > [Fallback Parameters] の順に選択し、フォールバック パラメータ ページを開きます。
- b) [Fallback Mode] ドロップダウン リストから、次のオプションのいずれかを選択します。
  - [Off] : RADIUS サーバのフォールバックを無効にします。これは、デフォルト値です。
  - [Passive] : コントローラが、関係のないプローブメッセージを使用することなく、使用可能なバックアップサーバからより低い優先順位を持つサーバへの復帰を実行するようにします。コントローラは、しばらくの間非アクティブなすべてのサーバを無視し、あとで RADIUS メッセージの送信が必要になったときに再試行します。

- [Active] : コントローラが、RADIUS プロブ メッセージを使用して、使用可能なバックアップサーバからより低い優先順位を持つサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断するようにします。コントローラは、すべてのアクティブな RADIUS 要求に対して、非アクティブなすべてのサーバを無視します。プライマリサーバが回復した ACS サーバからの応答を一旦受信すると、アクティブ フォールバック RADIUS サーバは、アクティブプロブ認証を要求しているサーバにプロブメッセージを送信しなくなります。
- c) ステップ *b* でフォールバック モードを [Active] にした場合は、非アクティブなサーバプロブで送信される名前を [Username] テキスト ボックスに入力します。最大 16 文字の英数字を入力できます。デフォルト値は「cisco-probe」です。
- d) ステップ *b* でフォールバック モードを [Active] にした場合は、[Sec] テキスト ボックスの [Interval] にプロブ間隔値 (秒単位) を入力します。この間隔は、Passive モードでの非アクティブ時間、および Active モードでのプロブ間隔としての意味を持ちます。有効な範囲は 180 ~ 3600 秒で、デフォルト値は 300 秒です。

**ステップ 24** 次の手順で、RADIUS DNS パラメータを指定します。

- a) [Security] > [AAA] > [RADIUS] > [DNS] を選択します。[RADIUS DNS Parameters] ページが表示されます。
- b) [DNS Query] チェックボックスをオンまたはオフにします。
- c) [Port Number] テキスト ボックスに、認証ポート番号を入力します。有効な範囲は 1 ~ 65535 です。アカウントングポート番号は認証ポート番号に 1 を加えた値です。たとえば、認証ポート番号を 1812 と定義すると、アカウントングポート番号は 1813 です。アカウントングポート番号は常に認証ポート番号から取得されます。
- d) [Secret Format] ドロップダウン リストから、秘密を設定する形式を選択します。有効なオプションは ASCII と Hex です。
- e) 選択した形式に応じて秘密を入力して確定します。  
(注) すべてのサーバで同じ認証ポートおよび同じ秘密を使用する必要があります。
- f) [DNS Timeout] テキスト ボックスに、DNS サーバから最新の更新を取得するために DNS クエリーがリフレッシュされるまでの日数を入力します。
- g) [URL] テキスト ボックスに、RADIUS サーバの完全修飾ドメイン名または絶対ドメイン名を入力します。
- h) [Server IP Address] テキスト ボックスに、DNS サーバの IP アドレスを入力します。
- i) [Apply] をクリックします。

**ステップ 25** [Security] > [Priority Order] > [Management User] の順に選択し、複数のデータベースを設定する際の認証の順序を指定します。[Priority Order > Management User] ページが表示されます。

**ステップ 26** [Order Used for Authentication] テキスト ボックスで、コントローラが管理ユーザを認証する際にどのサーバを優先するかを指定します。[Not Used] テキスト ボックスと [Order Used for Authentication] テキスト ボックスの間でサーバを移動するには、[>] および [<] ボタンを使用します。希望するサーバが [Order Used for Authentication] テキスト ボックスに表示されたら、[Up] ボタンと [Down] ボタンを使用して優先するサーバをリストの先頭に移動します。

デフォルトで、ローカルデータベースは常に最初に検索されます。ユーザ名が見つからない場合、コントローラは、RADIUS に設定されている場合は RADIUS サーバへの切り換え、TACACS+ に設定されている場合は TACACS+ サーバへの切り換えを行います。デフォルトの設定はローカル、RADIUS の順になっています。

ステップ 27 [Apply] をクリックします。

ステップ 28 [Save Configuration] をクリックします。

## RADIUS の設定 (CLI)

- 次のコマンドを入力して、発信元の IP アドレス、システム MAC アドレス、AP MAC アドレス、AP イーサネット MAC アドレスが Access-Request メッセージで RADIUS サーバに送信されるかどうかを指定します。

```
config radius callStationIdType {ipaddr | macaddr | ap-macaddr-only | ap-macaddr-ssid |
ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid |
ap-location | ap-name | ap-name-ssid | flex-group-name | vlan-id}
```



(注) デフォルトでは、システムの MAC アドレスです。



注意 IPv6 専用クライアントには発信側ステーション ID タイプを使用しないでください。

- 次のコマンドを入力して、Access-Request メッセージで RADIUS 認証サーバまたはアカウントサーバに送信される MAC アドレスにデリミタを指定します。

```
config radius {auth | acct} mac-delimiter {colon | hyphen | single-hyphen | none}
```

値は次のとおりです。

- **colon** はデリミタをコロンに設定します (書式は xx:xx:xx:xx:xx:xx となります)。
- **hyphen** はデリミタをハイフンに設定します (書式は xx-xx-xx-xx-xx-xx となります)。これは、デフォルト値です。
- **single-hyphen** はデリミタを単一のハイフンに設定します (書式は xxxxxx-xxxxxx となります)。
- **none** はデリミタを無効にします (書式は xxxxxxxxxxxx となります)。
- 次のコマンドを入力して、RADIUS 認証サーバを設定します。
  - **config radius auth add index server\_ip\_address port# {ascii | hex} shared\_secret** : RADIUS 認証サーバを追加します。

- **config radius auth keywrap {enable | disable}** : AES キー ラップを有効にします。これにより、コントローラと RADIUS サーバ間の共有秘密の安全性が高まります。AES キー ラップは、Federal Information Processing Standards (FIPS) を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。
- **config radius auth keywrap add {ascii | hex} kek mack index** : AES キー ラップ属性を設定します。  
値は次のとおりです。
  - *kek* では、16 バイトの Key Encryption Key (KEK) が指定されます。
  - *mack* では、20 バイトの Message Authentication Code Key (MACK) が指定されます。
  - *index* では、AES キー ラップを設定する RADIUS 認証サーバのインデックスが指定されます。
- **config radius auth rfc3576 {enable | disable} index** : RFC 3576 を有効または無効にします。RFC 3576 では、ユーザセッションの動的な変更を可能にするように RADIUS プロトコルが拡張されています。RFC 3576 では、ユーザの切断およびユーザセッションに適用される許可の変更のほか、Disconnect メッセージと Change-of-Authorization (CoA) メッセージがサポートされています。Disconnect メッセージはユーザセッションをただちに終了させ、CoA メッセージはデータフィルタなどのセッション認証属性を変更します。
- **config radius auth retransmit-timeout index timeout** : RADIUS 認証サーバの再送信のタイムアウト値を設定します。
- **config radius auth network index {enable | disable}** : ネットワーク ユーザ認証を有効または無効にします。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS 認証サーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius auth management index {enable | disable}** : 管理認証を有効または無効にします。この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。
- **config radius auth ipsec {enable | disable} index** : IP セキュリティ メカニズムを有効または無効にします。
- **config radius auth ipsec authentication {hmac-md5 | hmac-sha1} index** : IP セキュリティに使用する認証プロトコルを設定します。
- **config radius auth ipsec encryption {3des | aes | des | none} index** : IP セキュリティ暗号化メカニズムを設定します。
- **config radius auth ipsec ike dh-group {group-1 | group-2 | group-5 | 2048bit-group-14} index** : IKE Diffie-Hellman グループを設定します。
- **config radius auth ipsec ike lifetime interval index** : セッションのタイムアウト間隔を設定します。

- **config radius auth ipsec ike phase1 {aggressive | main} index** : Internet Key Exchange (IKE) プロトコルを設定します。
  - **config radius auth ipsec ike auth-mode {pre-shared-key index hex-ascii-index shared-secret | certificate index}** : IKE 認証方式を設定します。デフォルトでは、事前共有キーは IPSEC セッションで使用されます。
  - **config radius auth {enable | disable} index** : RADIUS 認証サーバを有効または無効にします。
  - **config radius auth delete index** : 以前に追加された RADIUS 認証サーバを削除します。
- 次のコマンドを入力して、RADIUS アカウンティング サーバを設定します。
    - **config radius acct add index server\_ip\_address port# {ascii | hex} shared\_secret** : RADIUS アカウンティング サーバを追加します。
    - **config radius acct server-timeout index timeout** : RADIUS アカウンティング サーバの再送信のタイムアウト値を設定します。
    - **config radius acct network index {enable | disable}** : ネットワーク ユーザ アカウンティングを有効または無効にします。この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS アカウンティングサーバと見なされます。WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
    - **config radius acct ipsec {enable | disable} index** : IP セキュリティ メカニズムを有効または無効にします。
    - **config radius acct ipsec authentication {hmac-md5 | hmac-sha1} index** : IP セキュリティに使用する認証プロトコルを設定します。
    - **config radius acct ipsec encryption {3des | aes | des | none} index** : IP セキュリティ暗号化メカニズムを設定します。
    - **config radius acct ipsec ike dh-group {group-1 | group-2 | group-5} index** : IKE Diffie Hellman グループを設定します。
    - **config radius acct ipsec ike lifetime interval index** : セッションのタイムアウト間隔を設定します。
    - **config radius acct ipsec ike phase1 {aggressive | main} index** : Internet Key Exchange (IKE) プロトコルを設定します。
    - **config radius acct {enable | disable} index** : RADIUS アカウンティング サーバを有効または無効にします。
    - **config radius acct delete index** : 以前に追加された RADIUS アカウンティング サーバを削除します。
    - **config radius auth callStationIdType {ap-ethmac-only | ap-ethmac-ssid}** : SSID の有無にかかわらず AP の無線 MAC アドレスになるように発信側ステーション ID タイプを設定します。

- **config radius auth callStationIdType ap-label-address** : 発信側ステーション ID タイプを、認証メッセージに対して、AP ラベルに表示されている AP MAC アドレスに設定します。
  - **config radius auth callStationIdType ap-label-address-ssid** : 発信側ステーション ID タイプを、認証メッセージに対して、<AP label MAC address>:<SSID> 形式に設定します。
- 次のコマンドを入力して、RADIUS サーバのフォールバック動作を設定します。  
**config radius fallback-test mode {off | passive | active}**  
値は次のとおりです。
    - **off** は、RADIUS サーバのフォールバックを無効にします。
    - **passive** は、コントローラが、関係のないプローブ メッセージを使用することなく、使用可能なバックアップサーバから優先順位のより低いサーバへ復帰するようにします。当座は非アクティブなすべてのサーバを無視し、その後、RADIUS メッセージの送信が必要になったとき再試行します。
    - **active** は、コントローラが、RADIUS プローブ メッセージを使用して、使用可能なバックアップサーバから優先順位のより低いサーバへ復帰し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断するようにします。アクティブな RADIUS 要求に対して、コントローラは単に非アクティブなすべてのサーバを無視します。プライマリサーバが回復した ACS サーバからの応答を一旦受信すると、アクティブフォールバック RADIUS サーバは、アクティブプローブ認証を要求しているサーバにプローブメッセージを送信しなくなります。
  - ステップ 5 で Active モードを有効にした場合は、次のコマンドを入力して追加のフォールバック パラメータを設定します。
    - **config radius fallback-test username username** : 非アクティブなサーバプローブで送信する名前を指定します。 *username* パラメータには、最大 16 文字の英数字を入力できます。
    - **config radius fallback-test interval interval** : プローブ間隔の値 (秒単位) を指定します。
  - 次のコマンドを入力して、RADIUS DNS パラメータを設定します。
    - **config radius dns global port-num {ascii | hex} secret** : RADIUS DNS のグローバルポート番号と機密情報を追加します。
    - **config radius dns query url timeout-in-days** : RADIUS サーバの FQDN、および DNS サーバから最新の更新を取得するためにリフレッシュが実行されるまでのタイムアウトを設定します。
    - **config radius dns serverip ip-addr** : DNSサーバの IP アドレスを設定します。
    - **config radius dns {enable | disable}** : DNS クエリーを有効または無効にします。
  - 次のコマンドを入力して、変更を保存します。  
**save config**

- 次のコマンドを入力して、複数のデータベースを設定する際の認証の順序を設定します。  
**config aaa auth mgmt AAA\_server\_type AAA\_server\_type**  
ここで、AAA\_server\_type は local、radius、または tacacs となります。  
現在の管理認証サーバの順序を表示するには、show aaa auth コマンドを入力します。
- 次のコマンドを入力して、RADIUS の統計情報を表示します
  - **show radius summary** : RADIUS サーバ、および AP イーサネット MAC 設定による統計情報の概要を表示します。
  - **show radius auth statistics** : RADIUS 認証サーバの統計情報を表示します。
  - **show radius acct statistics** : RADIUS アカウンティングサーバの統計情報を表示します。
  - **show radius rfc3576 statistics** : RADIUS RFC 3576 サーバの概要を表示します。
- 次のコマンドを入力して、アクティブなセキュリティ アソシエーションを表示します。
  - **show ike {brief | detailed} ip\_or\_mac\_addr** : アクティブな IKE セキュリティ アソシエーションの簡単な概要または詳しい要約を表示します。
  - **show ipsec {brief | detailed} ip\_or\_mac\_addr** : アクティブな IPSec セキュリティ アソシエーションの簡単な概要または詳しい要約を表示します。
- 次のコマンドを入力して、1 台または複数の RADIUS サーバの統計情報をクリアします。  
**clear stats radius {auth | acct} {index | all}**
- 次のコマンドを入力して、コントローラが RADIUS サーバに到達できることを確認します。  
**ping server\_ip\_address**

## コントローラによって送信される RADIUS 認証属性

次の表は、Access-Request パケットおよび Access-Accept パケットで、コントローラと RADIUS サーバ間で送信される RADIUS 認証属性を示しています。

表 8 : Access-Request パケットで送信される認証属性

| 属性 ID | 説明                        |
|-------|---------------------------|
| 1     | User-Name                 |
| 2     | Password                  |
| 3     | CHAP-Password             |
| 4     | NAS-IP-Address            |
| 5     | NAS-Port                  |
| 6     | Service-Type <sup>4</sup> |
| 12    | Framed-MTU                |

| 属性 ID | 説明                            |
|-------|-------------------------------|
| 30    | Called-Station-ID (MAC アドレス)  |
| 31    | Calling-Station-ID (MAC アドレス) |
| 32    | NAS-Identifier                |
| 33    | Proxy-State                   |
| 60    | CHAP-Challenge                |
| 61    | NAS-Port-Type                 |
| 79    | EAP-Message                   |
| 243   | TPLUS-Role                    |

- 4 RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性 (6) を設定する必要があります。読み取り専用アクセスが必要な場合は [Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。

表 9 : Access-Accept パケットで受け付けられる認証属性 (シスコ)

| 属性 ID | 説明                          |
|-------|-----------------------------|
| 1     | Cisco-LEAP-Session-Key      |
| 2     | Cisco-Keywrap-Msg-Auth-Code |
| 3     | Cisco-Keywrap-NonCE         |
| 4     | Cisco-Keywrap-Key           |
| 5     | Cisco-URL-Redirect          |
| 6     | Cisco-URL-Redirect-ACL      |



(注) シスコ固有の属性 Auth-Algo-Type および SSID はサポートされません。

表 10 : Access-Accept パケットで受け付けられる認証属性 (標準)

| 属性 ID | 説明                                                                                                                                                                                                                |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6     | Service-Type RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性 (6) を設定する必要があります。読み取り専用アクセスが必要な場合は [Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。 |



|    |                    |
|----|--------------------|
| 8  | Framed-IP-Address  |
| 25 | Class              |
| 26 | Vendor-Specific    |
| 27 | Timeout            |
| 29 | Termination-Action |
| 40 | Acct-Status-Type   |
| 64 | Tunnel-Type        |
| 79 | EAP-Message        |
| 81 | Tunnel-Group-ID    |



(注) メッセージ認証はサポートされていません。

表 11 : *Access-Accept* パケットで受け付けられる認証属性 (*Microsoft*)

| 属性 ID | 説明                  |
|-------|---------------------|
| 11    | MS-CHAP-Challenge   |
| 16    | MS-MPPE-Send-Key    |
| 17    | MS-MPPE-Receive-Key |
| 25    | MS-MSCHAP2-Response |
| 26    | MS-MSCHAP2-Success  |

表 12 : *Access-Accept* パケットで受け付けられる認証属性 (*Airespace*)

| 属性 ID | 説明                                   |
|-------|--------------------------------------|
| 1     | VAP-ID                               |
| 3     | DSCP                                 |
| 4     | 8021P-Type                           |
| 5     | VLAN-Interface-Name                  |
| 6     | ACL-Name                             |
| 7     | Data-Bandwidth-Average-Contract      |
| 8     | Real-Time-Bandwidth-Average-Contract |
| 9     | Data-Bandwidth-Burst-Contract        |

| 属性 ID | 説明                                      |
|-------|-----------------------------------------|
| 10    | Real-Time-Bandwidth-Burst-Contract      |
| 11    | Guest-Role-Name                         |
| 13    | Data-Bandwidth-Average-Contract-US      |
| 14    | Real-Time-Bandwidth-Average-Contract-US |
| 15    | Data-Bandwidth-Burst-Contract-US        |
| 16    | Real-Time-Bandwidth-Burst-Contract-US   |

## Access-Accept パケットで受け付けられる認証属性 (Airespace)

この項では、Cisco WLC で現在サポートされている RADIUS 認証の Airespace 属性について説明します。

### VAP ID

この属性は、クライアントが属する WLAN の WLAN ID を示します。RADIUS Access Accept に WLAN-ID 属性が指定されている場合、システムでは認証後に WLAN-ID (SSID) がクライアントステーションに適用されます。WLAN ID は、Cisco WLC によって IPsec 以外のすべての認証のインスタンスで送信されます。Web 認証では、Cisco WLC が AAA サーバからの認証応答で WLAN-ID 属性を受信し、これが WLAN の ID に一致しない場合、認証が拒否されます。Dot1X/Mac フィルタリングも拒否されます。AAA サーバからの応答に基づく拒否は、SSID Cisco-AVPair サポートが原因です。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+
| WLAN ID (VALUE) |
+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 1
- Vendor length – 4
- Value – クライアントが属する WLAN の ID。

## QoS-Level

この属性は、スイッチングファブリック内、および無線経由のモバイルクライアントのトラフィックに適用される QoS レベルを示しています。この例は、QoS-Level 属性フォーマットの要約を示しています。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| QoS Level |
+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – 3 オクテット :
  - 3 – Bronze (バックグラウンド)
  - 0 – Silver (ベストエフォート)
  - 1 – Gold (ビデオ)
  - 2 – Platinum (音声)

## Diffserv コード ポイント (DSCP)

DSCP は QoS レベルに基づく Diffserv の提供に使用できるパケットヘッダーコードです。この属性は、クライアントに適用される DSCP 値を定義します。RADIUS Access Accept に値が指定されている場合、DSCP 値によって、WLAN プロファイルで指定された DSCP 値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| DSCP (VALUE) |
+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179

- Vendor type – 3
- Vendor length – 4
- Value – クライアントに適用される DSCP 値。

### 802.1p Tag Type

クライアントから受信した 802.1p VLAN タグ (アクセス プライオリティを定義する)。このタグはクライアントとネットワーク間のパケットの QoS レベルにマッピングされます。この属性は、クライアントに適用される 802.1p プライオリティを定義します。RADIUS Access Accept に値が指定されている場合、802.1p 値によって、WLAN プロファイルで指定されたデフォルトが上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| 802.1p (VALUE) |
+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 4
- Vendor length – 3
- Value – クライアントに適用される 802.1p プライオリティ。

### VLAN Interface Name

この属性は、クライアントが関連付けられる VLAN インターフェイスを示します。Interface-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| Interface Name... |
+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5

- Vendor length ->0
- Value - クライアントが割り当てられるインターフェイスの名前を含む文字列



(注) この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

### ACL-Name

この属性は、クライアントに適用される ACL 名を示します。ACL-Name 属性形式の要約を次に示します。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+
| ACL Name... |
+-----+-----+-----+-----+-----+-----+

```

- Type - 26 (ベンダー固有)
- Length ->7
- Vendor-Id - 14179
- Vendor type - 6
- Vendor length ->0
- Value - クライアントに対して使用する ACL の名前を含む文字列

### Data Bandwidth Average Contract

この属性は、レート制限値です。TCPなどの非リアルタイムトラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Data Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均データレート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+
| Data Bandwidth Average Contract... |
+-----+-----+-----+-----+-----+-----+

```

- Type - 26 (ベンダー固有)
- Length - 10

- Vendor-Id – 14179
- Vendor type – 7
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Real Time Bandwidth Average Contract

この属性は、レート制限値です。UDP などのリアルタイム トラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均リアルタイム レート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| Real Time Bandwidth Average Contract...
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 8
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Data Bandwidth Burst Contract

この属性は、レート制限値です。TCP などの非リアルタイム トラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Data Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバースト データ レート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| Data Bandwidth Burst Contract...
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10

- Vendor-Id – 14179
- Vendor type – 9
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Real Time Bandwidth Burst Contract

この属性は、レート制限値です。UDP などのリアルタイム トラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバーストリアルタイム レート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| Real Time Bandwidth Burst Contract...
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 10
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Guest Role Name

この属性は、認証ユーザに適用される帯域幅コントラクト値を提供します。RADIUS Access Accept に値が指定されている場合、ゲストロールに定義された帯域幅コントラクト値によって、WLAN に指定された帯域幅コントラクト値 (QoS 値に基づく) が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| GuestRoleName ...
+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179

- Vendor type – 11
- Vendor length – ゲスト ロール名の長さに基づく変数
- Value – 英数字の文字列

### Data Bandwidth Average Contract Upstream

この属性は、レート制限値です。TCPなどの非リアルタイムトラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。この値は、無線から有線へのアップストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Data Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均データレート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| Type | Length | Vendor-Id
+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| Data Bandwidth Average Contract Upstream...
+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 13
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Real Time Bandwidth Average Contract Upstream

この属性は、レート制限値です。UDPなどのリアルタイムトラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。この値は、無線から有線へのアップストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均リアルタイムレート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+
| Type | Length | Vendor-Id
+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+
| Real Time Bandwidth Average Contract Upstream...
+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179



- Vendor type – 14
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Data Bandwidth Burst Contract Upstream

この属性は、レート制限値です。TCPなどの非リアルタイムトラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。この値は、無線から有線へのアップストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Data Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバーストデータ レート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Data Bandwidth Burst Contract Upstream...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 15
- Vendor length – 4
- Value – 値 (Kbps 単位)

### Real Time Bandwidth Burst Contract Upstream

この属性は、レート制限値です。UDPなどのリアルタイムトラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。この値は、無線から有線へのアップストリーム方向にのみ当てはまります。RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバーストリアルタイム レート値が上書きされます。フィールドは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Real Time Bandwidth Burst Contract Upstream...
+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179

- Vendor type – 16
- Vendor length – 4
- Value – 値 (Kbps 単位)

## RADIUS アカウンティング属性

次の表に、コントローラから RADIUS サーバに送信されるアカウンティング要求の RADIUS アカウンティング属性を示します。

表 13: アカウンティング要求のアカウンティング属性

| 属性 ID | 説明                                            |
|-------|-----------------------------------------------|
| 1     | User-Name                                     |
| 4     | NAS-IP-Address                                |
| 5     | NAS-Port                                      |
| 8     | Framed-IP-Address                             |
| 25    | Class                                         |
| 30    | Called-Station-ID (MAC アドレス)                  |
| 31    | Calling-Station-ID (MAC アドレス)                 |
| 32    | NAS-Identifier                                |
| 40    | Accounting-Status-Type                        |
| 41    | Accounting-Delay-Time (ストップおよび中間メッセージのみ)      |
| 42    | Accounting-Input-Octets (ストップおよび中間メッセージのみ)    |
| 43    | Accounting-Output-Octets (ストップおよび中間メッセージのみ)   |
| 44    | Accounting-Session-ID                         |
| 45    | Accounting-Authentic                          |
| 46    | Accounting-Session-Time (ストップおよび中間メッセージのみ)    |
| 47    | Accounting-Input-Packets (ストップおよび中間メッセージのみ)   |
| 48    | Accounting-Output-Packets (ストップおよび中間メッセージのみ)  |
| 49    | Accounting-Terminate-Cause (ストップおよび中間メッセージのみ) |
| 52    | Accounting-Input-Gigawords                    |
| 53    | Accounting-Output-Gigawords                   |
| 55    | Event-Timestamp                               |

| 属性 ID | 説明                  |
|-------|---------------------|
| 64    | Tunnel-Type         |
| 65    | Tunnel-Medium-Type  |
| 81    | Tunnel-Group-ID     |
|       | IPv6-Framed-Prefix  |
| 190   | IPv6-Framed-Address |

次の表に Accounting-Status-Type 属性（40）のさまざまな値の一覧を示します。

表 14 : *Accounting-Status-Type* 属性の値

| 属性 ID | 説明                 |
|-------|--------------------|
| 1     | Start              |
| 2     | Stop               |
| 3     | Interim-Update     |
| 7     | Accounting-On      |
| 8     | Accounting-Off     |
| 9-14  | トンネリングのアカウントング用に予約 |
| 15    | Failed 用に予約        |





## 第 44 章

# TACACS+ の設定

---

- [TACACS+ について, 455 ページ](#)
- [ACS 上での TACACS+ の設定, 459 ページ](#)
- [TACACS+ の設定 \(GUI\) , 461 ページ](#)
- [TACACS+ の設定 \(CLI\) , 463 ページ](#)
- [TACACS+ 管理サーバのログの表示, 465 ページ](#)

## TACACS+ について

Terminal Access Controller Access Control System Plus (TACACS+) は、コントローラへの管理アクセスを取得しようとするユーザに中央管理されたセキュリティを提供する、クライアント/サーバプロトコルです。このプロトコルは、ローカルおよびRADIUSに類似したバックエンドのデータベースとして機能します。ただし、ローカルおよびRADIUSでは、認証サポートと制限のある認可サポートしか提供されないのに対し、TACACS+ では、次の3つのサービスが提供されます。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

コントローラで TACACS+ サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。認証サービスおよび認可サービスは、互いに密接に関連しています。たとえば、ローカルまたはRADIUSデータベースを使用して認証が実行された場合、認可ではそのローカルまたはRADIUSデータベース内のユーザに関連したアクセス権 (read-only、read-write、lobby-adminのいずれか) が使用され、TACACS+ は使用されません。同様に、TACACS+ を使用して認証が実行されると、認可は TACACS+ に関連付けられます。



---

(注) 複数のデータベースを設定する場合、コントローラ GUI または CLI を使用して、バックエンドデータベースが試行される順序を指定できます。

---

- **認可**：ユーザのアクセスレベルに基づいて、ユーザがコントローラで実行できる処理を決定するプロセス。

TACACS+ の場合、認可は特定の処理ではなく、権限（またはロール）に基づいて実行されます。利用可能なロールは、コントローラ GUI の 7 つのメニューオプション ([MONITOR]、[WLAN]、[CONTROLLER]、[WIRELESS]、[SECURITY]、[MANAGEMENT]、および [COMMANDS]) に対応しています。ロビーアンバサダー権限のみを必要とするユーザは、追加のロールである LOBBY を使用できます。ユーザが割り当てられるロールは、TACACS+ サーバ上で設定されます。ユーザは 1 つまたは複数のロールに対して認可されます。最小の認可は MONITOR のみで、最大は ALL です。ALL では、ユーザは 7 つのメニューオプションすべてに関連付けられた機能を実行できるよう認可されます。たとえば、SECURITY のロールを割り当てられたユーザは、[Security] メニューに表示される（または CLI の場合はセキュリティコマンドとして指定される）すべてのアイテムに対して変更を実行できます。ユーザが特定のロール（WLAN など）に対して認可されていない場合でも、そのユーザは読み取り専用モード（または関連する CLI の **show** コマンド）で、そのメニューオプションにアクセスできます。TACACS+ 許可サーバが接続不能または認可不能になった場合、ユーザはコントローラにログインできません。



- 
- (注) ユーザが割り当てられたロールでは許可されていないコントローラ GUI のページに変更を加えようとする、十分な権限がないことを示すメッセージが表示されます。ユーザが割り当てられたロールでは許可されていないコントローラ CLI コマンドを入力すると、実際にはそのコマンドは実行されていないのに、正常に実行されたというメッセージが表示されます。この場合、「Insufficient Privilege! Cannot execute command!」というメッセージがさらに表示され、コマンドを実行するための十分な権限がないことがユーザに通知されます。
- 

- **アカウントिंग**：ユーザによる処理と変更を記録するプロセス。

ユーザによる処理が正常に実行される度に、TACACS+ アカウントिंगサーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモートホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。TACACS+ アカウントिंगサーバが接続不能になった場合、ユーザはセッションを中断されずに続行できます。

RADIUS でユーザデータグラムプロトコル (UDP) を使用するのとは異なり、TACACS+ では、転送にトランスミッションコントロールプロトコル (TCP) を使用します。1 つのデータベースを維持し、TCP ポート 49 で受信要求をリッスンします。アクセスコントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

最大 3 台の TACACS+ 認証サーバ、認可サーバ、およびアカウントिंगサーバをそれぞれ設定できます。たとえば、1 台の TACACS+ 認証サーバを中央に配置し、複数の TACACS+ 許可サーバを異なる地域に配置できます。同じタイプの複数のサーバを設定していると、最初のサーバで

障害が発生したり、接続不能になっても、コントローラは自動的に 2 台目、および必要に応じて 3 台目のサーバを試行します。



(注) 複数の TACACS+ サーバが冗長性のために設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバにおいてユーザ データベースを同一にする必要があります。

次に、TACACS+ についての注意事項を示します。

- CiscoSecure Access Control Server (ACS) とコントローラの両方で、TACACS+ を設定する必要があります。コントローラは、GUI または CLI のいずれかを使用して設定できます。
- TACACS+ は、CiscoSecure ACS バージョン 3.2 以降のリリースでサポートされます。実行しているバージョンに対応する CiscoSecure ACS のマニュアルを参照してください。
- ワンタイムパスワード (OTP) は、TACACS を使用しているコントローラでサポートされません。この設定では、コントローラがトランスペアレント パススルー デバイスとして動作します。コントローラは、クライアント動作をチェックせずにすべてのクライアント要求を TACACS サーバに転送します。OTP を使用する場合は、クライアントが正しく機能するためにはコントローラへの接続を 1 つ確立する必要があります。現在、コントローラには、複数の接続を確立しようとしているクライアントを修正するチェック機能はありません。
- 再認証が繰り返し試行されたり、プライマリサーバがアクティブで接続可能なときにコントローラがバックアップサーバにフォールバックしたりする場合には、TACACS+ 認証サーバ、認可サーバ、およびアカウントサーバの再送信のタイムアウト値を増やすことをお勧めします。デフォルトの再送信のタイムアウト値は 2 秒です。この値は最大 30 秒まで増やすことができます。

### TACACS+ DNS

完全修飾ドメイン名 (FQDN) を使用できます。これにより、必要に応じて IP アドレスを変更できます (たとえば、ロード バランシングの更新)。サブメニューの [DNS] が [Security > AAA > TACACS+] メニューに追加されます。これを使用して、DNS から TACACS+ IP 情報を取得できます。DNS クエリーはデフォルトでは無効になっています。

スタティック リストおよび DNS リストを同時に使用することはできません。DNS によって返されるアドレスはスタティック エントリを上書きします。

スタティック リストおよび DNS リストを同時に使用することはできません。DNS によって返されるアドレスはスタティック エントリを上書きします。

DNS AAA は、中央認証を使用する FlexConnect AP クライアントに対して有効です。

DNS AAA は、FlexConnect AP グループに対する RADIUS の定義ではサポートされていません。ローカルスイッチングを使用する FlexConnect クライアントの場合、手動で AAA を定義する必要があります。

不正、802.1X、Web 認証、MAC フィルタリング、メッシュ、およびグローバル リストを使用するその他の機能は、DNS 定義のサーバを使用します。

## TACACS+ VSA

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワークアクセスサーバと TACACS+ サーバの間でベンダー固有属性（VSA）を伝達する方法が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、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。

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用した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、サポートされるオプションのベンダータイプは 1（名前付き `cisco-av-pair`）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

`protocol` は、特定の許可タイプを表すシスコの属性です。`separator` は、必須属性の場合は =（等号）、オプションの属性の場合は \*（アスタリスク）です。



## ACS 上での TACACS+ の設定

ステップ 1 ACS のメインページで、[Network Configuration] を選択します。

ステップ 2 [AAA Clients] の下の [Add Entry] を選択し、使用しているコントローラをサーバに追加します。[Add AAA Client] ページが表示されます。

図 41 : CiscoSecure ACS の [Add AAA Client] ページ

The screenshot shows the 'Add AAA Client' configuration page in a Microsoft Internet Explorer browser window. The browser address bar shows 'http://127.0.0.1:19491/'. The page title is 'Network Configuration' and the sub-page title is 'Add AAA Client'. The left sidebar contains a navigation menu with options like 'User Setup', 'Group Setup', 'Shared Profile Components', 'Network Configuration', 'System Configuration', 'Interface Configuration', 'Administration Control', 'External User Databases', 'Posture Validation', 'Network Access Profiles', 'Reports and Activity', and 'Online Documentation'. The main content area has the following fields and options:

- AAA Client Hostname: [Text Input]
- AAA Client IP Address: [Text Input]
- Shared Secret: [Text Input]
- RADIUS Key Wrap:
  - Key Encryption Key: [Text Input]
  - Message Authenticator Code Key: [Text Input]
  - Key Input Format:  ASCII  Hexadecimal
- Authenticate Using: [Dropdown Menu] (Selected: TACACS+ (Cisco IOS))
- 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:

ステップ 3 [AAA Client Hostname] テキスト ボックスに、コントローラの名前を入力します。

ステップ 4 [AAA Client IP Address] テキスト ボックスに、コントローラの IP アドレスを入力します。

ステップ 5 [Shared Secret] テキスト ボックスに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

(注) 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

- ステップ 6 [Authenticate Using] ドロップダウン リストから [TACACS+ (Cisco IOS)] を選択します。
- ステップ 7 [Submit + Apply] をクリックして、変更内容を保存します。
- ステップ 8 ACS のメイン ページで、左のナビゲーション ペインから [Interface Configuration] を選択します。
- ステップ 9 [TACACS+ (Cisco IOS)] を選択します。 [TACACS+ (Cisco)] ページが表示されます。
- ステップ 10 [TACACS+ Services] の [Shell (exec)] チェックボックスをオンにします。
- ステップ 11 [New Services] で最初のチェックボックスをオンにし、 [Service] テキスト ボックスに **ciscowlc**、 [Protocol] テキスト ボックスに **common** と入力します。
- ステップ 12 [Advanced Configuration] オプションの [Advanced TACACS+ Features] チェックボックスをオンにします。
- ステップ 13 [Submit] をクリックして変更を保存します。
- ステップ 14 ACS のメイン ページで、左のナビゲーション ペインから [System Configuration] を選択します。
- ステップ 15 [Logging] を選択します。
- ステップ 16 [Logging Configuration] ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。
- ステップ 17 ACS のメイン ページで、左のナビゲーション ペインから [Group Setup] を選択します。
- ステップ 18 [Group] ドロップダウン リストから、以前に作成したグループを選択します。  
 (注) この手順では、ユーザが割り当てられることになるロールに基づいて、ACS のグループにすでにユーザが割り当てられていることを想定しています。
- ステップ 19 [Edit Settings] をクリックします。 [Group Setup] ページが表示されます。
- ステップ 20 [TACACS+ Settings] の [ciscowlc common] チェックボックスをオンにします。
- ステップ 21 [Custom Attributes] チェックボックスをオンにします。
- ステップ 22 [Custom Attributes] の下のテキストボックスで、このグループに割り当てるロールを指定します。 使用可能なロールは、MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT、COMMANDS、ALL、および LOBBY です。 最初の 7 つのロールは、コントローラ GUI のメニュー オプションに対応しており、これら特定のコントローラ機能へのアクセスを許可します。 特定のタスクに対する権限がユーザに与えられていない場合でも、ユーザは読み取り専用モードでそのタスクにアクセスできるようになります。 グループでの必要性に応じて、1 つまたは複数のロールを入力できます。 7 つのロールすべてを指定するには ALL を、ロビー アンバサダー ロールを指定するには LOBBY を使用します。 次の形式を使用してロールを入力します。  
**role=ROLE**
- たとえば、特定のユーザ グループに対して WLAN、CONTROLLER、および SECURITY のロールを指定するには、次のテキストを入力します。
- ```
role1=WLAN
role2=CONTROLLER
role3=SECURITY?
```
- あるユーザ グループに 7 つのロールすべてに対するアクセスを付与するには、次のテキストを入力します。
- ```
role1=ALL?
```

- (注) 必ず上記の形式を使用してロールを入力するようにしてください。ロールはすべて大文字で入力する必要があり、テキスト間にスペースは挿入できません。
- (注) MONITOR ロールまたは LOBBY ロールは、その他のロールと組み合わせることはできません。[Custom Attributes] テキストボックスにこれら2つのロールのどちらかを指定すると、追加のロールが指定された場合でも、ユーザには MONITOR または LOBBY 権限のみが付与されます。

ステップ 23 [Submit] をクリックして変更を保存します。

## TACACS+ の設定 (GUI)

ステップ 1 [Security] > [AAA] > [TACACS+] の順に選択します。

ステップ 2 次のいずれかの操作を行います。

- TACACS+ サーバを認証用に設定する場合は、[Authentication] を選択します。
- TACACS+ サーバを許可用に設定する場合は、[Authorization] を選択します。
- TACACS+ サーバをアカウントिंग用に設定する場合、[Accounting] をクリックします。

(注) 認証、許可、アカウントिंगの設定に使用されるページでは、すべて同じテキストボックスが表示されます。そのため、ここでは [Authentication] ページを例にとって、設定の手順を一度だけ示します。同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

(注) TACACS+ を使用して基本的な管理認証が正常に行われるには、WLC で認証サーバと許可サーバを設定する必要があります。アカウントिंगの設定は任意です。

[TACACS+ (Authentication, Authorization, または Accounting) Servers] ページが表示されます。このページでは、これまでに設定されたすべての TACACS+ サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 3 次のいずれかの操作を行います。

- 既存の TACACS+ サーバを編集するには、そのサーバのサーバインデックス番号をクリックします。[TACACS+ (Authentication, Authorization, or Accounting) Servers > Edit] ページが表示されます。

- TACACS+ サーバを追加するには、[New] をクリックします。[TACACS+ (Authentication, Authorization, または Accounting) Servers > New] ページが表示されます。

- ステップ 4** 新しいサーバを追加している場合は、[Server Index (Priority)] ドロップダウンリストから数字を選択し、同じサービスを提供するその他の設定済みの TACACS+ サーバに対してこのサーバの優先順位を指定します。最大 3 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目および必要に応じて 3 番目のサーバへの接続を試行します。
- ステップ 5** 新しいサーバを追加している場合は、[Server IP Address] テキストボックスに TACACS+ サーバの IP アドレスを入力します。
- ステップ 6** [Shared Secret Format] ドロップダウンリストから [ASCII] または [Hex] を選択し、コントローラと TACACS+ サーバ間で使用される共有秘密キーの形式を指定します。デフォルト値は [ASCII] です。
- ステップ 7** [Shared Secret] テキストボックスと [Confirm Shared Secret] テキストボックスに、コントローラとサーバ間で認証に使用される共有秘密キーを入力します。  
(注) 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。
- ステップ 8** 新しいサーバを追加している場合は、[Port Number] テキストボックスに、インターフェイスプロトコルに対応する TACACS+ サーバの TCP ポート番号を入力します。有効な範囲は 1 ~ 65535 で、デフォルト値は 49 です。
- ステップ 9** [Server Status] テキストボックスから [Enabled] を選択してこの TACACS+ サーバを有効にするか、[Disabled] を選択して無効にします。デフォルト値は [Enabled] です。
- ステップ 10** [Server Timeout] テキストボックスに、再送信の間隔を秒単位で入力します。有効な範囲は 5 ~ 30 秒で、デフォルト値は 5 秒です。  
(注) 再認証が繰り返し試行されたり、プライマリサーバがアクティブで接続可能なときにコントローラがバックアップサーバにフォールバックしたりする場合には、タイムアウト値を増やすことをお勧めします。
- ステップ 11** [Apply] をクリックします。
- ステップ 12** 次の手順で、TACACS+ DNS パラメータを指定します。
- a) [Security] > [AAA] > [TACACS+] > [DNS] を選択します。[TACACS DNS Parameters] ページが表示されます。
  - b) [DNS Query] チェックボックスをオンまたはオフにします。
  - c) [Port Number] テキストボックスに、認証ポート番号を入力します。有効な範囲は 1 ~ 65535 です。アカウントングポート番号は認証ポート番号に 1 を加えた値です。たとえば、認証ポート番号を 1812 と定義すると、アカウントングポート番号は 1813 です。アカウントングポート番号は常に認証ポート番号から取得されます。
  - d) [Secret Format] ドロップダウンリストから、秘密を設定する形式を選択します。有効なオプションは ASCII と Hex です。
  - e) 選択した形式に応じて秘密を入力して確定します。  
(注) すべてのサーバで同じ認証ポートおよび同じ秘密を使用する必要があります。

- f) [DNS Timeout] テキスト ボックスに、DNS サーバから最新の更新を取得するために DNS クエリーがリフレッシュされるまでの日数を入力します。
- g) [URL] テキスト ボックスに、TACACS+ サーバの完全修飾ドメイン名または絶対ドメイン名を入力します。
- h) [Server IP Address] テキスト ボックスに、DNS サーバの IP アドレスを入力します。
- i) [Apply] をクリックします。

ステップ 13 [Save Configuration] をクリックします。

ステップ 14 同じサーバ上で、または追加の TACACS+ サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 15 [Security] > [Priority Order] > [Management User] の順に選択し、複数のデータベースを設定する際の認証の順序を指定します。[Priority Order > Management User] ページが表示されます。

ステップ 16 [Order Used for Authentication] テキスト ボックスで、コントローラが管理ユーザを認証する際にどのサーバを優先するかを指定します。  
[Not Used] テキスト ボックスと [Order Used for Authentication] テキスト ボックスの間でサーバを移動するには、[>] および [<] ボタンを使用します。希望するサーバが [Order Used for Authentication] テキスト ボックスに表示されたら、[Up] ボタンと [Down] ボタンを使用して優先するサーバをリストの先頭に移動します。デフォルトで、ローカル データベースは常に最初に検索されます。ユーザ名が見つからない場合、コントローラは、RADIUS に設定されている場合は RADIUS サーバへの切り換え、TACACS+ に設定されている場合は TACACS+ サーバへの切り換えを行います。デフォルトの設定はローカル、RADIUS の順になっています。

ステップ 17 [Apply] をクリックします。

ステップ 18 [Save Configuration] をクリックします。

## TACACS+ の設定 (CLI)

- 次のコマンドを入力して、TACACS+ 認証サーバを設定します。

- **config tacacs auth add index server ip\_address port# {ascii | hex} shared\_secret** : TACACS+ 認証サーバを追加します。
- **config tacacs auth delete index** : 以前に追加された TACACS+ 認証サーバを削除します。
- **config tacacs auth (enable | disable) index** : TACACS+ 認証サーバを有効または無効にします。
- **config tacacs auth server-timeout index timeout** : TACACS+ 認証サーバの再送信のタイムアウト値を設定します。

- 次のコマンドを入力して、TACACS+ 許可サーバを設定します。

- **config tacacs athr add index server ip\_address port# {ascii | hex} shared\_secret** : TACACS+ 許可サーバを追加します。

- **config tacacs athr delete index** : 以前に追加された TACACS+ 許可サーバを削除します。
  - **config tacacs athr (enable | disable) index** : TACACS+ 許可サーバを有効または無効にします。
  - **config tacacs athr server-timeout index timeout** : TACACS+ 許可サーバの再送信のタイムアウト値を設定します。
- 次のコマンドを入力して、TACACS+ アカウンティング サーバを設定します。
    - **config tacacs acct add index server\_ip\_address port# {ascii | hex} shared\_secret** : TACACS+ アカウンティング サーバを追加します。
    - **config tacacs acct delete index** : 以前に追加された TACACS+ アカウンティング サーバを削除します。
    - **config tacacs acct (enable | disable) index** : TACACS+ アカウンティング サーバを有効または無効にします。
    - **config tacacs acct server-timeout index timeout** : TACACS+ アカウンティング サーバの再送信のタイムアウト値を設定します。
- 次のコマンドを入力して、TACACS+ の統計情報を表示します
    - **show tacacs summary** : TACACS+ サーバと統計情報の概要を表示します。
    - **show tacacs auth stats** : TACACS+ 認証サーバの統計情報を表示します。
    - **show tacacs athr stats** : TACACS+ 許可サーバの統計情報を表示します。
    - **show tacacs acct stats** : TACACS+ アカウンティング サーバの統計情報を表示します。
- 次のコマンドを入力して、1 台または複数の TACACS+ サーバの統計情報をクリアします。  
**clear stats tacacs [auth | athr | acct] {index | all}**
- 次のコマンドを入力して、複数のデータベースを設定する際の認証の順序を設定します。デフォルト設定では local、radius の順になっています。  
**config aaa auth mgmt [radius | tacacs]**  
現在の管理認証サーバの順序を表示するには、**show aaa auth** コマンドを入力します。
- 次のコマンドを入力して、コントローラが TACACS+ サーバに到達できることを確認します。  
**ping server\_ip\_address**
- 次のコマンドを入力して、TACACS+ DNS パラメータを設定します。
    - **config tacacs dns global port-num {ascii | hex} secret** : TACACS+ DNS のグローバルポート番号と秘密情報を追加します。
    - **config tacacs dns query url timeout-in-days** : TACACS+ サーバの FQDN、および DNS サーバから最新の更新を取得するためにリフレッシュが実行されるまでのタイムアウトを設定します。

- `config tacacs dns serverip ip-addr` : DNSサーバの IP アドレスを設定します。
- `config tacacs dns {enable | disable}` : DNS クエリーを有効または無効にします。
- 次のコマンドを入力して、TACACS+ のデバッグを有効または無効にします。  
`debug aaa tacacs {enable | disable}`
- 次のコマンドを入力して、変更を保存します。  
`save config`

## TACACS+ 管理サーバのログの表示

ステップ1 ACS のメインページで、左のナビゲーションペインから [Reports and Activity] を選択します。

ステップ2 [Reports] の [TACACS+ Administration] を選択します。

表示するログの日付に対応する .csv ファイルをクリックします。 [TACACS+ Administration .csv] ページが表示されます。

図 42 : CiscoSecure ACS の [TACACS+ Administration .csv] ページ

The screenshot shows the CiscoSecure ACS web interface. The left sidebar contains navigation 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 displays the 'Reports and Activity' section, with 'TACACS+ Administration' selected. Below this, there is a table titled 'Tacacs+ Administration active.csv' with columns for Date, Time, User-Name, Group-Name, cmd, priv-lvl, service, task id, NAS-IP-Address, and addr. The table contains several rows of log entries for the date 01/24/2007 at 19:35:42, showing various commands like 'wlan interface 1 dyn1', 'wlan enable 1', 'wlan mac-filtering enable 1', 'wlan security 802.1X disable 1', 'wlan qos 1 bronze', and 'wlan dhcp\_server 1'.

| Date       | Time     | User-Name    | Group-Name | cmd                            | priv-lvl | service | task id | NAS-IP-Address  | addr            |
|------------|----------|--------------|------------|--------------------------------|----------|---------|---------|-----------------|-----------------|
| 01/24/2007 | 19:35:42 | avinash_wlan | Group 12   | wlan interface 1 dyn1          | 9        | shell   | 1937    | 209.165.200.225 | 209.165.200.225 |
| 01/24/2007 | 19:35:42 | avinash_wlan | Group 12   | wlan enable 1                  | 9        | shell   | 1952    | 209.165.200.225 | 209.165.200.225 |
| 01/24/2007 | 19:35:42 | avinash_wlan | Group 12   | wlan mac-filtering enable 1    | 9        | shell   | 1948    | 209.165.200.225 | 209.165.200.225 |
| 01/24/2007 | 19:35:42 | avinash_wlan | Group 12   | wlan security 802.1X disable 1 | 9        | shell   | 1946    | 209.165.200.225 | 209.165.200.225 |
| 01/24/2007 | 19:35:42 | avinash_wlan | Group 12   | wlan qos 1 bronze              | 9        | shell   | 1944    | 209.165.200.225 | 209.165.200.225 |
| 01/24/2007 | 19:35:42 | avinash_wlan | Group 12   | wlan dhcp_server 1             | 9        | shell   | 1942    | 209.165.200.225 | 209.165.200.225 |

このページは、次の情報を表示します。

- 処理が実行された日付と時刻

- 処理を実行したユーザの名前と割り当てられたロール
- ユーザが属するグループ
- ユーザが実行した特定の処理
- 処理を実行したユーザの権限レベル
- コントローラの IP アドレス
- 処理が実行されたノートパソコンまたはワークステーションの IP アドレス

単一の処理（またはコマンド）が、コマンド内のパラメータごとに、複数回ログ記録される場合があります。たとえば、**snmp community ipaddr ip\_address subnet\_mask community\_name** コマンドを入力すると、ある行では、IPアドレスはログに記録されても、サブネットマスクとコミュニティ名はログに「E」と記録されることがあります。また別の行では、サブネットマスクがログに記録され、IPアドレスとコミュニティ名はログに「E」と記録されることがあります。次の図の例の最初の行と3番目の行を参照してください。

図 43 : CiscoSecure ACS の [TACACS+ Administration .csv] ページ

| Date       | Time     | User-Name          | Group-Name | cmd                                     | priv-ly | service | task_id | NAS-IP-Address |
|------------|----------|--------------------|------------|-----------------------------------------|---------|---------|---------|----------------|
| 02/13/2007 | 14:07:19 | avinash_management | Group 16   | snmp community ipaddr E 255.255.255.0 E | 129     | shell   | 217     | 209.165.200.   |
| 02/13/2007 | 14:07:19 | avinash_management | Group 16   | snmp community mode enable cisco        | 129     | shell   | 219     | 209.165.200.   |
| 02/13/2007 | 14:07:19 | avinash_management | Group 16   | snmp community ipaddr 209.165.200. E E  | 129     | shell   | 216     | 209.165.200.   |
| 02/13/2007 | 14:07:19 | avinash_management | Group 16   | snmp community accessmode rw cisco      | 129     | shell   | 218     | 209.165.200.   |
| 02/13/2007 | 14:07:19 | avinash_management | Group 16   | snmp community ipaddr E 255.255.255.0 E | 129     | shell   | 217     | 209.165.200.   |





# 第 45 章

## FIPS 設定、CC、UCAPL

- FIPS の概要, 467 ページ
- FIPS のセルフテスト, 468 ページ
- CC について, 469 ページ
- UCAPL について, 469 ページ
- FIPS の設定 (CLI) , 469 ページ
- CC の設定 (CLI) , 470 ページ
- UCAPL の設定 (CLI) , 470 ページ

### FIPS の概要

連邦情報処理標準 (FIPS) 140-2 は、暗号化モジュールの検証に使用されるセキュリティ規格です。暗号化モジュールは、米国政府機関およびその他の規制産業 (金融機関や医療機関など) が取扱注意ではあるが機密ではない (SBU) 情報の収集、保存、転送、共有、および配布に使用するために民間企業によって製造されます。

FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。FIPS の詳細については、<http://csrc.nist.gov/> を参照してください。

#### ロールおよびサービスについて

- **AP ロール** : コントローラ (MFP、802.11i、iGTK) に関連付けられたアクセス ポイントのロール。
- **クライアント ロール** : コントローラに関連付けられたワイヤレス クライアントのロール。
- **ユーザ ロール** : 読み取り専用権限を持つ管理ユーザ。

- **Crypto Officer (CO) ロール**：読み取りおよび書き込み権限を持つ管理ユーザで、暗号の初期化や管理操作を実行できる者。



(注) FIPS 140-2 で定義されているセキュリティ強化のレベルは 4 つあります。

## FIPS のセルフテスト

暗号モジュールは、適正に動作していることを確認するために、電源投入時のセルフテストと条件付きセルフテストを実行しなければなりません。

電源投入時セルフテストは、デバイスの電源が投入された後に自動的に実行されます。デバイスが FIPS モードになるのは、すべてのセルフテストが正常に完了した後だけです。いずれかのセルフテストが失敗すると、デバイスはシステム メッセージをログに記録し、エラー状態に移行します。

既知解テスト (KAT) を利用すると、暗号アルゴリズムは正しい出力があらかじめわかっているデータに対して実行され、その計算出力は前回生成された出力と比較されます。計算出力が既知解と等しくない場合は、既知解テストに失敗したことになります。

電源投入時セルフテストでは次を含むテストが行われます。

- ソフトウェアの整合性
- アルゴリズム テスト

何かに対応してセキュリティ機能または操作が始動された場合は、条件付きセルフテストが実行されなければなりません。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

デバイスは、既知解テスト (KAT) という暗号化アルゴリズムを使用して、デバイス上に実装されている FIPS 140-2 で承認された暗号機能 (暗号化、復号化、認証、および乱数生成) ごとに FIPS モードをテストします。デバイスは、このアルゴリズムを、すでに正しい出力がわかっているデータに対して適用します。次に、計算された出力を、以前に生成された出力と比較します。計算された出力が既知解に等しくない場合は、KAT が失敗します。

適用可能なセキュリティ機能または操作が呼び出された場合は、条件付きセルフテストが自動的に実行されます。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

- ペア整合性テスト：このテストは公開キー/秘密キーペアが生成されたときに実行されます。
- 乱数連続生成テスト：このテストは乱数が生成されたときに実行されます。
- Bypass
- ソフトウェア ロード

## CC について

Common Criteria (CC) は、開発者が要求するセキュリティ機能を製品が備えているかを確認するテスト基準です。CC 評価は、作成された保護プロファイル (PP) またはセキュリティ ターゲット (ST) に対するものです。

FIPS 140-2 の 4 つのセキュリティ レベルは、特定の CC EAL または CC 機能要件に直接マッピングされません。CC の詳細については、[Common Critical Portal](#) および [CC 評価と検証方法](#) を参照してください。

コントローラを CC 動作モードに設定するには、[Common Critical Portal Web](#) サイトの「認証済み製品」ページで公開されている『*Admin Guidance Document*』を参照してください。

コントローラ用の CC を提供すると、コントローラのシリーズ名が [Common Critical Portal](#) に表示されます。コントローラに使用可能なドキュメントのリストを表示するには、[Security Documents] タブをクリックします。

## UCAPL について

米国国防総省 (DoD) 統合機能認定製品リスト (APL) の認定プロセスは、国防情報システム局 (DISA) Unified Capabilities Certification Office (UCCO) の管轄です。認定は、相互運用性テストコマンド (JITC) を含む承認された分散テストセンターで行われます。

DoD のお客様は、認定済みの統合機能関連設備 (ハードウェアとソフトウェアの両方) しか購入できません。認定済みの設備は DoD UC APL に掲載されます。UC APL 認定は、システムが DISA Field Security Office (FSO) Security Technical Implementation Guides (STIG) に準拠し、それに基づいて設定されていることを確認します。

UC APL プロセスの詳細については、[国防情報システム局](#)のページを参照してください。

## FIPS の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、コントローラで FIPS を設定します。

```
config switchconfig fips-prerequisite{enable | disable}
```

**ステップ 2** 次のコマンドを入力して、FIPS の設定を表示します。

```
show switchconfig
```

以下に類似した情報が表示されます。

```
802.3x Flow Control Mode..... Disable
FIPS prerequisite features..... Enabled
WLANCC prerequisite features..... Enabled
UCAPL prerequisite features..... Disabled
secret obfuscation..... Enabled
```

## CC の設定 (CLI)

はじめる前に

FIPS をコントローラで有効にする必要があります。

**ステップ 1** 次のコマンドを入力して、コントローラで FIPS を設定します。  
**config switchconfig wlancc {enable | disable}**

**ステップ 2** 次のコマンドを入力して、FIPS の設定を表示します。  
**show switchconfig**

以下に類似した情報が表示されます。

```
802.3x Flow Control Mode..... Disable
FIPS prerequisite features..... Enabled
WLANCC prerequisite features..... Enabled
UCAPL prerequisite features..... Disabled
secret obfuscation..... Enabled
```

## UCAPL の設定 (CLI)

はじめる前に

FIPS および WLAN CC をコントローラ上で有効にする必要があります。

**ステップ 1** コントローラで UCAPL を設定するには、次のコマンドを入力します。  
**config switchconfig ucapl {enable | disable}**

**ステップ 2** 次のコマンドを入力して、FIPS の設定を表示します。  
**show switchconfig**

以下に類似した情報が表示されます。

```
802.3x Flow Control Mode..... Disable
FIPS prerequisite features..... Enabled
WLANCC prerequisite features..... Enabled
UCAPL prerequisite features..... Enabled
secret obfuscation..... Enabled
```



## 最大ローカルデータベースエントリの設定

- [最大ローカルデータベースエントリの設定について](#), 471 ページ
- [最大ローカルデータベースエントリの設定 \(GUI\)](#), 471 ページ
- [最大ローカルデータベースエントリの設定 \(CLI\)](#), 472 ページ

### 最大ローカルデータベースエントリの設定について

コントローラを設定して、ユーザ認証情報を格納するために使用するローカルデータベースエントリの最大数を指定できます。データベースエントリには、ローカル管理ユーザ（ロビーアンバサダーを含む）、ローカルネットワークユーザ（ゲストユーザを含む）、MACフィルタエントリ、除外リストエントリ、およびアクセスポイント許可リストエントリが含まれます。これらを合わせて、設定されている最大値を超えることはできません。

### 最大ローカルデータベースエントリの設定 (GUI)

- ステップ 1** [Security] > [AAA] > [General] の順に選択して、[General] ページを開きます。
- ステップ 2** [Maximum Local Database Entries] テキストボックスに、次回コントローラがリブートしたときにローカルデータベースに追加できる最大エントリ数を入力します。現在設定されている値が、テキストボックスの右側のカッコ内に表示されます。有効な範囲は 512 ~ 2048 で、デフォルトの設定は 2048 です。  
[Number of Entries, Already Used] テキストボックスに、データベースに現存するエントリ数が表示されます。
- ステップ 3** [Apply] をクリックして、変更を確定します。
- ステップ 4** [Save Configuration] をクリックして設定を保存します。

## 最大ローカル データベース エントリの設定 (CLI)

---

**ステップ 1** 次のコマンドを入力して、次回コントローラがリブートしたときにローカルデータベースに追加できる最大エントリ数を指定します。

**config database size *max\_entries***

**ステップ 2** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 3** 次のコマンドを入力して、データベース エントリの最大数およびデータベースの現在の内容を表示します。

**show database summary**

---



# 第 47 章

## コントローラでのローカル ネットワーク ユーザの設定

- [コントローラ上のローカル ネットワーク ユーザについて](#), 473 ページ
- [コントローラに対するローカル ネットワーク ユーザの設定 \(GUI\)](#), 473 ページ
- [コントローラに対するローカル ネットワーク ユーザの設定 \(CLI\)](#), 475 ページ

### コントローラ上のローカル ネットワーク ユーザについて

コントローラ上のローカル ユーザ データベースに、ローカル ネットワーク ユーザを追加することができます。ローカル ユーザ データベースには、すべてのローカル ネットワーク ユーザの資格情報 (ユーザ名とパスワード) が保存されます。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカル EAP では、ユーザの資格情報を取得するのに、バックエンド データベースとしてローカル ユーザ データベースを使用する場合があります。



(注) コントローラはクライアント情報をまず RADIUS 認証サーバに渡します。クライアント情報が RADIUS データベースのエントリに一致しない場合、RADIUS 認証サーバは認証失敗メッセージで応答します。RADIUS 認証サーバが応答しない場合は、ローカル ユーザ データベースにクエリーが送信されます。RADIUS 認証が失敗した場合、または存在しない場合は、このデータベースで見つかったクライアントがネットワーク サービスへのアクセスを付与されます。

### コントローラに対するローカル ネットワーク ユーザの設定 (GUI)

ステップ 1 [Security] > [AAA] > [Local Net Users] の順に選択して、[Local Net Users] ページを開きます。

(注) 既存のユーザを削除するには、そのユーザの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

**ステップ 2** 次のいずれかの操作を行います。

- 既存のローカル ネットワーク ユーザを編集するには、そのユーザのユーザ名をクリックします。 [Local Net Users > Edit] ページが表示されます。
- ローカル ネットワーク ユーザを追加するには、[New] をクリックします。 [Local Net Users > New] ページが表示されます。

**ステップ 3** 新しいユーザを追加している場合は、[User Name] テキスト ボックスにローカルユーザのユーザ名を入力します。最大 24 文字の英数字を入力できます。

(注) ローカルネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

**ステップ 4** [Password] および [Confirm Password] テキスト ボックスに、ローカルユーザのパスワードを入力します。最大 24 文字の英数字を入力できます。

**ステップ 5** 新しいユーザを追加している場合、そのユーザがローカルネットワークにアクセスできる時間を制限するには、[Guest User] チェックボックスをオンにします。デフォルト設定は選択されていません。

**ステップ 6** 新しいユーザを追加していて、[Guest User] チェックボックスをオンにした場合は、[Lifetime] テキストボックスに、ゲストユーザアカウントをアクティブにしておく時間 (秒単位) を入力します。有効な範囲は 60 ~ 2,592,000 (30 日間) 秒 (両端の値を含む) で、デフォルトの設定は 86,400 秒です。

**ステップ 7** 新しいユーザを追加していて、[Guest User] チェックボックスをオンにした場合、そのゲストユーザに QoS ロールを割り当てるには、[Guest User Role] チェックボックスをオンにします。デフォルト設定は選択されていません。

(注) ゲストユーザに QoS ロールを割り当てない場合、このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

**ステップ 8** 新しいユーザを追加していて、[Guest User Role] チェックボックスをオンにした場合は、そのゲストユーザに割り当てる QoS ロールを [Role] ドロップダウン リストから選択します。

**ステップ 9** [WLAN Profile] ドロップダウン リストから、ローカルユーザによってアクセスされる WLAN の名前を選択します。デフォルトの設定である [Any WLAN] を選択すると、ユーザは設定済みのどの WLAN にもアクセスできるようになります。

(注) ネットワークユーザに関連付けられている WLAN を削除しようとする、システムが、WLAN 自体を削除する前に WLAN に関連付けられたすべてのネットワークユーザを削除するように指示するプロンプトを表示します。

**ステップ 10** [Description] テキスト ボックスに、ローカルユーザを説明するタイトル (「ユーザ 1」など) を入力します。

**ステップ 11** [Apply] をクリックして、変更を確定します。

**ステップ 12** [Save Configuration] をクリックして、変更を保存します。



## コントローラに対するローカル ネットワーク ユーザの設定 (CLI)

- 次のコマンドを入力して、ローカル ネットワーク ユーザを設定します。
  - **config netuser add username password wlan wlan\_id userType permanent description**  
*description* : コントローラ上のローカル ユーザ データベースに永久ユーザを追加します。
  - **config netuser add username password {wlan | guestlan} {wlan\_id | guest\_lan\_id} userType guestlifetime seconds description**  
*description* : WLAN または有線ゲスト LAN 上のゲストユーザを、コントローラのローカル ユーザ データベースに追加します。



(注) 永久ユーザまたはゲスト ユーザをコントローラからローカル ユーザ データベースに追加する代わりに、RADIUS サーバ上にユーザに対するエントリを作成して Web 認証が実行される WLAN に対して RADIUS 認証を有効にするよう選択できます。

- **config netuser delete {username username | wlan-id wlan-id}**

◦ *username* : コントローラ上のローカル ユーザ データベースからユーザを削除します。



(注) ローカル ネットワーク ユーザ名は、すべて同じデータベース内に保存されるため、一意である必要があります。

◦ *wlan-id* : WLAN ID に関連付けられたネットワーク ユーザをすべて削除します。



(注) ネットワーク ユーザに関連付けられている WLAN を削除すると、システムは、先に WLAN に関連付けられているすべてのネットワーク ユーザを削除するように指示するプロンプトを表示します。ネットワーク ユーザを削除した後に、WLAN を削除できます。

- 次のコマンドを入力して、コントローラに設定されたローカル ネットワーク ユーザに関する情報を表示します。
  - **show netuser detail username** : ローカル ユーザ データベース内の特定のユーザの設定を表示します。
  - **show netuser summary** : ローカル ユーザ データベース内のすべてのユーザの一覧を表示します。
- 次のコマンドを入力して、変更を保存します。  
**save config**





# 第 48 章

## パスワードポリシーの設定

---

- [パスワードポリシーについて](#), 477 ページ
- [パスワードポリシーの設定 \(GUI\)](#), 478 ページ
- [パスワードポリシーの設定 \(CLI\)](#), 478 ページ

### パスワードポリシーについて

パスワードポリシーを使用すると、コントローラおよびアクセスポイントの追加管理ユーザ用に新しく作成されたパスワードに対し、強力なパスワードチェックを適用できます。新規パスワードには次の要件が適用されます。

- コントローラが旧バージョンからアップグレードされた場合、古いパスワードはすべて現状のまま維持されます。ただし、パスワードの強度は低下します。システムのアップグレード後、強力なパスワードチェックが有効になると、それ以降は強力なパスワードチェックが適用され、以前に追加されたパスワードの強度のチェックまたは変更は行われません。
- [Password Policy] ページで設定された内容によっては、ローカル管理ユーザおよびアクセスポイントユーザの設定が影響を受けます。

## パスワードポリシーの設定 (GUI)

- 
- ステップ1** [Security] > [AAA] > [Password Policies] の順に選択して、[Password Policies] ページを開きます。
- ステップ2** 小文字、大文字、数字、特殊文字の中から少なくとも3種類の文字をパスワードに含める場合は、[Password must contain characters from at least 3 different classes] チェックボックスをオンにします。
- ステップ3** 新規パスワード内で同じ文字が4回以上連続して繰り返されないようにするには、[No character can be repeated more than 3 times consecutively] チェックボックスをオンにします。
- ステップ4** パスワードに Cisco、ocsic、admin、nimda や、大文字と小文字を変更したり、1、|、または!を代用したり、oの代わりに0や、sの代わりに\$を使用したりするだけの変形文字列をパスワードに含めないようにするには、[Password cannot be the default words like cisco, admin] チェックボックスをオンにします。
- ステップ5** パスワードにユーザ名またはユーザ名を逆にした文字を含めないようにするには、[Password cannot contain username or reverse of username] チェックボックスをオンにします。
- ステップ6** [Apply] をクリックして、変更を確定します。
- ステップ7** [Save Configuration] をクリックして、変更を保存します。
- 

## パスワードポリシーの設定 (CLI)

- 次のコマンドを入力して、AP および WLC に対して強力なパスワードチェックを有効または無効にします。  
**config switchconfig strong-pwd {case-check | consecutive-check | default-check | username-check | all-checks| position-check | case-digit-check} {enable | disable}**  
 値は次のとおりです。
  - **case-check** : 同じ文字が3回連続して使用されているかを確認します。
  - **consecutive-check** : デフォルト値またはそのバリエーションが使用されているかを確認します。
  - **default-check** : ユーザ名またはそれを逆にした文字が使用されているかを確認します。
  - **all-checks** : 強力なパスワードチェックをすべて有効または無効にします。
  - **position-check** : 古いパスワードからの4文字の流用を確認します。
  - **case-digit-check** : 小文字、大文字、数字、特殊文字の4つすべての組み合わせが含まれているかを確認します。
- 次のコマンドを入力して、パスワード内の小文字、大文字、数字、特殊文字の最小数を設定します。  
**config switchconfig strong-pwd minimum {upper-case | lower-case | digits | special-chars} num-of-chars**

- 次のコマンドを入力して、パスワードの最小長を設定します。  
**config switchconfig strong-pwd min-length** *pwd-length*
- 次のコマンドを入力して、管理または SNMPv3 ユーザのロックアウトを設定します。  
**config switchconfig strong-pwd lockout** {*mgmtuser* | *snmpv3user*} {*enable* | *disable*}
- 次のコマンドを入力して、管理または SNMPv3 ユーザのロックアウト時間を設定します。  
**config switchconfig strong-pwd lockout time** {*mgmtuser* | *snmpv3user*} *timeout-in-mins*
- 次のコマンドを入力して、管理または SNMPv3 ユーザの試行連続失敗回数を設定します。  
**config switchconfig strong-pwd lockout attempts** {*mgmtuser* | *snmpv3user*} *num-of-failure-attempts*
- 次のコマンドを入力して、管理または SNMPv3 ユーザのライフタイムを設定します。  
**config switchconfig strong-pwd lifetime** {*mgmtuser* | *snmpv3user*} *lifetime-in-days*
- 次のコマンドを入力して、強力なパスワードチェックに設定されたオプションを表示します。

**show switchconfig**

以下に類似した情報が表示されます。

```
802.3x Flow Control Mode..... Disabled
FIPS prerequisite features..... Disabled
secret obfuscation..... Enabled
Strong Password Check Features:

 case-checkEnabled
 consecutive-checkEnabled
 default-checkEnabled
 username-checkEnabled
```





# 第 49 章

## LDAP の設定

---

- [LDAP について](#), 481 ページ
- [LDAP の設定 \(GUI\)](#), 482 ページ
- [LDAP の設定 \(CLI\)](#), 484 ページ

### LDAP について

LDAPバックエンドデータベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）をLDAPサーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。たとえば、ローカルEAPでは、ユーザの資格情報を取得するのに、バックエンドデータベースとしてLDAPを使用する場合があります。

#### LDAP Servers のフォールバック

LDAPサーバは認証用にWLANに設定されます。フォールバック動作が行われるようにするには、少なくとも2台のLDAPサーバでそれらを設定する必要があります。WLANごとにフォールバック動作が行われるように、最大3台のLDAPサーバを設定できます。サーバは認証の優先順位で表示されます。最初のLDAPサーバが応答しない場合、コントローラは次のLDAPサーバに切替えます。2番目のLDAPサーバが応答しない場合、コントローラは、3番目のLDAPサーバに再度切替えます。



---

(注) LDAPバックエンドデータベースでは、ローカルEAP方式として、EAP-TLS、EAP-FAST/GTC、およびPEAPv1/GTCがサポートされます。LEAP、EAP-FAST/MSCHAPv2、およびPEAPv0/MSCHAPv2もサポートされていますが、平文のパスワードを返すようにLDAPサーバが設定されている場合にのみサポートされます。

---



- (注) Cisco ワイヤレス LAN コントローラは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカル EAP 認証をサポートしています。Novell の eDirectory に対するローカル EAP 認証をコントローラに設定する方法については、[http://www.cisco.com/en/US/products/ps6366/products\\_white\\_paper09186a0080b4cd24.shtml](http://www.cisco.com/en/US/products/ps6366/products_white_paper09186a0080b4cd24.shtml) で『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。

## LDAP の設定 (GUI)

**ステップ 1** [Security] > [AAA] > [LDAP] の順に選択して、[LDAP Servers] ページを開きます。

- 既存の LDAP サーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

**ステップ 2** 次のいずれかの操作を行います。

- 既存の LDAP サーバを編集するには、そのサーバのインデックス番号をクリックします。[LDAP Servers > Edit] ページが表示されます。
- LDAP サーバを追加するには、[New] をクリックします。[LDAP Servers > New] ページが表示されます。新しいサーバを追加している場合は、[Server Index (Priority)] ドロップダウン リストから数字を選択し、その他の設定済み LDAP サーバに対してこのサーバの優先順位を指定します。最大 17 台のサーバを設定できます。コントローラが最初のサーバに接続できない場合、リスト内の 2 番目のサーバへの接続を試行する、というようになります。

**ステップ 3** 新しいサーバを追加している場合は、[Server IP Address] テキスト ボックスに LDAP サーバの IP アドレスを入力します。

**ステップ 4** 新しいサーバを追加している場合は、[Port Number] テキスト ボックスに LDAP サーバの TCP ポート番号を入力します。有効な範囲は 1 ~ 65535 で、デフォルト値は 389 です。

**ステップ 5** [Server Mode (via TLS)] ドロップダウン リストから [Disabled] を選択し、TCP を使用して LDAP サーバと Cisco WLC 間の LDAP 接続 (セキュア トンネルなし) を確立します。または [Enabled] を選択し、TLS を使用してセキュア LDAP 接続を確立します。

**ステップ 6** [Enable Server Status] チェックボックスをオンにしてこの LDAP サーバを有効にするか、オフにして無効にします。デフォルト値はディセーブルです。

**ステップ 7** [Simple Bind] ドロップダウン リストから [Anonymous] または [Authenticated] を選択して、LDAP サーバ用のローカル認証バインド方式を指定します。[Anonymous] 方式では、LDAP サーバへの匿名アクセスが可能



能です。[Authenticated] 方式では、ユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルト値は [Anonymous] です。

**ステップ 8** 前の手順で [Authenticated] を選択した場合は、次の手順に従ってください。

a) [Bind Username] テキストボックスに、LDAP サーバのローカル認証に使用されるユーザ名を入力します。ユーザ名には、最大 80 文字を使用できます。

(注) ユーザ名が「cn=」(小文字)で始まる場合、コントローラはユーザ名に完全な LDAP データベースパスが含まれていると見なし、ユーザベース DN を付加しません。この指定により、認証済みのバインドユーザをユーザベース DN の外に置くことができます。

b) [Bind Username] テキストボックスに、LDAP サーバのローカル認証に使用されるユーザ名を入力します。ユーザ名には、最大 80 文字を使用できます。

**ステップ 9** [User Base DN] テキストボックスに、全ユーザのリストが含まれた、LDAP サーバ内のサブツリーの識別名 (DN) を入力します。たとえば、ou=organizational unit、.ou=next organizational unit、o=corporation.com のようになります。ユーザを含むツリーがベース DN である場合は、次を入力します。

`o=corporation.com`

または

`dc=corporation,dc=com`

**ステップ 10** [User Attribute] テキストボックスに、ユーザ名が含まれたユーザレコード内の属性の名前を入力します。この属性はディレクトリサーバから取得できます。

**ステップ 11** [User Object Type] テキストボックスに、レコードをユーザとして識別する LDAP objectType 属性の値を入力します。多くの場合、ユーザレコードには複数の objectType 属性の値が含まれています。そのユーザに一意の値と、他のオブジェクトタイプと共有する値があります。

**ステップ 12** [Server Timeout] テキストボックスに、再送信の間隔を秒単位で入力します。有効な範囲は 2 ~ 30 秒で、デフォルト値は 2 秒です。

**ステップ 13** [Apply] をクリックして、変更を確定します。

**ステップ 14** [Save Configuration] をクリックして、変更を保存します。

**ステップ 15** 次の手順を実行して、LDAP をローカル EAP 認証用の優先バックエンドデータベースサーバとして指定します。

a) [Security] > [Local EAP] > [Authentication Priority] の順に選択して、[Priority Order > Local-Auth] ページを開きます。

b) [LOCAL] を強調表示して、[<] をクリックし、それを左の [User Credentials] ボックスに移動します。

c) [LDAP] を強調表示して、[>] をクリックし、それを右の [User Credentials] ボックスに移動します。右側の [User Credentials] ボックスの上部に表示されるデータベースは、ユーザの資格情報を取得する際に使用されます。

(注) [LDAP] と [LOCAL] の両方が右側の [User Credentials] ボックスに表示され、[LDAP] が上部で [LOCAL] が下部にある場合、ローカル EAP は LDAP バックエンドデータベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカルユーザデータベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が上部にある場合、ローカル EAP はローカルユーザデータベースのみを使用して認証を試行します。LDAP バックエンドデータベースへのフェールオーバーは行われません。

- d) [Apply] をクリックして、変更を確定します。
- e) [Save Configuration] をクリックして、変更を保存します。

**ステップ 16** (任意) 次の手順を実行して、特定の LDAP サーバを WLAN に割り当てます。

- a) [WLANs] を選択して、[WLANs] ページを開きます。
- b) 必要な WLAN の ID 番号をクリックします。
- c) [WLANs>Edit] ページが表示されたら [Security]>[AAA Servers] タブを選択し、[WLANs>Edit] ([Security>AAA Servers]) ページを開きます。
- d) [LDAP Servers] ドロップダウンリストから、この WLAN で使用する LDAP サーバを選択します。最大 3 台の LDAP サーバを選択できます。これらのサーバは優先順位に従って試行されます。  
(注) これらの LDAP サーバは、Web 認証が有効になっている WLAN にのみ適用されます。ローカル EAP によって使用されません。
- e) [Apply] をクリックして、変更を確定します。
- f) [Save Configuration] をクリックして、変更を保存します。

**ステップ 17** 次の手順を実行して、LDAP サーバフォールバックの動作を指定します。

- a) [WLAN]>[AAA Server] を選択して、[Fallback Parameters] ページを開きます。
- b) [LDAP Servers] ドロップダウン リストから、コントローラが管理ユーザを認証しようとする際の優先順位に従って、LDAP サーバを選択します。認証順序はサーバから開始します。
- c) [Security]>[AAA]>[LDAP] の順に選択して、コントローラに設定されたグローバル LDAP サーバのリストを表示します。

## LDAP の設定 (CLI)

- 次のコマンドを入力して、LDAP サーバを設定します。

- **config ldap add index server\_ip\_address port# user\_base user\_attr user\_type secure** : セキュア LDAP 用の LDAP サーバを追加します。
- **config ldap delete index** : 以前に追加された LDAP サーバを削除します。
- **config ldap {enable | disable} index** : LDAP サーバを有効または無効にします。
- **config ldap security-mode enable index** : 既存のコマンドと共にインデックスを使用して LDAP をイネーブルにします。
- **config ldap simple-bind {anonymous index | authenticated index username username password password}** : LDAP サーバ用のローカル認証バインド方式を指定します。匿名方式では LDAP サーバへの匿名アクセスが可能です。一方、許可方式ではユーザ名とパスワードを入力してアクセスをセキュリティで保護する必要があります。デフォルト値は [anonymous] です。ユーザ名には、最大 80 文字を使用できます。  
ユーザ名が「cn=」 (小文字) で始まる場合、コントローラはユーザ名に完全な LDAP データベースパスが含まれていると見なし、ユーザベース DN を付加しません。この

指定により、認証済みのバインドユーザをユーザベース DN の外に置くことができます。

- **config ldap retransmit-timeout index timeout** : LDAP サーバの再送信の間隔 (秒数) を設定します。

- 次のコマンドを入力して、LDAP を優先バックエンドデータベースサーバとして指定します。

#### **config local-auth user-credentials ldap**

**config local-auth user-credentials ldap local** コマンドを入力すると、ローカル EAP は LDAP バックエンドデータベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカルユーザデータベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。 **config local-auth user-credentials local ldap** コマンドを入力すると、ローカル EAP はローカルユーザデータベースのみを使用して認証を試行します。LDAP バックエンドデータベースへのフェールオーバーは行われません。

- (任意) 次のコマンドを入力して、特定の LDAP サーバを WLAN に割り当てます。
  - **config wlan ldap add wlan\_id server\_index** : 設定済みの LDAP サーバを WLAN に接続します。  
このコマンドで指定される LDAP サーバは、Web 認証が有効になっている WLAN にのみ適用されます。ローカル EAP によって使用されません。
  - **config wlan ldap delete wlan\_id {all|index}** : 特定の、またはすべての設定済み LDAP サーバを WLAN から削除します。

- 次のコマンドを入力して、設定済みの LDAP サーバに関連する情報を表示します。

- **show ldap summary** : 設定済みの LDAP サーバの概要を表示します。

| Idx | Server Address | Port | Enabled |
|-----|----------------|------|---------|
| 1   | 2.3.1.4        | 389  | No      |
| 2   | 10.10.20.22    | 389  | Yes     |

| Idx | Server Address | Port | Enabled | Secure |
|-----|----------------|------|---------|--------|
| 1   | 2.3.1.4        | 389  | No      | No     |
| 2   | 2.3.1.5        | 389  | Yes     | No     |

- **show ldap index** : 詳細な LDAP サーバ情報を表示します。次のような情報が表示されます。

```

Server Index..... 2
Address..... 10.10.20.22
Port..... 389
Enabled..... Yes
User DN..... ou=active,ou=employees,ou=people,
 o=cisco.com
User Attribute..... uid
User Type..... Person
Retransmit Timeout..... 2 seconds

```

```

Bind Method Authenticated
Bind Username..... user1
Controller# show ldap 1
Server Index..... 1
Address..... 9.1.0.100
Port..... 389
Server State..... Disabled
User DN..... user1
User Attribute..... user
User Type..... user
Retransmit Timeout..... 2 seconds
Secure (via TLS)..... Disabled
Bind Method Anonymous

```

◦ **show ldap statistics** : LDAP サーバの統計情報を表示します。

```

Server Index..... 1
Server statistics:
 Initialized OK..... 0
 Initialization failed..... 0
 Initialization retries..... 0
 Closed OK..... 0
Request statistics:
 Received..... 0
 Sent..... 0
 OK..... 0
 Success..... 0
 Authentication failed..... 0
 Server not found..... 0
 No received attributes..... 0
 No passed username..... 0
 Not connected to server..... 0
 Internal error..... 0
 Retries..... 0

Server Index..... 2
..

```

◦ **show wlan wlan\_id** : WLAN に適用される LDAP サーバを表示します。

- 次のコマンドを入力して、コントローラが LDAP サーバに到達できることを確認します。  
**ping server\_ip\_address**
- 次のコマンドを入力して、変更を保存します。  
**save config**
- 次のコマンドを入力して、LDAP のデバッグを有効または無効にします。  
**debug aaa ldap {enable | disable}**



# 第 50 章

## ローカル EAP の設定

---

- [ローカル EAP について](#), 487 ページ
- [ローカル EAP の制約事項](#), 489 ページ
- [ローカル EAP の設定 \(GUI\)](#), 490 ページ
- [ローカル EAP の設定 \(CLI\)](#), 495 ページ

### ローカル EAP について

ローカル EAP は、ユーザおよびワイヤレスクライアントのローカル認証を可能にする認証方式です。この方式は、バックエンドシステムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレスクライアントへの接続を維持できるように、リモートオフィスで使用する目的で設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカルユーザデータベースとして機能するため、外部認証サーバに依存する必要がなくなります。ローカル EAP は、ローカルユーザデータベースまたは LDAP バックエンドデータベースからユーザの資格情報を取得して、ユーザを認証します。ローカル EAP では、コントローラとワイヤレスクライアント間で、LEAP、EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC 認証方式をサポートします。



(注) LDAP バックエンドデータベースでは、ローカル EAP 方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すように LDAP サーバが設定されている場合にのみサポートされます。

---



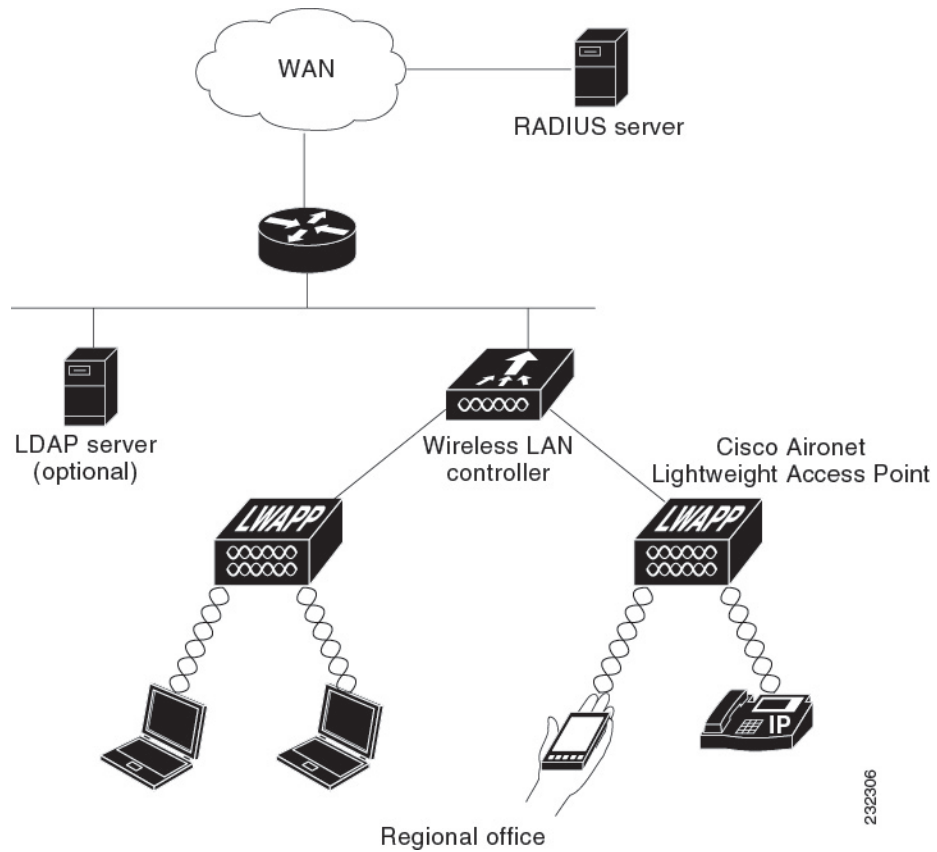
(注) Cisco ワイヤレス LAN コントローラは、Microsoft Active Directory や Novell の eDirectory などの外部 LDAP データベースに対するローカル EAP 認証をサポートしています。Novell の eDirectory に対するローカル EAP 認証をコントローラに設定する方法については、[http://www.cisco.com/en/US/products/ps6366/products\\_white\\_paper09186a0080b4cd24.shtml](http://www.cisco.com/en/US/products/ps6366/products_white_paper09186a0080b4cd24.shtml) で『Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database』ホワイトペーパーを参照してください。

コントローラ上で RADIUS サーバが設定されている場合は、コントローラはまず RADIUS サーバを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバがタイムアウトしていたり、RADIUS サーバが設定されていない場合など、RADIUS サーバが見つからない場合にのみ試行されます。4 台の RADIUS サーバが設定されている場合、コントローラは最初の RADIUS サーバを使用してクライアントの認証を試行し、次に 2 番目の RADIUS サーバ、その次にローカル EAP を試行します。その後クライアントが手動で再認証を試みると、コントローラは 3 番目の RADIUS サーバを試行し、次に 4 番目の RADIUS サーバ、その次にローカル EAP を試行します。コントローラで外部 RADIUS サーバを使用したクライアント認証を行いたくない場合は、次の CLI コマンドを示された順序どおりに入力します。

- **config wlan disable *wlan\_id***
- **config wlan radius\_server auth disable *wlan\_id***

- `config wlan enable wlan_id`

図 44 : ローカル EAP の例



## ローカル EAP の制約事項

ローカル EAP プロファイルは、Cisco 600 シリーズ OfficeExtend アクセス ポイントではサポートされません。

## ローカル EAP の設定 (GUI)

はじめる前に



- (注) EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は、認証に証明書を使用し、EAP-FAST は、証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority (CA; 認証局) の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。

- ステップ 1** 上記に示したいずれかの EAP タイプを使用するようにローカル EAP を設定する場合は、適切な証明書と PAC (手動の PAC プロビジョニングを使用する場合) がコントローラにインポートされていることを確認してください。
- ステップ 2** コントローラでローカル ユーザ データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。
- ステップ 3** コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。
- ステップ 4** 次の手順を実行して、ユーザの資格情報をバックエンド データベース サーバから取得する順序を指定します。
- [Security] > [Local EAP] > [Authentication Priority] の順に選択して、[Priority Order > Local-Auth] ページを開きます。
  - ユーザの資格情報がローカルまたは LDAP データベースから取得される優先順位を決定します。たとえば、LDAP データベースがローカル ユーザ データベースよりも優先されるようにすることも、または LDAP データベースがまったく考慮されないようにすることもできます。
  - 優先順位を決定したら、目的のデータベースを強調表示します。次に、左と右の矢印および [Up] ボタンと [Down] ボタンを使用して、目的のデータベースを右側の [User Credentials] ボックスの上部に移動します。
 

(注) [LDAP] と [LOCAL] の両方が右側の [User Credentials] ボックスに表示され、[LDAP] が上部で [LOCAL] が下部にある場合、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。[LOCAL] が上部にある場合、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。
  - [Apply] をクリックして、変更を確定します。
- ステップ 5** 次の手順を実行して、ローカル EAP タイマーの値を指定します。
- [Security] > [Local EAP] > [General] の順に選択して、[General] ページを開きます。



- b) [Local Auth Active Timeout] テキスト ボックスに、コントローラが設定済み RADIUS サーバのペアによる認証に失敗した後、ローカル EAP を使用してワイヤレス クライアントを認証する際の試行時間 (秒単位) を入力します。有効な範囲は 1 ~ 3600 秒で、デフォルトの設定は 100 秒です。

**ステップ 6** 次のように Advanced EAP パラメータの値を指定します。

- a) [Security] > [Advanced EAP] を選択します。
- b) [Identity Request Timeout] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求を送信する際の試行時間 (秒単位) を入力します。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
- c) [Identity Request Max Retries] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ~ 20 回で、デフォルトの設定は 20 回です。
- d) [Dynamic WEP Key Index] テキスト ボックスに、Dynamic Wired Equivalent Privacy (WEP) に使用するキーインデックスを入力します。デフォルト値は 0 で、これはキーインデックス 1 に相当します。有効な値は 0 ~ 3 (キーインデックス 1 ~ 4) です。
- e) [Request Timeout] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求を送信する際の試行時間 (秒単位) を入力します。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
- f) [Request Max Retries] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求を再送信する際の最大試行回数を入力します。有効な値の範囲は 1 ~ 120 回で、デフォルトの設定は 20 回です。
- g) [Max-Login Ignore Identity Response] ドロップダウン リストから [Enable] を選択して、同じユーザ名を使用してコントローラに接続できるデバイスの数を制限できます。同じコントローラ上の異なるデバイス (PDA、ノートパソコン、IP 電話など) から最大 8 台までログインできます。デフォルト値はイネーブルです。
- h) [EAPOL-Key Timeout] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーを送信する際の試行時間 (秒単位) を入力します。有効な値の範囲は 1 ~ 5 秒で、デフォルトの設定は 1 秒です。  
(注) コントローラとアクセス ポイントが WAN リンクによって分離されている場合、デフォルト タイムアウト値の 1 秒では不十分な場合があります。
- i) [EAPOL-Key Max Retries] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ~ 4 回で、デフォルトの設定は 2 回です。
- j) [Apply] をクリックして、変更を確定します。

**ステップ 7** 次の手順を実行して、ワイヤレス クライアントでサポートされる EAP 認証タイプを指定する、ローカル EAP プロファイルを作成します。

- a) [Security] > [Local EAP] > [Profiles] の順に選択して、[Local EAP Profiles] ページを開きます。  
このページでは、これまでに設定されたすべてのローカル EAP プロファイルが表示され、その EAP タイプを指定します。最大 16 個のローカル EAP プロファイルを作成できます。  
(注) 既存のプロファイルを削除するには、そのプロファイルの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

- b) [New] をクリックして、[Local EAP Profiles > New] ページを開きます。
- c) [Profile Name] テキストボックスに新しいプロファイルの名前を入力し、[Apply] をクリックします。
  - (注) プロファイル名には最大 63 文字の英数字を入力できます。スペースは含めないでください。
- d) [Local EAP Profiles] ページが再度表示されたら、新しいプロファイルの名前をクリックします。[Local EAP Profiles > Edit] ページが表示されます。
- e) [LEAP]、[EAP-FAST]、[EAP-TLS]、または [PEAP] チェックボックスをオンにし、ローカル認証に使用できる EAP タイプを指定します。
  - (注) プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ（証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、PEAPv1/GTC など）を選択する場合、すべての EAP タイプで同じ証明書（Cisco または他のベンダーが発行する）を使用する必要があります。
  - (注) [PEAP] チェックボックスをオンにすると、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。
- f) EAP-FAST を選択し、コントローラ上のデバイス証明書を認証に使用する場合は、[Local Certificate Required] チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにしておきます。これはデフォルトの設定です。
  - (注) デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このオプションは EAP-FAST にのみ適用されます。
- g) EAP-FAST を選択し、ワイヤレスクライアントが認証のためデバイス証明書をコントローラに送信するよう設定するには、[Client Certificate Required] チェックボックスをオンにします。証明書の代わりに PAC を使用する EAP-FAST を使用する場合は、このチェックボックスをオフのままにしておきます。これはデフォルトの設定です。
  - (注) クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このオプションは EAP-FAST にのみ適用されます。
- h) 証明書を使用する EAP-FAST、EAP-TLS、または PEAP を選択する場合は、クライアントに送信される証明書がシスコから発行されるものか、別のベンダーから発行されるものかを指定します。[Cisco] または [Vendor] を [Certificate Issuer] ドロップダウンリストから選択してください。デフォルトの設定は、[Cisco] になっています。
- i) 証明書を使用する EAP-FAST または EAP-TLS を選択し、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証する場合は、[Check Against CA Certificates] チェックボックスをオンにします。デフォルト設定はイネーブルです。
- j) 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信する証明書での Common Name (CN) をコントローラ上の CA 証明書の CN と照合して検証する場合は、[Verify Certificate CN Identity] チェックボックスをオンにします。デフォルト設定では無効になっています。
- k) 証明書を使用する EAP-FAST または EAP-TLS を選択し、受信するデバイス証明書が現在有効であり、期限切れでないことをコントローラで検証されるようにする場合は、[Check Certificate Date Validity] チェックボックスをオンにします。デフォルト設定はイネーブルです。
  - (注) 証明書の日付の有効性が、コントローラに設定された現在の UTC (GMT) 時間と照合されます。タイムゾーンのオフセットは無視されます。

- l) [Apply] をクリックして、変更を確定します。

**ステップ 8** EAP-FAST プロファイルを作成した場合、EAP-FAST パラメータを設定する手順は、次のとおりです。

- a) [Security] > [Local EAP] > [EAP-FAST Parameters] の順に選択して、[EAP-FAST Method Parameters] ページを開きます。
- b) [Server Key] テキスト ボックスおよび [Confirm Server Key] フィールドに、PAC の暗号化と暗号化解除に使用するキー (16 進数文字) を入力します。
- c) [Time to Live for the PAC] テキスト ボックスに、PAC の有効日数を入力します。有効な範囲は 1 ~ 1000 日で、デフォルトの設定は 10 日です。
- d) [Authority ID] テキスト ボックスに、ローカル EAP-FAST サーバの認証局 ID を 16 進数文字で入力します。最大 32 文字の 16 進数文字を入力できますが、文字数は偶数である必要があります。
- e) [Authority ID Information] テキスト ボックスに、ローカル EAP-FAST サーバの Authority ID をテキスト形式で入力します。
- f) 匿名プロビジョニングを有効にするには、[Anonymous Provision] チェックボックスをオンにします。この機能を使用すると、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。この機能を無効にする場合、PAC は手動でプロビジョニングされる必要があります。デフォルト設定はイネーブルです。  
(注) ローカル証明書またはクライアント証明書、あるいはその両方を必要とし、すべての EAP-FAST クライアントで証明書が使用されるよう強制する場合は、[Anonymous Provision] チェックボックスをオフにしてください。
- g) [Apply] をクリックして、変更を確定します。

**ステップ 9** 次の手順を実行して、WLAN 上でローカル EAP を有効にします。

- a) [WLANs] を選択して、[WLANs] ページを開きます。
- b) 必要な WLAN の ID 番号をクリックします。
- c) [WLANs > Edit] ページが表示されたら [Security] > [AAA Servers] タブを選択し、[WLANs > Edit] ([Security > AAA Servers]) ページを開きます。
- d) この WLAN に対して RADIUS アカウンティングおよび認証をディセーブルにするには、RADIUS 認証サーバおよびアカウンティングサーバの [Enabled] チェックボックスをオフにします。
- e) [Local EAP Authentication] チェックボックスをオンにして、この WLAN に対してローカル EAP を有効にします。
- f) [EAP Profile Name] ドロップダウン リストから、この WLAN に使用する EAP プロファイルを選択します。
- g) 必要に応じて、[LDAP Servers] ドロップダウン リストから、この WLAN でローカル EAP と共に使用する LDAP サーバを選択します。
- h) [Apply] をクリックして、変更を確定します。

**ステップ 10** 次の手順を実行して、WLAN で EAP パラメータを有効にします。

- a) [WLANs] を選択して、[WLANs] ページを開きます。
- b) 必要な WLAN の ID 番号をクリックします。
- c) [WLANs > Edit] ページが表示されたら [Security] > [AAA Servers] タブを選択し、[WLANs > Edit] ([Security > AAA Servers]) ページを開きます。
- d) この WLAN に対して EAP パラメータを設定するには、[Enable] チェックボックスをオンにします。

- e) [EAPOL Key Timeout (200 to 5000 millisc)] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーを送信する際の試行時間を入力します (ミリ秒単位)。有効な範囲は 200 ~ 5000 ミリ秒で、デフォルト値は 1000 ミリ秒です。
- f) [EAPOL Key Retries (0 to 4)] テキスト ボックスに、コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーを送信する際の最大試行回数を入力します。有効な範囲は 0 ~ 4 回で、デフォルトの設定は 2 回です。
- g) [Identity Request Timeout (1 to 120 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求を送信する際の試行時間を入力します (秒単位)。有効な範囲は 1 ~ 120 秒で、デフォルト値は 30 秒です。
- h) [Identity Request Retries (1 to 20 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求を再送信する際の最大試行回数を入力します。有効な範囲は 1 ~ 20 回で、デフォルトの設定は 2 回です。
- i) [Request Timeout (1 to 120 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求を送信する際の試行時間を入力します (秒単位)。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
- j) [Request Retries (1 to 20 sec)] テキスト ボックスに、コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求を再送信する際の最大試行回数を入力します。有効な範囲は 1 ~ 20 回で、デフォルトの設定は 2 回です。
- k) [Apply] をクリックして、変更を確定します。

**ステップ 11** [Save Configuration] をクリックして、変更を保存します。

---

## ローカル EAP の設定 (CLI)

はじめる前に



- (注) EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC は認証に証明書を使用し、EAP-FAST は証明書または PAC のいずれかを使用します。コントローラには、シスコによりインストールされたデバイスの証明書と、Certificate Authority (CA; 認証局) の証明書が付属しています。ただし、ご自身のベンダー固有の証明書を使用する場合は、それらの証明書をコントローラにインポートする必要があります。

- ステップ 1** 上記に示したいずれかの EAP タイプを使用するようにローカル EAP を設定する場合は、適切な証明書と PAC (手動の PAC プロビジョニングを使用する場合) がコントローラにインポートされていることを確認してください。
- ステップ 2** コントローラでローカル ユーザ データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上でローカル ネットワーク ユーザを適切に設定していることを確認してください。
- ステップ 3** コントローラで LDAP バックエンド データベースからユーザの資格情報を取得するようにする場合は、そのコントローラ上で LDAP サーバを適切に設定していることを確認してください。
- ステップ 4** 次のコマンドを入力して、ローカルまたは LDAP データベースからユーザの資格情報を取得する順位を指定します。

```
config local-auth user-credentials {local | ldap}
```

- (注) **config local-auth user-credentials ldap local** コマンドを入力すると、ローカル EAP は LDAP バックエンド データベースを使用してクライアントの認証を試行し、LDAP サーバが接続不能である場合は、ローカル ユーザ データベースにフェールオーバーします。ユーザが見つからない場合、認証の試行は拒否されます。**config local-auth user-credentials local ldap** コマンドを入力すると、ローカル EAP はローカル ユーザ データベースのみを使用して認証を試行します。LDAP バックエンド データベースへのフェールオーバーは行われません。

- ステップ 5** 次のコマンドを入力して、ローカル EAP タイマーの値を指定します。
- **config local-auth active-timeout timeout** : 設定済み RADIUS サーバのペアによる認証が失敗した後に、コントローラがローカル EAP を使用してワイヤレス クライアントを認証する際の試行時間 (秒単位) を指定します。有効な範囲は 1 ~ 3600 秒で、デフォルトの設定は 100 秒です。
  - **config advanced eap identity-request-timeout timeout** : コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求を送信する際の試行時間 (秒単位) を指定します。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
  - **config advanced eap identity-request-retries retries** : コントローラがローカル EAP を使用してワイヤレス クライアントに EAP ID 要求を再送信する際の最大試行回数を指定します。有効な値の範囲は 1 ~ 20 回で、デフォルトの設定は 20 回です。

- **config advanced eap key-index *index*** : Dynamic Wired Equivalent Privacy (WEP) に使用するキー インデックスを指定します。デフォルト値は 0 で、これはキー インデックス 1 に相当します。有効な値は 0 ~ 3 (キー インデックス 1 ~ 4) です。
- **config advanced eap request-timeout *timeout*** : コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求を送信する際の試行時間 (秒単位) を指定します。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
- **config advanced eap request-retries *retries*** : コントローラがローカル EAP を使用してワイヤレス クライアントに EAP 要求を再送信する際の最大試行回数を指定します。有効な値の範囲は 1 ~ 120 回で、デフォルトの設定は 20 回です。
- **config advanced eap eapol-key-timeout *timeout*** : コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーを送信する際の試行時間 (秒単位) を指定します。有効な値の範囲は 1 ~ 5 秒で、デフォルトの設定は 1 秒です。  
(注) コントローラとアクセス ポイントが WAN リンクによって分離されている場合、デフォルト タイムアウト値の 1 秒では不十分な場合があります。
- **config advanced eap eapol-key-retries *retries*** : コントローラがローカル EAP を使用してワイヤレス クライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ~ 4 回で、デフォルトの設定は 2 回です。
- **config advanced eap max-login-ignore-identity-response {enable | disable}** : このコマンドを有効にすると、同じユーザ名を使用してコントローラに接続できるデバイスの数を制限できます。同じコントローラ上の異なるデバイス (PDA、ノートパソコン、IP 電話など) から最大 8 台までログインできます。デフォルト値はイネーブルです。

ステップ 6 次のコマンドを入力して、WLAN でローカル EAP タイマーの値を指定します。

- **config wlan security eap-params {enable | disable} *wlan\_id*** : SSID 固有の EAP タイムアウトまたは再試行をイネーブルまたはディセーブルに指定します。デフォルト値は [disabled] です。
- **config wlan security eap-params eapol-key-timeout *timeout wlan\_id*** : コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーを送信する際の試行時間を指定します (ミリ秒単位)。有効な範囲は 200 ~ 5000 ミリ秒で、デフォルト設定は 1000 ミリ秒です。
- **config wlan security eap-params eapol-key-retries *retries wlan\_id*** : コントローラがローカル EAP を使用してワイヤレス クライアントに WLAN 経由で EAP キーを送信する際の最大試行回数を指定します。有効な値の範囲は 0 ~ 4 回で、デフォルトの設定は 2 回です。
- **config wlan security eap-params identity-request-timeout *timeout wlan\_id*** : コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求を送信する際の試行時間を指定します (秒単位)。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
- **config wlan security eap-params identity-request-retries *retries wlan\_id*** : コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP ID 要求を再送信する際の最大試行回数を指定します。有効な範囲は 1 ~ 20 回で、デフォルトの設定は 2 回です。

- **config wlan security eap-params request-timeout timeout wlan\_id** : コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求を送信する際の試行時間を指定します (秒単位)。有効な範囲は 1 ~ 120 秒で、デフォルトの設定は 30 秒です。
- **config wlan security eap-params request-retries retries wlan\_id** : コントローラがローカル EAP を使用して WLAN 内のワイヤレス クライアントに EAP パラメータ要求を再送信する際の最大試行回数を指定します。有効な範囲は 1 ~ 20 回で、デフォルトの設定は 2 回です。

**ステップ 7** 次のコマンドを入力して、ローカル EAP プロファイルを作成します。

**config local-auth eap-profile add profile\_name**

- (注) プロファイル名にスペースを含めないでください。
- (注) ローカル EAP プロファイルを削除するには、**config local-auth eap-profile delete profile\_name** コマンドを入力します。

**ステップ 8** 次のコマンドを入力して、ローカル EAP プロファイルに EAP 方式を追加します。

**config local-auth eap-profile method add method profile\_name**

サポートされている方式は leap、fast、tls、および peap です。

- (注) peap を選択する場合、コントローラ上で PEAPv0/MSCHAPv2 と PEAPv1/GTC の両方が有効になります。
- (注) プロファイルごとに複数の EAP タイプを指定できます。ただし、証明書を使用する複数の EAP タイプ (証明書を使用する EAP-FAST、EAP-TLS、PEAPv0/MSCHAPv2、および PEAPv1/GTC など) でプロファイルを作成する場合、すべての EAP タイプで同じ証明書 (Cisco または他のベンダーが発行する) を使用する必要があります。
- (注) ローカル EAP プロファイルから EAP 方式を削除するには、**config local-auth eap-profile method delete method profile\_name** コマンドを入力します。

**ステップ 9** EAP-FAST プロファイルを作成した場合は、次のコマンドを入力して EAP-FAST パラメータを設定します。

**config local-auth method fast ?**

ここで、? は、次のいずれかを示します。

- **anon-prov {enable|disable}** : コントローラで匿名プロビジョニングが許可されるように設定します。これにより、PAC プロビジョニング中に、PAC がないクライアントに PAC が自動的に送信されるようになります。
- **authority-id auth\_id** : ローカル EAP-FAST サーバの Authority ID を指定します。
- **pac-ttl days** : PAC の有効日数を指定します。
- **server-key key** : PAC を暗号化および暗号化解除するために使用されるサーバ キーを指定します。

**ステップ 10** 次のコマンドを入力して、プロファイルごとに証明書パラメータを設定します。

- **config local-auth eap-profile method fast local-cert {enable|disable} profile\_name** : 認証にコントローラ上のデバイス証明書が必要かどうかを指定します。

(注) デバイス証明書は LEAP と共に使用されず、EAP-TLS と PEAP には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile method fast client-cert {enable | disable} profile\_name** : 認証用のデバイス証明書をコントローラへ送信するために、ワイヤレスクライアントが必要かどうかを指定します。

(注) クライアント証明書は LEAP または PEAP と共に使用されず、EAP-TLS には必須であるため、このコマンドは EAP-FAST にのみ適用されます。

- **config local-auth eap-profile cert-issuer {cisco | vendor} profile\_name** : 証明書を使用する EAP-FAST、EAP-TLS、または PEAP を指定した場合は、クライアントに送信される証明書がシスコから発行されるものか、別のベンダーから発行されるものかを指定します。

- **config local-auth eap-profile cert-verify ca-issuer {enable | disable} profile\_name** : 証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、クライアントから受信する証明書をコントローラ上の CA 証明書と照合して検証するかどうかを指定します。

- **config local-auth eap-profile cert-verify cn-verify {enable | disable} profile\_name** : 証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、受信する証明書での Common Name (CN) をコントローラ上の CA 証明書の CN と照合して検証するかどうかを指定します。

- **config local-auth eap-profile cert-verify date-valid {enable | disable} profile\_name** : 証明書を使用する EAP-FAST または EAP-TLS を選択する場合は、受信するデバイスの証明書が現在も有効であり期限が切れていないことがコントローラで検証されるようにするかどうかを指定します。

**ステップ 11** 次のコマンドを入力して、ローカル EAP を有効にし、EAP プロファイルを WLAN に接続します。

```
config wlan local-auth enable profile_name wlan_id
```

(注) WLAN でローカル EAP を無効にするには、**config wlan local-auth disable wlan\_id** コマンドを入力します。

**ステップ 12** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 13** 次のコマンドを入力して、ローカル EAP に関連する情報を表示します。

- **show local-auth config** : コントローラ上のローカル EAP の設定を表示します。

```
User credentials database search order:
 Primary Local DB

Timer:
 Active timeout 300

Configured EAP profiles:
 Name fast-cert
 Certificate issuer vendor
 Peer verification options:
 Check against CA certificates Enabled
 Verify certificate CN identity Disabled
 Check certificate date validity Enabled
 EAP-FAST configuration:
 Local certificate required Yes
 Client certificate required Yes
 Enabled methods fast
 Configured on WLANs 1

Name tls
```



```

Certificate issuer vendor
Peer verification options:
 Check against CA certificates Enabled
 Verify certificate CN identity Disabled
 Check certificate date validity Enabled
EAP-FAST configuration:
 Local certificate required No
 Client certificate required No
Enabled methods tls
Configured on WLANs 2

EAP Method configuration:
EAP-FAST:
 Server key <hidden>
 TTL for the PAC 10
 Anonymous provision allowed Yes
 Accept client on auth prov No
 Authority ID 436973636f00000000000000000000000000000000
 Authority Information Cisco A-ID

```

- **show local-auth statistics** : ローカル EAP の統計情報を表示します。
- **show local-auth certificates** : ローカル EAP で使用可能な証明書を表示します。
- **show local-auth user-credentials** : コントローラがローカル データベースまたは LDAP データベースからユーザの資格情報を取得する際の優先順位を表示します。
- **show advanced eap** : ローカル EAP のタイマーの値を表示します。

```

EAP-Identity-Request Timeout (seconds)..... 1
EAP-Identity-Request Max Retries..... 20
EAP Key-Index for Dynamic WEP..... 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds)..... 20
EAP-Request Max Retries..... 20
EAPOL-Key Timeout (seconds)..... 1
EAPOL-Key Max Retries..... 2

```

- **show ap stats wlan Cisco\_AP** : 各 WLAN の特定のアクセス ポイントにおける EAP タイムアウト回数および失敗回数を表示します。
- **show client detail client\_mac** : アソシエートされた特定のクライアントについて、EAP タイムアウト回数および失敗回数を表示します。これらの統計は、クライアント アソシエーションの問題のトラブルシューティングを行う際に有用です。

```

...
Client Statistics:
 Number of Bytes Received..... 10
 Number of Bytes Sent..... 10
 Number of Packets Received..... 2
 Number of Packets Sent..... 2
 Number of EAP Id Request Msg Timeouts..... 0
 Number of EAP Id Request Msg Failures..... 0
 Number of EAP Request Msg Timeouts..... 2
 Number of EAP Request Msg Failures..... 1
 Number of EAP Key Msg Timeouts..... 0
 Number of EAP Key Msg Failures..... 0
 Number of Policy Errors..... 0
 Radio Signal Strength Indicator..... Unavailable
 Signal to Noise Ratio..... Unavailable

```

- **show wlan wlan\_id** : 特定の WLAN のローカル EAP のステータスを表示します。

**ステップ 14** (任意) 次のコマンドを入力して、ローカル EAP セッションのトラブルシューティングを行います。

- **debug aaa local-auth eap method {all | errors | events | packets | sm} {enable | disable}** : ローカル EAP 方式のデバッグを有効または無効にします。
- **debug aaa local-auth eap framework {all | errors | events | packets | sm} {enable | disable}** : ローカル EAP フレームワークのデバッグを有効または無効にします。  
 (注) 上記の 2 つのコマンドでは、**sm** とはステートマシンを指します。
- **clear stats local-auth** : ローカル EAP のカウンタをクリアします。
- **clear stats ap wlan Cisco\_AP** : 各 WLAN の特定のアクセスポイントにおける EAP タイムアウト回数および失敗回数をクリアします。

```

WLAN 1
 EAP Id Request Msg Timeouts..... 0
 EAP Id Request Msg Timeouts Failures..... 0
 EAP Request Msg Timeouts..... 2
 EAP Request Msg Timeouts Failures..... 1
 EAP Key Msg Timeouts..... 0
 EAP Key Msg Timeouts Failures..... 0
WLAN 2
 EAP Id Request Msg Timeouts..... 1
 EAP Id Request Msg Timeouts Failures..... 0
 EAP Request Msg Timeouts..... 0
 EAP Request Msg Timeouts Failures..... 0
 EAP Key Msg Timeouts..... 3
 EAP Key Msg Timeouts Failures..... 1

```



## 第 51 章

# SpectraLink 社の NetLink 電話用システムの 設定

---

- [SpectraLink NetLink 電話について, 501 ページ](#)
- [SpectraLink 社の NetLink 電話の設定, 501 ページ](#)

## SpectraLink NetLink 電話について

SpectraLink 社の NetLink 電話を Cisco UWN ソリューションと最適な形で統合するには、長いプリアンブルを有効にするようオペレーティングシステムを設定する必要があります。無線プリアンブル（ヘッダーとも呼ばれる）とは、パケットの先頭部分のデータセクションのことであり、ここでは、無線デバイスでのパケットの送受信に必要な情報が格納されています。ショートプリアンブルの方がスループットパフォーマンスが向上するため、デフォルトではこちらが有効になっています。ただし、SpectraLink 社の NetLink 電話などの一部の無線デバイスは、ロングプリアンブルを必要とします。

## SpectraLink 社の NetLink 電話の設定

### 長いプリアンブルの有効化（GUI）

- 
- ステップ 1** [Wireless] > [802.11b/g/n] > [Network] の順に選択して、[802.11b/g Global Parameters] ページを開きます。
  - ステップ 2** [Short Preamble] チェックボックスがオンの場合は、以降の手順に進みます。[Short Preamble] チェックボックスがオフの場合（つまり、長いプリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話用に最適化されているため、これ以降の手順を実行する必要はありません。
  - ステップ 3** [Short Preamble] チェックボックスをオフにして、長いプリアンブルを有効にします。
  - ステップ 4** [Apply] をクリックして、コントローラの設定を更新します。

(注) コントローラへの CLI セッションがアクティブでない場合は、CLI セッションを開始してコントローラをリブートし、リブートプロセスを監視することをお勧めします。コントローラがリブートすると GUI が切断されるため、その意味でも CLI セッションは役に立ちます。

**ステップ 5** [Commands] > [Reboot] > [Reboot] > [Save and Reboot] の順に選択して、コントローラをリブートします。次のプロンプトに対し [OK] をクリックします。

Configuration will be saved and the controller will be rebooted. Click ok to confirm.  
コントローラがリブートします。

**ステップ 6** コントローラの GUI にもう一度ログインし、コントローラが正しく設定されていることを確認します。

**ステップ 7** [Wireless] > [802.11b/g/n] > [Network] の順に選択して、[802.11b/g Global Parameters] ページを開きます。[Short Preamble] チェックボックスがオフの場合、コントローラは SpectraLink 社の NetLink 電話用に最適化されています。

## 長いプリアンブルの有効化 (CLI)

**ステップ 1** コントローラ CLI にログインします。

**ステップ 2** show 802.11b コマンドを入力し、Short preamble mandatory パラメータを選択します。短いプリアンブルが有効になっている場合は、以降の手順に進みます。短いプリアンブルが有効な場合、次のように表示されます。

```
Short Preamble mandatory..... Enabled
```

短いプリアンブルが無効になっている場合（つまり長いプリアンブルが有効な場合）、コントローラはすでに SpectraLink 社の NetLink 電話に対して最適化されているため、以降の手順を実行する必要はありません。

**ステップ 3** 次のコマンドを入力して、802.11b/g ネットワークを無効にします。

```
config 802.11b disable network
```

802.11a ネットワークでは、長いプリアンブルを有効化できません。

**ステップ 4** 次のコマンドを入力して、長いプリアンブルを有効にします。

```
config 802.11b preamble long
```

**ステップ 5** 次のコマンドを入力して、802.11b/g ネットワークを再度有効にします。

```
config 802.11b enable network
```

**ステップ 6** reset system コマンドを入力し、コントローラをリブートします。システムの変更を保存するためのプロンプトが表示されたら、y と入力します。コントローラがリブートします。

**ステップ 7** CLI にログインし直し、show 802.11b コマンドを入力して次のパラメータを表示して、コントローラが正しく設定されていることを確認します。

```
802.11b Network..... Enabled
Short Preamble mandatory..... Disabled
```

上記のパラメータは、802.11b/g ネットワークが有効になっていて、短いプリアンプルが無効になっていることを示しています。

## Enhanced Distributed Channel Access の設定 (CLI)

802.11 Enhanced Distributed Channel Access (EDCA) パラメータを設定して SpectraLink の電話をサポートするには、次の CLI コマンドを入力します。

```
config advanced edca-parameter {custom-voice | optimized-video-voice | optimized-voice | svp-voice | wmm-default}
```

値は次のとおりです。

- **custom-voice** : カスタム音声 EDCA パラメータを有効にします
- **optimized-video-voice** : ビデオと音声用に最適化された複合パラメータを有効にします
- **optimized-voice** : 非 SpectraLink の音声用に最適化されたパラメータを有効にします
- **svp-voice** : SpectraLink Voice Priority (SVP) パラメータを有効にします
- **wmm-default** : Wireless Multimedia (WMM) のデフォルト パラメータを有効にします



(注) このコマンドをコントローラに接続されたすべてのアクセス ポイントに適用するには、このコマンドを入力したあと、802.11b/g ネットワークを無効にし、その後再び有効にしてください。





## 第 52 章

# RADIUS NAC サポートの設定

- [RADIUS NAC サポートについて](#), 505 ページ
- [RADIUS NAC サポートの制約事項](#), 506 ページ
- [RADIUS NAC サポートの設定 \(GUI\)](#), 508 ページ
- [RADIUS NAC サポートの設定 \(CLI\)](#), 508 ページ

## RADIUS NAC サポートについて

Cisco Identity Services Engine (ISE) は、次世代のコンテキストベース アクセス コントロール ソリューションで、Cisco Secure Access Control System (ACS) と Cisco Network Admission Control (NAC) の機能を 1 つの統合されたプラットフォームで提供します。

ISE は Cisco Unified Wireless Network のリリース 7.0.116.0 で導入されています。ISE を使用して、配備されたネットワークで高度なセキュリティを実現できます。ISE は、コントローラ上で設定できる認証サーバです。RADIUS NAC 対応の WLAN 上のコントローラにクライアントがアソシエートされると、コントローラは ISE サーバに要求を転送します。

ISE サーバはデータベースでユーザを検証し、認証が正常に完了すると、URL と事前認証 ACL がクライアントに送信されます。このときクライアントは Posture Required 状態になり、ISE サーバから返された URL にリダイレクトされます。



(注) ISE サーバから返された URL にキーワード「**cwa**」が含まれる場合、クライアントは、Central Web Authentication の状態になります。

クライアントの NAC エージェントによって、ポスチャ検証プロセスがトリガーされます。ISE サーバによるポスチャ検証が正常に完了すると、クライアントは RUN 状態になります。



(注) RADIUS NAC による Flex ローカル スイッチングは、リリース 7.2.110.0 で追加されました。これは、7.0 リリースおよび 7.2 リリースではサポートされていません。RADIUS NAC 対応の WLAN 機能が動作するよう再設定するには、7.2.110.0 以降のリリースを 7.2 または 7.0 リリースにダウングレードする必要があります。

## デバイス登録

デバイス登録を行うと、RADIUS NAC を使用して WLAN の新しいデバイスの認証とプロビジョニングを行えるようになります。デバイスを WLAN に登録すると、設定されている ACL に基づいてネットワークを使用できるようになります。

## 中央 Web 認証

中央 Web 認証 (CWA) の場合、Web 認証は ISE サーバで行われます。ISE サーバの Web ポータルに、クライアント用のログインページが表示されます。ISE サーバで資格情報が検証されると、クライアントがプロビジョニングされます。CoA が適用されるまで、クライアントは POSTURE\_REQD 状態のままです。資格情報と ACL が ISE サーバから送信されます。

## ローカル Web 認証

ローカル Web 認証は、RADIUS NAC でサポートされていません。

次の表に、一般的な ISE でのデバイス登録、CWA、および LWA の有効な組み合わせを示します。

表 15: ISE ネットワーク認証フロー

| WLAN の設定      | CWA  | LWA                 | デバイス登録 |
|---------------|------|---------------------|--------|
| RADIUS NAC 対応 | Yes  | No                  | Yes    |
| L2 なし         | No   | PSK、Static WEP、CKIP | No     |
| L3 なし         | 該当なし | 内部/外部               | 該当なし   |
| MAC フィルタリング対応 | Yes  | No                  | Yes    |

## RADIUS NAC サポートの制約事項

- RADIUS NAC 対応の WLAN は、オープン認証と MAC フィルタリングをサポートしています。
- 設定されたアカウントングサーバが認証 (ISE) サーバではない場合、RADIUS NAC は機能しません。ISE 機能を使用する場合は、認証およびアカウントングサーバと同じサーバ



を設定する必要があります。ISE を ACS 機能専用にする場合は、アカウントिंगサーバを柔軟に設定できます。

- 認証またはアカウントING RADIUS サーバに障害が発生した場合、認証またはアカウントING サーバのリスト内の該当するサーバが起動しなくなります。これは、クライアント認証およびアカウントINGが同じ IP 認証およびアカウントING サーバで実行されていることを意味しています。ただし、認証およびアカウントING サーバを連携させる場合、RADIUS サーバの設定時にこれらのサーバを同じ順序で追加する必要があります。
- クライアントがある WLAN から別の WLAN へ移動し、アイドルタイムアウトが発生する前に元の WLAN に戻った場合、コントローラはそのクライアントの監査セッション ID を保持しています。したがって、アイドルタイムアウトセッションの期限が切れる前にクライアントがコントローラに join すると、それらのクライアントはただちに RUN 状態になります。セッションがタイムアウトしてから、クライアントがコントローラに再アソシエートされているかどうかを検証されます。
- たとえば 2 つの WLAN があり、1 台のコントローラに WLAN 1 が設定され (WLC1)、もう 1 台のコントローラに WLAN 2 が設定され (WLC2)、その両方が RADIUS NAC 対応であるとします。クライアントはまず WLC1 に接続し、ポスチャ検証のあと RUN 状態になります。次にこのクライアントは、WLC2 に移動するとします。WLC1 内のこのクライアントに対する PMK の期限が切れる前に、クライアントが WLC1 に再接続した場合、このクライアントに対するポスチャ検証は省略されます。クライアントはポスチャ検証を省略してただちに RUN 状態になります。これは、コントローラがこのクライアントの古い監査セッション ID を保持し、ISE がその ID をすでに認識しているからです。
- ワイヤレス ネットワークに RADIUS NAC を導入する場合は、プライマリおよびセカンダリ ISE サーバを設定しないでください。代わりに、2 つの ISE サーバ間に HA を設定することをお勧めします。プライマリおよびセカンダリ ISE を設定すると、クライアントが RUN 状態に移行する前に、ポスチャ検証が必要になります。HA を設定すると、クライアントはフォールバック ISE サーバで自動的に RUN 状態に移行します。
- RADIUS NAC が設定されたコントローラ ソフトウェアは、サービス ポートでの認可変更 (CoA) をサポートしません。
- アクティブなネットワーク内で AAA サーバインデックスを入れ替えないでください。クライアントが切断され、RADIUS サーバへの再接続が必要になる可能性があります。それによって、ISE サーバログにログ メッセージが追加される場合があります。
- RADIUS NAC を使用するには、WLAN 上で AAA Override を有効にする必要があります。
- WLAN 上で WPA および WPA2 または dot1X を有効にする必要があります。
- 低速なローミング中に、クライアントのポスチャ検証が行われます。
- ゲストのトンネリング モビリティは、ISE NAC 対応の WLAN でサポートされます。
- VLAN Select はサポートされません。
- ワークグループブリッジはサポートされません。
- AP Group over NAC は RADIUS NAC ではサポートされません。

- FlexConnect ローカル スイッチングはサポートされません。
- RADIUS NAC を有効にすると、RADIUS サーバの上書きインターフェイスはサポートされません。
- クライアントとサーバ間の DHCP 通信。DHCP プロファイルは一度だけ解析されます。これは一度だけ ISE サーバに送信されます。
- AAA の `url-redirect-acl` および `url-redirect` 属性を AAA サーバが要求する場合、AAA Override 機能をコントローラで有効にする必要があります。

## RADIUS NAC サポートの設定 (GUI)

---

ステップ 1 [WLANs] タブを選択します。

ステップ 2 ISE を有効にする WLAN の WLAN ID をクリックします。  
[WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [NAC State] ドロップダウン リストから [Radius NAC] を選択します。

- [SNMP NAC] : WLAN に SNMP NAC を使用します。
- [Radius NAC] : WLAN に Radius NAC を使用します。  
(注) WLAN 上で RADIUS NAC を使用すると、自動的に AAA Override が有効になります。

ステップ 5 [Apply] をクリックします。

---

## RADIUS NAC サポートの設定 (CLI)

次のコマンドを入力します。

```
config wlan nac radius { enable | disable } wlan_id
```



# 第 53 章

## 設定の RADIUS VSA およびレルム

- [RADIUS VSA の設定, 509 ページ](#)
- [RADIUS レルムの設定, 512 ページ](#)

### RADIUS VSA の設定

#### RADIUS VSA に関する情報

インターネット エンジニアリング タスク フォース (IETF) のドラフト標準では、ネットワーク アクセスサーバと RADIUS サーバ間でベンダー固有の属性 (VSA) を使用してベンダー固有の情報を伝達する方法が規定されています。VSA を使用すれば、ベンダーは一般的な用途に適さない独自の拡張属性をサポートできます。VSA は XML ファイル内で事前に定義されます。XML ファイルにベンダー固有の属性を追加する必要があり、この XML ファイルがコントローラにダウンロードされます。このサポートを有効にするためにコントローラ上で実施しなければならない設定はありません。ファイルには、XML タグを指定するための XML スキーマで規定されている特定の形式で RADIUS 属性が含まれています。

定義されたベンダー固有の属性を含む XML ファイルは FTP サーバからダウンロードできます。ダウンロードしたファイルはフラッシュメモリに保存され、複数のリブートプロセスを通して保持されます。ファイルは、ダウンロードが成功したときとコントローラが起動するたびに解析されます。XML ファイルは RADIUS サーバにアップロードして認証とアカウントングに使用できます。コントローラは、これらの値を解析すると、そのファイルをベンダー固有の属性を保存するための別のデータ構造に保存します。また、指定された使用形式に基づいて、認証パケットとアカウントングパケットのどちらかまたはその両方でこれらの属性値を使用します。ファイルにエラーが含まれている場合は、コントローラの解析が失敗して、属性が適用されません。ファイル内のエラーを修正するか、ファイルを FTP サーバからコントローラにダウンロードし直す必要があります。

## RADIUS AVP リストの XML サンプル ファイル

参照用に、RADIUS AVP リストの XML サンプル ファイルを使用できます。サンプル XML ファイルには2個の属性のみが含まれていて、1つは認証用、もうひとつはアカウントング用です。RADIUS の属性と値のペアを追加することができますが、これらの属性と値のペアは、指定された形式で追加する必要があります。

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file edited by User1-->

<radiusFile>
<avpList SSID_PROF="test" incAuth="true" incAcct="false">
 <radiusAttributes>
 <attributeName>Idle-Timeout</attributeName>
 <vendorId>9</vendorId>
 <attributeId>21</attributeId>
 <valueType>INTEGER</valueType>
 <attributeValue>100</attributeValue>
 </radiusAttributes>
 <radiusAttributes>
 <attributeName>remote-name</attributeName>
 <vendorId>9</vendorId>
 <attributeId>26</attributeId>
 <valueType>STRING</valueType>
 <attributeValue>TEST</attributeValue>
 </radiusAttributes>
</avpList>
<avpList SSID_PROF="test" incAcct="true">
 <radiusAttributes>
 <attributeName>Idle-Timeout</attributeName>
 <vendorId>9</vendorId>
 <attributeId>21</attributeId>
 <valueType>INTEGER</valueType>
 <attributeValue>100</attributeValue>
 </radiusAttributes>
 <radiusAttributes>
 <attributeName>remote-name</attributeName>
 <vendorId>9</vendorId>
 <attributeId>26</attributeId>
 <valueType>STRING</valueType>
 <attributeValue>TEST</attributeValue>
 </radiusAttributes>
</avpList>
</radiusFile>
```

## RADIUS AVP リストのダウンロード (GUI)

**ステップ 1** [Commands] > [Download File] の順に選択して、[Download File to Controller] ページを開きます。

**ステップ 2** [File Type] ドロップダウン リストから、[RADIUS AVP List] を選択します。

**ステップ 3** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- TFTP
- FTP

- SFTP

**ステップ 4** [IP Address] テキスト ボックスに、サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

**ステップ 5** [File Path] テキスト ボックスに、RADIUS AVP リストのディレクトリ パスを入力します。

**ステップ 6** [File Name] テキスト ボックスに、RADIUS AVP リストの名前を入力します。

**ステップ 7** FTP サーバを使用している場合は、次の手順に従います。

a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。

b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。

c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。SFTP のデフォルト値は 22 です。

**ステップ 8** コントローラに RADIUS AVP リストをダウンロードするには、[Download] をクリックします。ダウンロードのステータスを示すメッセージが表示されます。

**ステップ 9** [Security] > [AAA] > [RADIUS] > [Downloaded AVP] を選択して、[Download RADIUS AVP List] ページを開きます。

**ステップ 10** [WLAN SSID Profile name] ドロップダウン リストから、WLAN SSID プロファイル名を選択します。

**ステップ 11** AVP リストにマッピングされた RADIUS 認証属性を表示するには、[Auth AVP] タブをクリックします。

**ステップ 12** AVP リストにマッピングされた RADIUS アカウンティング属性を表示するには、[Acct AVP] タブをクリックします。

## RADIUS AVP リストのアップロード (GUI)

**ステップ 1** [Commands] > [Upload File] の順に選択して、[Upload File from Controller] ページを開きます。

**ステップ 2** [File Type] ドロップダウン リストから、[RADIUS AVP List] を選択します。

**ステップ 3** [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。

- TFTP
- FTP
- SFTP

**ステップ 4** [IP Address] テキスト ボックスに、サーバの IPv4 アドレスまたは IPv6 アドレスを入力します。

**ステップ 5** [File Path] テキスト ボックスに、RADIUS AVP リストのディレクトリ パスを入力します。

**ステップ 6** [File Name] テキスト ボックスに、RADIUS AVP リストの名前を入力します。

**ステップ 7** FTP サーバを使用している場合は、次の手順に従います。

- a) [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
- b) [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
- c) [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。SFTP のデフォルト値は 22 です。

**ステップ 8** コントローラから RADIUS AVP リストをアップロードするには、[Upload] をクリックします。アップロードのステータスを示すメッセージが表示されます。

## RADIUS AVP リストのアップロードおよびダウンロード (CLI)

**ステップ 1** コントローラ CLI にログインします。

**ステップ 2** 次のコマンドを入力して、FTP サーバからコントローラに XML ファイル形式の RADIUS AVP をダウンロードします。

```
transfer download datatyperadius-avplist
```

**ステップ 3** 次のコマンドを使用して、コントローラから RADIUS サーバへ XML ファイルをアップロードします。

```
transfer upload datatyperadius-avplist
```

**ステップ 4** 次のコマンドを使用して、VSA AVP を表示します。

```
show radius avp-listssid-profile-name
```

## RADIUS レルムの設定

### RADIUS レルムについて

モバイルクライアントが WLAN にアソシエートするときに、RADIUS レルムが認証要求パケット内の EAP-AKA ID 応答要求の一部として受信されます。WLAN のネットワークアクセス識別子 (NAI) 形式 (EAP-AKA) は、`0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org` として指定できます。NAI 形式のレルムは @ 記号の後ろに示され、`wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org` のように指定されます。ベンダー固有の属性が MCC については 311、MNC については 480 ~ 489 として追加された場合、その NAI 形式は `0311480999999999@wlan.mnc480.mcc311.3gppnetwork.org` のように指定できます。

モバイル加入者の場合、コントローラは、デバイスから受信した NAI 形式のレルムが特定の標準に従っている場合にのみ、AAA サーバに認証要求を送信します。認証とは別に、アカウントینگ要求もレルム フィルタリングに基づいて AAA サーバに送信する必要があります。

コントローラ上でレルム フィルタリングをサポートするには、RADIUS 上でレルムを設定する必要があります。ユーザが特定の SSID を使用して接続されている場合、RADIUS サーバ上で設定されたレルムに対して受信された NAI 形式を使用してユーザが認証および認可されます。

#### WLAN 上のレルム サポート

各 WLAN は NAI レルムをサポートするように設定されます。レルムが特定の SSID に対して有効になっている場合は、RADIUS サーバ上で設定されたレルムに対して EAPID 応答で受信されたレルムを照合するためのルックアップが実施されます。

#### RADIUS サーバ上のレルム サポート

RADIUS サーバは、設定されたレルムに基づいて認証要求とアカウントिंग要求をリダイレクトする必要があります。1つの RADIUS サーバが認証とアカウントिंगごとに最大 30 のレルムをサポートします。

- **認証用のレルム照合**：EAP 方式を使用した WPA2 dot1x (EAP AKA と同様) では、ユーザ名が EAP ID 応答の一部として受信されます。レルムは、ユーザ名から抽出され、RADIUS 認証サーバで設定されたレルムと照合されます。一致した場合は、認証要求が RADIUS サーバに転送されます。一致しなかった場合は、クライアントが認証解除されます。
- **アカウントिंग用のレルム照合**：ユーザ名が Access Accept メッセージで受信されます。アカウントING メッセージがトリガーされると、レルムがユーザ名から抽出され、RADIUS アカウントING サーバ上で設定されたアカウントING レルムと比較されます。一致した場合は、アカウントING 要求が RADIUS サーバに転送されます。一致しなかった場合は、アカウントING 要求が破棄されます。たとえば、レルムがコントローラ上で **cisco** として設定されている場合は、RADIUS サーバ上でユーザ名が **xyz@cisco** として認証されます。



(注) NAI レルムが WLAN 上で有効になっていても、レルムがユーザ名に含まれていない場合は、動作がデフォルトでルックアップなしに設定され、RADIUS サーバの通常の選択が使用されません。



(注) クライアントが高速再認証識別を使用すると、コントローラで対応する要求を正しいサーバに転送するために、認証サーバからレルム名が要求されます。

EAP-AKA をレルムと組み合わせて使用したとき、eap サーバがユーザ名部分とレルム部分の両方がある AT\_NEXT\_REAUTH\_ID 属性で応答すると、高速再認証がサポートされます。レルムの目的は、受信コントローラが後続の高速再認証要求で正しいサーバをつかまえることです。たとえば EAP-AKA をサポートしているホスト apd サーバはレルム部分をサポートしません。したがって Cisco WLC は、この互換性がある eap サーバについてのみ、高速再認証をサポートしています。

## RADIUS レルムの設定の前提条件

RADIUS 認証またはアカウントिंग サーバは、レルムを追加する前に無効し、コントローラ上でレルムを追加した後に有効にする必要があります。

## RADIUS レルムの設定に関する制約事項

- 1つのコントローラに、最大 17 個の RADIUS 認証サーバおよびアカウントングサーバを設定できます。
- 1つの RADIUS 認証サーバおよびアカウントングサーバに対して、設定できるレルムの合計数は 30 です。

## WLAN でのレルムの設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
  - ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
  - ステップ 3 [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。
  - ステップ 4 WLAN でレルムを有効にするには、[RADIUS NAI-Realm] チェックボックスをオンにします。
  - ステップ 5 [Apply] をクリックして、変更を確定します。
  - ステップ 6 [Save Configuration] をクリックして、変更を保存します。
- 

## WLAN でのレルムの設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、WLAN でレルムを有効または無効にします。  
**config wlanradius\_server realm {enable | disable} wlan-id**
  - ステップ 2 次のコマンドを入力して、WLAN のレルムの設定を表示します。  
**show wlan wlan-id**
-



## RADIUS 認証サーバでのレルムの設定 (GUI)

- 
- ステップ 1 [Security] > [AAA] > [RADIUS] > [Authentication] の順に選択して、[RADIUS Authentication Servers > Edit] ページを開きます。
  - ステップ 2 [Realm List] リンクをクリックし、[Authentication Server Index] ページを開きます。
  - ステップ 3 [Realm Name] テキストボックスにレルム名を入力します。
  - ステップ 4 [Add] をクリックします。
- 

## RADIUS 認証サーバでのレルムの設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、RADIUS 認証サーバにレルムを追加します。  
**config radius auth realm add *radius\_index realm\_string***
  - ステップ 2 次のコマンドを入力して、RADIUS 認証サーバからレルムを削除します。  
**config radius auth realm delete *radius\_index realm\_string***
  - ステップ 3 このコマンドを入力して、RADIUS 認証サーバの情報を表示します。  
**show radius auth detailed *radius\_index***
- 

## RADIUS アカウンティングサーバでのレルムの設定 (GUI)

- 
- ステップ 1 [Security] > [AAA] > [RADIUS] > [Accounting] の順に選択して、[RADIUS Accounting Servers > Edit] ページを開きます。
  - ステップ 2 [Realm List] リンクをクリックし、[Accounting Server Index] ページを開きます。
  - ステップ 3 [Realm Name] テキストボックスにレルム名を入力します。
  - ステップ 4 [Add] をクリックします。
- 

## RADIUS アカウンティングサーバでのレルムの設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、RADIUS アカウンティングサーバにレルムを追加します。

**config radius acct realm add***radius\_indexrealm\_string*

**ステップ 2** このコマンドを使用して RADIUS アカウンティング サーバからレルムを削除します。

**config radius acct realm delete***radius\_indexrealm\_string*

**ステップ 3** このコマンドを使用して RADIUS アカウンティング サーバの情報を表示します。

**show radius acct detailed***radius\_index*

---



# 第 54 章

## 無線による管理機能の使用

---

- [無線による管理機能について](#), 517 ページ
- [無線による管理機能の有効化 \(GUI\)](#), 517 ページ
- [無線による管理機能の有効化 \(CLI\)](#), 517 ページ

### 無線による管理機能について

無線による管理機能を使用すると、ワイヤレスクライアントを使用してローカルコントローラを監視および設定できます。この機能は、コントローラとの間のアップロードおよびダウンロード（転送）以外のすべての管理タスクに対して使用できます。

### 無線による管理機能の有効化 (GUI)

---

- ステップ 1 [Management] > [Mgmt Via Wireless] の順に選択して、[Management Via Wireless] ページを開きます。
  - ステップ 2 [Enable Controller Management to be accessible from Wireless Clients] チェックボックスをオンにして無線による WLAN の管理を有効にするか、オフにしてこの機能を無効にします。デフォルト値はオフです。
  - ステップ 3 [Apply] をクリックして、変更を確定します。
  - ステップ 4 [Save Configuration] をクリックして、変更を保存します。
- 

### 無線による管理機能の有効化 (CLI)

---

- ステップ 1 次のコマンドを入力して、無線による管理インターフェイスが有効か無効かを検証します。

**show network summary**

- 無効である場合は、**config network mgmt-via-wireless enable** コマンドを入力して、無線による管理を有効にします。
- 無効でない場合は、ワイヤレス クライアントを使用して、管理対象のコントローラに接続されているアクセス ポイントにアソシエートします。

**ステップ 2** 次のコマンドを入力して CLI にログインし、ワイヤレス クライアントを使用して WLAN を管理できることを確認します。

**telnet controller-ip-address command**

---



# 第 55 章

## 動的インターフェイスによる管理機能

- [動的インターフェイスによる管理機能について](#), 519 ページ
- [動的インターフェイスによる管理機能の設定 \(CLI\)](#), 520 ページ

### 動的インターフェイスによる管理機能について

動的インターフェイス IP アドレスのいずれかを使用して、コントローラにアクセスできます。有線コンピュータでは、WLC の動的インターフェイスを使用した CLI アクセスのみが可能ですが、ワイヤレスクライアントでは、動的インターフェイスを使用して CLI アクセスと GUI アクセスの両方が可能です。

動的インターフェイスによる管理機能が無効な場合、SSH プロトコルが有効であれば、デバイスは SSH 接続を開くことができます。ただし、ログオンプロンプトは表示されません。さらに、CPU ACL が設定されていない限り、動的インターフェイス VLAN から管理アドレスへのアクセスは引き続き可能です。動的インターフェイスを使用した管理が CPU ACL とともに有効になっている場合、CPU ACL が優先されます。

次に、管理アクセスの例および動的インターフェイスを使用した管理アクセスの例を示します。この例では、Cisco WLC の管理 VLAN IP アドレスは 209.165.201.1 です。また Cisco WLC のダイナミック VLAN IP アドレスは 209.165.202.129 です。

- Cisco WLC の動的インターフェイス VLAN からのソース有線クライアントは、管理インターフェイス VLAN にアクセスして、管理アクセスを試みます。これは、管理アクセスの例です。
- Cisco WLC の管理インターフェイス VLAN からのソース有線クライアントは、動的インターフェイス VLAN にアクセスして、管理アクセスを試みます。これは、動的インターフェイスを使用した管理の例です。
- Cisco WLC の動的インターフェイス VLAN からのソース有線クライアントは、動的インターフェイス VLAN にアクセスして、管理アクセスを試みます。これは、動的インターフェイスを使用した管理の例です。

- レイヤ 3 VLAN インターフェイスからのソース有線クライアントは、動的インターフェイスまたは管理インターフェイスにアクセスして、管理アクセスを試みます。これは、動的インターフェイスを使用した管理の例です。

ここでの管理とは、管理インターフェイスではなくコンフィギュレーションアクセスです。Cisco WLC の設定に、管理 IP 以外の Cisco WLC の他の IP アドレスからもアクセスする場合は、動的インターフェイスを使用して管理されます。

## 動的インターフェイスによる管理機能の設定 (CLI)

次のコマンドを入力して、動的インターフェイスを使用した管理を有効または無効にします。

```
config network mgmt-via-dynamic-interface {enable | disable}
```



# 第 56 章

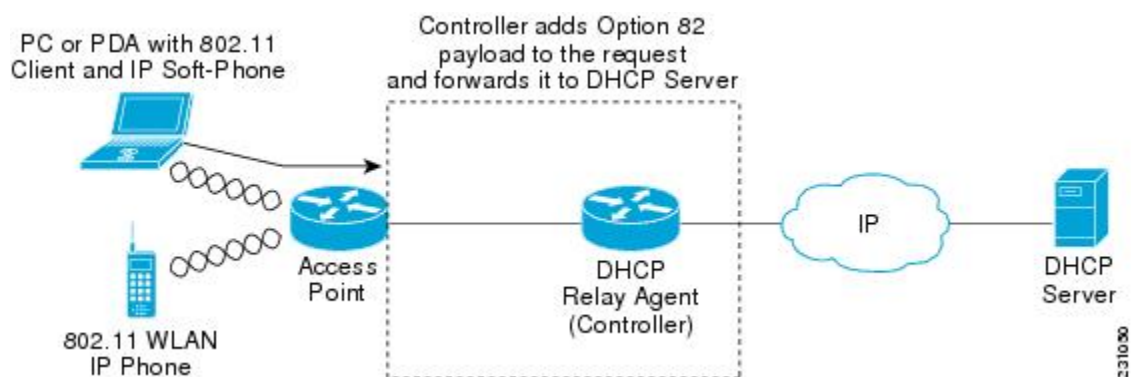
## DHCP オプション 82 の設定

- [DHCP オプション 82 について, 521 ページ](#)
- [DHCP オプション 82 の制約事項, 522 ページ](#)
- [DHCP オプション 82 の設定 \(GUI\) , 522 ページ](#)
- [DHCP オプション 82 の設定 \(CLI\) , 522 ページ](#)

### DHCP オプション 82 について

DHCP オプション 82 では、DHCP を使用してネットワークアドレスを割り当てる場合のセキュリティが強化されます。コントローラが DHCP リレー エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP サーバに転送するようにクライアントからの DHCP 要求にオプション 82 情報を追加するようにコントローラを設定できます。

図 45: DHCP オプション 82



アクセス ポイントは、クライアントからのすべての DHCP 要求をコントローラに転送します。コントローラは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送しま

す。このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセスポイントの SSID が含まれます。



(注) すでにリレーエージェントオプションが含まれている DHCP パケットは、コントローラでドロップされます。

DHCP オプション 82 が正しく動作するには、DHCP プロキシが有効でなければなりません。

## DHCP オプション 82 の制約事項

- DHCP オプション 82 は、自動アンカー モビリティと共に使用することはできません。

## DHCP オプション 82 の設定 (GUI)

- 
- ステップ 1 [Controller] > [Advanced] > [DHCP] を選択して、[DHCP Parameters] ページを開きます。
- ステップ 2 [Enable DHCP Proxy] チェックボックスをオンにして、DHCP プロキシを有効にします。
- ステップ 3 ドロップダウンリストから [DHCP Option 82 Remote ID field format] を選択して、DHCP オプション 82 ペイロードの形式を指定します。  
使用可能なオプションの詳細については、コントローラのオンラインヘルプを参照してください。
- ステップ 4 DHCP タイムアウト時間を入力します。タイムアウト値はグローバルに適用できます。
- ステップ 5 [Apply] をクリックします。
- ステップ 6 [Save Configuration] をクリックします。
- 

### 次の作業

コントローラの CLI で、次のコマンドを入力して、WLAN が関連付けられている動的インターフェイスの DHCP オプション 82 を有効にできます。

```
config interface dhcp dynamic-interface interface-name option-82 enable
```

## DHCP オプション 82 の設定 (CLI)

- 次のコマンドのいずれかを入力して、DHCP オプション 82 ペイロードの形式を設定します。
  - `config dhcp opt-82 remote-id ap_mac` : DHCP オプション 82 ペイロードにアクセスポイントの MAC アドレスを追加します。
  - `config dhcp opt-82 remote-id ap_mac:ssid` : DHCP オプション 82 ペイロードにアクセスポイントの MAC アドレスと SSID を追加します。



- **config dhcp opt-82 remote-id ap-ethmac** : DHCP オプション 82 ペイロードにアクセスポイントのイーサネット MAC アドレスを追加します。
  - **config dhcp opt-82 remote-id apname:ssid** : DHCP オプション 82 ペイロードにアクセスポイントの AP 名と SSID を追加します。
  - **config dhcp opt-82 remote-id ap-group-name** : DHCP オプション 82 ペイロードに AP グループ名を追加します。
  - **config dhcp opt-82 remote-id flex-group-name** : DHCP オプション 82 ペイロードに FlexConnect グループ名を追加します。
  - **config dhcp opt-82 remote-id ap-location** : DHCP オプション 82 ペイロードに AP ロケーションを追加します。
  - **config dhcp opt-82 remote-id apmac-vlan-id** : DHCP オプション 82 ペイロードにアクセスポイントの MAC アドレスと VLAN ID を追加します。
  - **config dhcp opt-82 remote-id apname-vlan-id** : DHCP オプション 82 ペイロードに AP 名とその VLAN ID を追加します。
  - **config dhcp opt-82 remote-id ap-ethmac-ssid** : DHCP オプション 82 ペイロードにアクセスポイントのイーサネット MAC アドレスと SSID を追加します。
- 次のコマンドを入力して、WLAN が関連付けられている動的インターフェイスに対して DHCP オプション 82 を有効にします。  
**config interface dhcp dynamic-interface *interface-name* option-82 enable**
  - **show interface detailed *dynamic-interface-name*** コマンドを入力して、動的インターフェイスの DHCP オプション 82 のステータスを確認してください。





# 第 57 章

## アクセスコントロールリストの設定と適用

- [アクセスコントロールリストについて](#), 525 ページ
- [アクセスコントロールリストの制約事項](#), 526 ページ
- [アクセスコントロールリストの設定と適用 \(GUI\)](#), 527 ページ
- [アクセスコントロールリストの設定と適用 \(CLI\)](#), 531 ページ
- [レイヤ2アクセスコントロールリストの設定](#), 533 ページ
- [DNS ベースのアクセスコントロールリストの設定](#), 538 ページ

### アクセスコントロールリストについて

アクセスコントロールリスト (ACL) は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです (たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます)。コントローラで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレスクライアントとやり取りするデータトラフィックの制御用の WLAN、あるいは Central Processing Unit (CPU; 中央処理装置) 宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

または、Web 認証用に事前認証 ACL を作成することもできます。事前認証 ACL を使用すると、認証が完了する前に、特定の種類のトラフィックを許可することができます。

IPv4 ACL および IPv6 ACL のどちらもサポートされています。IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。



(注) ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

## アクセスコントロールリストの制約事項

- IPv4 および IPv6 の両方に最大 64 の ACL を定義し、各 ACL に最大 64 のルール（またはフィルタ）を適用できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットが1つのルールの全パラメータと一致した場合、そのルールに設定された処理がそのパケットに適用されます。
- Cisco 5500 シリーズ コントローラまたは Cisco WiSM2 で CPU ACL を適用する場合、Web 認証のために仮想インターフェイス IP アドレスに送信されるトラフィックを許可する必要があります。
- すべての ACL で、最後のルールとして暗黙の「deny all」ルールが適用されます。パケットがどのルールとも一致しない場合、コントローラによってドロップされます。
- Cisco 5500 シリーズ コントローラまたはコントローラ ネットワーク モジュールと共に外部の Web サーバを使用している場合は、WLAN 上で外部 Web サーバに対する事前認証 ACL を設定する必要があります。
- インターフェイスまたは WLAN に ACL を適用すると、1 Gbps ファイルサーバからのダウンロードの際にワイヤレス スループットが低下します。スループットを改善するには、インターフェイスまたは WLAN から ACL を削除するか、ポリシー レート制限制約機能を持つ隣接有線デバイスに ACL を移動するか、1 Gbps ではなく 100 Mbps を使用してファイルサーバを接続します。
- 有線ネットワークから受信した無線クライアントに向かうマルチキャスト トラフィックは WLC ACL では処理されません。無線クライアントから開始され同じコントローラの有線ネットワークまたはその他のワイヤレスクライアントに向かうマルチキャスト トラフィックは、WLC ACL によって処理されます。
- ACL はコントローラ上で直接設定されるか、Cisco Prime Infrastructure のテンプレートを使用して設定されます。ACL 名は固有の名前でなければなりません。
- クライアント（AAA によって上書きされる ACL）ごと、もしくはインターフェイスまたは WLAN で ACL を設定できます。AAA によって上書きされる ACL の優先度が最も高くなります。ただし、適用する各インターフェイス、WLAN、またはクライアントごとの ACL の設定は、お互いを上書きできます。
- ピアツーピア ブロッキングが有効になると、トラフィックは ACL で許可されてもピア間でブロックされます。

## アクセスコントロール リストの設定と適用 (GUI)

### アクセスコントロール リストの設定

- ステップ 1** [Security] > [Access Control Lists] > [Access Control Lists] を選択して、[Access Control Lists] ページを開きます。
- ステップ 2** パケットがコントローラに設定された ACL のいずれかに一致するかどうかを確認する場合は、[Enable Counters] チェックボックスをオンにして [Apply] をクリックします。それ以外の場合、このチェックボックスはオフ (デフォルト値) のままにしておきます。この機能は、システムのトラブルシューティングを実行する際に役立ちます。
- (注) ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。
- ステップ 3** [New] をクリックして、新しい ACL を追加します。[Access Control Lists > New] ページが表示されます。
- ステップ 4** [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。
- ステップ 5** ACL タイプを選択します。IPv4 と IPv6 の 2 つの ACL のタイプがサポートされています。
- ステップ 6** [Apply] をクリックします。[Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。
- ステップ 7** [Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。[Access Control Lists > Rules > New] ページが表示されます。
- ステップ 8** この ACL のルールを次のように設定します。
- a) コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] テキスト ボックスで、値 (1 ~ 64) を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。
 

(注) ルール 1 ~ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。
  - b) [Source] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの送信元を指定します。
    - [Any] : 任意の送信元 (これはデフォルト値です)。
    - [IP Address] : 特定の送信元。このオプションを選択する場合は、テキスト ボックスに送信元の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、テキスト ボックスに宛先の IPv6 アドレスとプレフィックスの長さを入力します。
  - c) [Destination] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するパケットの宛先を指定します。

- [Any] : 任意の宛先 (これはデフォルト値です)。
  - [IP Address] : 特定の宛先。このオプションを選択する場合は、テキストボックスに宛先の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、テキストボックスに宛先の IPv6 アドレスとプレフィックスの長さを入力します。
- d) [Protocol] ドロップダウンリストから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコルオプションは次のとおりです。
- [Any] : 任意のプロトコル (これはデフォルト値です)
  - [TCP] : トランスミッションコントロールプロトコル
  - [UDP] : ユーザデータグラムプロトコル
  - [ICMP/ICMPv6] : インターネット制御メッセージプロトコル
    - (注) ICMPv6 は IPv6 ACL でのみ使用可能です。
  - [ESP] : IP カプセル化セキュリティペイロード
  - [AH] : 認証ヘッダー
  - [GRE] : Generic Routing Encapsulation
  - [IP in IP] : Internet Protocol (IP) in IP (IP-in-IP パケットのみを許可または拒否)
  - [Eth Over IP] : Ethernet-over-Internet プロトコル
  - [OSPF] : Open Shortest Path First
  - [Other] : その他の Internet Assigned Numbers Authority (IANA) プロトコル
    - (注) [Other] を選択する場合は、[Protocol] テキストボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルのリストは IANA Web サイトで確認できます。

コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット (ARP パケットなど) は指定できません。

- e) 前の手順で [TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つのパラメータも追加で表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポートオプションは、ネットワークスタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。
- (注) ACL タイプに基づく送信元および宛先ポート。
- f) [DSCP] ドロップダウンリストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point (DSCP) 値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダーテキストボックスです。
- [Any] : 任意の DSCP (これはデフォルト値です)
  - [Specific] : DSCP 編集ボックスに入力する、0 ~ 63 の特定の DSCP

- g) [Direction] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL を適用するトラフィックの方向を指定します。
- [Any] : 任意の方向 (これはデフォルト値です)
  - [Inbound] : クライアントから
  - [Outbound] : クライアントへ
- (注) この ACL をコントローラ CPU に適用する予定の場合、パケットの方向は重要ではないので常に「Any」です。
- h) [Action] ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。
- i) [Apply] をクリックして、変更を確定します。[Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。  
[Deny Counters] フィールドには、パケットが明示的拒否 ACL ルールに一致した回数が表示されます。  
[Number of Hits] フィールドには、パケットが ACL ルールに一致した回数が表示されます。これらのフィールドを有効にするには、[Access Control Lists] ページ上で ACL カウンタを有効にする必要があります。
- (注) ルールを編集する場合は、希望のルールのシーケンス番号をクリックし、[Access Control Lists > Rules > Edit] ページを開きます。ルールを削除するには、該当するルールの青いドロップダウン矢印の上にカーソルを置き、[Remove] を選択します。
- j) この ACL にさらにルールを追加するにはこの手順を繰り返します。

**ステップ 9** [Save Configuration] をクリックして、変更を保存します。

**ステップ 10** さらに ACL を追加するにはこの手順を繰り返します。

## インターフェイスへのアクセス コントロール リストの適用

**ステップ 1** [Controller] > [Interfaces] の順に選択します。

**ステップ 2** 目的のインターフェイスの名前をクリックします。そのインターフェイスの [Interfaces > Edit] ページが表示されます。

**ステップ 3** [ACL Name] ドロップダウン リストから必要な ACL を選択し、[Apply] をクリックします。デフォルトは [None] です。

(注) インターフェイス ACL としてサポートされるのは IPv4 ACL だけです。

**ステップ 4** [Save Configuration] をクリックして、変更を保存します。

## コントローラ CPU へのアクセスコントロールリストの適用

- 
- ステップ 1** [Security] > [Access Control Lists] > [CPU Access Control Lists] の順に選択して、[CPU Access Control Lists] ページを開きます。
- ステップ 2** [Enable CPU ACL] チェックボックスをオンにして、指定した ACL でコントローラの CPU へのトラフィックを制御できるようにするか、チェックボックスをオフにして CPU ACL の機能を無効にし、CPU にすでに適用されている ACL をすべて削除します。デフォルト値はオフです。
- ステップ 3** [ACL Name] ドロップダウンリストから、コントローラの CPU へのトラフィックを制御する ACL を選択します。デフォルト値は [None] で、CPU ACL 機能は無効にされています。[CPU ACL Enable] チェックボックスをオンにして [None] を選択すると、ACL を選択する必要があることを示すエラーメッセージが表示されます。
- (注) このパラメータは、[CPU ACL Enable] チェックボックスをオンにした場合のみ使用できません。
  - (注) CPU ACL が有効な場合、その CPU ACL は無線トラフィックと有線トラフィックの両方に適用されます。CPU ACL としてサポートされるのは IPv4 ACL だけです。
- ステップ 4** [Apply] をクリックして、変更を確定します。
- ステップ 5** [Save Configuration] をクリックして、変更を保存します。
- 

## WLAN へのアクセスコントロールリストの適用

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
- ステップ 3** [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。
- ステップ 4** [Override Interface ACL] ドロップダウンリストから、この WLAN に適用する IPv4 または IPv6 ACL を選択します。選択した ACL は、インターフェイスに設定されたすべての ACL を上書きします。デフォルト値は [None] です。
- (注) ISE や ACS などの AAA サーバを介した中央集中型のアクセス制御をサポートするには、コントローラに IPv6 ACL を設定し、WLAN で AAA Override 機能を有効にする必要があります。
- ステップ 5** [Apply] をクリックします。
- ステップ 6** [Save Configuration] をクリックします。
-



## WLAN への事前認証アクセス コントロール リストの適用

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
- ステップ 3** [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit] ([Security] > [Layer 3]) ページを開きます。
- ステップ 4** [Web Policy] チェックボックスをオンにします。
- ステップ 5** [Preauthentication ACL] ドロップダウン リストから目的の ACL を選択し、[Apply] をクリックします。デフォルト値は [None] です。
- ステップ 6** [Save Configuration] をクリックして、変更を保存します。
- 

## アクセス コントロール リストの設定と適用 (CLI)

### アクセス コントロール リストの設定

- 
- ステップ 1** 次のコマンドを入力して、コントローラ上に設定されているすべての ACL を表示します。  
**show [ipv6] acl summary**
- ステップ 2** 次のコマンドを入力して、特定の ACL の詳細情報を表示します。  
**show [ipv6] acl detailed acl\_name**  
パケットが ACL ルールと一致するたびに、[Counter] テキスト ボックスの値が増加します。[DenyCounter] テキスト ボックスの値は、パケットがいずれのルールとも一致しない場合に増加します。  
(注) 許可ルールによってトラフィック/要求がコントローラから許可されると、反対方向でもトラフィック/要求への応答が許可され、ACL の拒否ルールではブロックできなくなります。
- ステップ 3** 次のコマンドを入力して、コントローラの ACL カウンタを有効または無効にします。  
**config acl counter {start | stop}**  
(注) ACL の現在のカウンタをクリアする場合は、**clear acl counters acl\_name** コマンドを入力します。
- ステップ 4** 次のコマンドを入力して、新しい ACL を追加します。  
**config [ipv6] acl create acl\_name**  
*acl\_name* パラメータには、最大 32 文字の英数字を入力できます。  
(注) スペースが含まれたインターフェイス名を作成しようとする、コントローラ CLI でインターフェイスは作成されません。たとえば、int3 というインターフェイス名を作成しようとする、int と 3 の間にスペースがあるため CLI でこのインターフェイス名は作成されません。int3 をインターフェイス名として使用するには、'int 3' のように単一引用符で囲む必要があります。

ステップ5 次のコマンドを入力して、ACL のルールを追加します。

```
config [ipv6] acl rule add acl_name rule_index
```

ステップ6 **config [ipv6] acl rule** コマンドを入力して、ACL のルールを設定します。

ステップ7 次のコマンドを入力して、設定を保存します。

```
save config
```

(注) ACL を削除するには、**config [ipv6] acl delete acl\_name** コマンドを入力します。ACL ルールを削除するには、**config [ipv6] acl rule delete acl\_name rule\_index** コマンドを入力します。

## アクセスコントロールリストの適用

ステップ1 次のいずれかの操作を行います。

- ACL をデータパスに適用するには、次のコマンドを入力します。

```
config acl apply acl_name
```

- ACL をコントローラの CPU に適用して、CPU に転送されるトラフィックのタイプ (有線、無線、または両方) を制限するには、次のコマンドを入力します。

```
config acl cpu acl_name {wired | wireless | both}
```

(注) コントローラ CPU に適用されている ACL を表示するには、**show acl cpu** コマンドを入力します。コントローラ CPU に適用されている ACL を削除するには、**config acl cpu none** コマンドを入力します。

(注) 2504 および 4400 シリーズの WLC の場合、CAPWAP トラフィックの制御に、CPU ACL は使用できません。ネットワークのアクセスリストを使用して、CAPWAP トラフィックを制御します。

- ACL を WLAN に適用するには、次のコマンドを入力します。

```
config wlan acl wlan_id acl_name
```

(注) WLAN に適用されている ACL を表示するには、**show wlan wlan\_id** コマンドを入力します。WLAN に適用されている ACL を削除するには、**config wlan acl wlan\_id none** コマンドを入力します。

- 事前認証 ACL を WLAN に適用するには、次のコマンドを入力します。

```
config wlan security web-auth acl wlan_id acl_name
```

ステップ2 次のコマンドを入力して、変更を保存します。

```
save config
```

## レイヤ2アクセスコントロールリストの設定

### レイヤ2アクセスコントロールリストの設定について

パケットに関連付けられた EtherType に基づいてレイヤ2アクセスコントロールリスト (ACL) のルールを設定できます。中央スイッチングの WLAN に PPPoE クライアントのみをサポートさせる必要がある場合は、この機能を使用してレイヤ2 ACL ルールを WLAN に適用し、クライアントが認証され他のパケットがドロップされてから PPPoE パケットのみを許可することができます。同様に、WLAN に IPv4 クライアントまたは IPv6 クライアントのみをサポートさせる必要がある場合は、レイヤ2 ACL ルールを WLAN に適用し、クライアントが認証され他のパケットがドロップされてから IPv4 または IPv6 パケットのみを許可することができます。ローカルにスイッチされる WLAN の場合、WLAN または FlexConnect AP のいずれかに同じレイヤ2 ACL を適用できます。AP 固有のレイヤ2 ACL は FlexConnect AP にのみ設定できます。これは、ローカルにスイッチされる WLAN にのみ適用されます。FlexConnect AP に適用されるレイヤ2 ACL は WLAN に適用されるレイヤ2 ACL よりも優先されます。

モビリティのシナリオでは、モビリティアンカー設定が適用できます。

次のトラフィックはブロックされません。

- ワイヤレスクライアントのワイヤレストラフィック
  - 802.1X
  - Inter-Access Point Protocol
  - 802.11
  - Cisco Discovery Protocol
- 分散システムのトラフィック
  - Broadcast
  - マルチキャスト
  - IPv6 ネイバー探索プロトコル (NDP)
  - アドレス解決プロトコル (ARP) および Gratuitous ARP の保護 (GARP)
  - ダイナミックホストコンフィギュレーションプロトコル (DHCP)
  - ドメインネームシステム (DNS)

#### WLAN にマッピングされているレイヤ2 ACL

WLAN にレイヤ2 ACL をマッピングすると、設定したレイヤ2 ACL がその WLAN に関連付けられたすべてのクライアントに適用されます。

レイヤ2 ACL を中央でスイッチされる WLAN にマッピングすると、EtherType に基づいてトラフィックを渡すルールが WLAN に関連付けられたすべてのクライアントに対してファストパス

により決定されます。ファストパスは、パケットに関連付けられたイーサネットヘッダー内を検索し、ACLに対して設定されたものと一致するEtherTypeを持つパケットを転送します。

レイヤ2 ACLをローカルにスイッチされるWLANにマッピングすると、EtherTypeに基づいてトラフィックを渡すルールがWLANに関連付けられたすべてのクライアントに対してAPの転送プレーンにより決定されます。APの転送プレーンは、パケットに関連付けられたイーサネットヘッダー内を検索し、EtherTypeがACLに対する設定と一致するアクションに基づいてパケットを転送または拒否します。

## レイヤ2アクセスコントロールリストの制約事項

- レイヤ2 ACLに対して最大16のルールを作成できます。
- AP固有のレイヤ2 ACLはFlexConnect APにのみ設定できます。これは、ローカルにスイッチされるWLANにのみ適用されます。
- コントローラには、最大で64個のLayer2 ACLを作成できます。
- APは最大16のWLANをサポートするので、APごとに最大16のレイヤ2 ACLがサポートされます。
- APはレイヤ2およびレイヤ3の同じACL名をサポートしないため、レイヤ2 ACL名がFlexConnect ACL名と競合しないことを確認します。

## レイヤ2アクセスコントロールリストの設定 (CLI)

- **config acl layer2 {create | delete} acl-name** : レイヤ2 ACLを作成または削除します。
- **config acl layer2 apply acl-name** : データパスにレイヤ2 ACLを適用します。
- **config acl layer2 rule {add | delete} acl-rule-name index** : レイヤ2 ACLルールを作成または削除します。
- **config acl layer2 rule change index acl-rule-name old-index new-index** : レイヤ2 ACLルールのインデックスを変更します。
- **config acl layer2 rule action acl-rule-name index {permit | deny}** : ルールのアクションを設定します。
- **config acl layer2 rule etherType name index ether-type-number-in-hex ether-type-mask-in-hex** : ルールの宛先IPアドレスおよびネットマスクを設定します。
- **config acl layer2 rule swap index acl-rule-name index-1 index-2** : 2つのルールのインデックス値をスワップします。
- **config acl counter {start | stop}** : ACLカウンタを開始または停止します。このコマンドはすべてのACLのタイプに適用されます。HA環境では、カウンタは、アクティブコントローラとスタンバイコントローラ間では同期されません。
- **show acl layer2 summary** : レイヤ2 ACLプロファイルの要約を表示します。

- **show acl layer2 detailed *acl-name*** : 指定されたレイヤ2 ACL プロファイルの詳細な説明を表示します。
- **show client detail *client-mac-addr*** : クライアントに適用されるレイヤ2 ACL ルールを表示します。

### WLAN とレイヤ2 ACL のマッピング (CLI)

これは、中央でスイッチされる WLAN、および FlexConnect アクセス ポイントがなくローカルにスイッチされる WLAN に適用されます。

- **config wlan layer2 acl *wlan-id acl-name*** : レイヤ2 ACL を中央でスイッチされる WLAN にマッピングします。
- **config wlan layer2 acl *wlan-id none*** : WLAN にマッピングされたレイヤ2 ACL をクリアします。
- **show wlan *wlan-id*** : WLAN にマッピングされたレイヤ2 ACL のステータスを表示します。

### FlexConnect アクセス ポイントを使用したローカルにスイッチされる WLAN とレイヤ2 ACL のマッピング (CLI)

これは、FlexConnect アクセス ポイントを持つローカルにスイッチされる WLAN に適用されます。

- **config ap flexconnect wlan l2acl add *wlan-id ap-name acl-name*** : レイヤ2 ACL をローカルにスイッチされる WLAN にマッピングします。
- **config ap flexconnect wlan l2acl delete *wlan-id ap-name*** : マッピングを削除します。
- **show ap config general *ap-name*** : マッピングの詳細を表示します。

## レイヤ2アクセスコントロールリストの設定 (GUI)

- ステップ 1** [Security] > [Access Control Lists] > [Layer2 ACLs] の順に選択して、[Layer2 Access Control Lists] ページを開きます。
- ステップ 2** [New] をクリックして、新しい ACL を追加します。[Layer2 Access Control Lists > New] ページが表示されます。
- ステップ 3** [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。
- ステップ 4** [Apply] をクリックします。[Layer2 Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。
- ステップ 5** [Layer2 Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。[Layer2 Access Control Lists > Rules > New] ページが表示されます。
- ステップ 6** この ACL のルールを次のように設定します。

- a) コントローラは各 ACL について最大 16 のルールをサポートします。これらのルールは、1 から 16 の順にリストアップされます。[Sequence] テキストボックスで、値 (1 ~ 16) を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

(注) ルール 1 ~ 4 がすでに定義されている場合にルール 15 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

- b) [Ether Type] ドロップダウンリストから、次のイーサネットタイプのいずれかのオプションを選択します。

- AppleTalk Address Resolution Protocol
- VLAN-tagged Frame & Short Path Bridging
- IPX (0x8137)
- IPX (0x8138)
- QNS Qnet
- Internet Protocol Version 6
- Ethernet Flow Control
- Slow Protocol
- CobraNet
- MPLS Unicast
- MPLS Multicast
- PPPoE Discovery Stage
- PPPoE Session Stage
- ジャンボ フレーム
- HomePlug 1.0 MME
- EAP over LAN
- PROFINET over Protocol
- HyperSCSI
- ATA over Ethernet
- EtherCAT Protocol

(注) [Ether Type] ドロップダウン リストから定義済みのイーサネットタイプを選択することもできますし、[Ether Type] ドロップダウン リストのカスタム オプションを使用して独自のイーサネットタイプ値を入力することもできます。

- c) [Action] ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。

- d) [Apply] をクリックして、変更を確定します。 [Layer2 Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。
- e) この ACL にさらにルールを追加するにはこの手順を繰り返します。

**ステップ7** [Save Configuration] をクリックして、変更を保存します。

**ステップ8** さらに ACL を追加するにはこの手順を繰り返します。

---

## WLAN へのレイヤ2アクセスコントロールリストの適用 (GUI)

---

**ステップ1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ2** 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

**ステップ3** [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。

**ステップ4** [Layer2 ACL] ドロップダウンリストから、作成した ACL を選択します。

**ステップ5** [Apply] をクリックします。

**ステップ6** [Save Configuration] をクリックします。

---

## WLAN の AP へのレイヤ2アクセスコントロールリストの適用 (GUI)

---

**ステップ1** [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

**ステップ2** 目的のアクセスポイントの名前をクリックして、[All APs > Details] ページを開きます。

**ステップ3** [All APs > Details] ページで、[FlexConnect] タブをクリックします。

**ステップ4** [PreAuthentication Access Control Lists] 領域で、[Layer2 ACLs] リンクをクリックして [ACL Mappings] ページを開きます。

**ステップ5** [WLAN ACL Mapping] 領域の [Layer2 ACL] ドロップダウンリストから、作成した ACL を選択して [Add] をクリックします。

**ステップ6** [Apply] をクリックします。

**ステップ7** [Save Configuration] をクリックします。

---

## DNS ベースのアクセスコントロールリストの設定

### DNS ベースのアクセスコントロールリストについて

DNS ベースの ACL は、Apple および Android デバイスなどのクライアント デバイスに使用されます。これらのデバイスを使用する場合、デバイスがアクセス権を持つ範囲を特定するために Cisco WLC に事前認証 ACL を設定できます。

Cisco WLC で DNS ベースの ACL を有効にするには、ACL の許可された URL を設定する必要があります。URL は、ACL で事前設定しておく必要があります。

DNS ベースの ACL によって、登録フェーズ中のクライアントは、設定された URL への接続を許可されます。Cisco WLC は ACL 名で設定され、事前認証 ACL が適用されるように AAA サーバによって返されます。ACL 名が AAA サーバによって返されると、ACL は Web リダイレクト用にクライアントに適用されます。

クライアント認証フェーズでは、ISE サーバが事前認証 ACL (`url-redirect acl`) を返します。DNS スヌーピングは、登録が完了してクライアントが SUPPLICANT PROVISIONING 状態になるまで、各クライアントの AP で実行されます。URL で設定された ACL が Cisco WLC で受信されると、CAPWAP ペイロードは AP に送信され、クライアントの DNS スヌーピングが有効になり URL がスヌーピングされます。

適切な URL スヌーピングにより、AP は DNS 応答の解決済みドメイン名の IP アドレスを学習します。ドメイン名が設定された URL に一致すると、DNS 応答が IP アドレスについて解析され、IP アドレスは CAPWAP ペイロードとして Cisco WLC に送信されます。Cisco WLC によって IP アドレスの許可リストに IP アドレスが追加されるため、クライアントは設定された URL にアクセスできます。

### DNS ベースのアクセスコントロールリストの制約事項

- 最大 10 の URL をアクセスコントロールリストに許可できます。
- Cisco WLC では、1 つのクライアントに対して 20 の IP アドレスが許可されています。
- ローカル認証は FlexConnect AP でサポートされていません。
- DNS ベースの ACL は、Cisco 1130 および 1240 シリーズのアクセスポイントでサポートされていません。
- 認証トラフィックは、DNS ベースの ACL が AP に対してローカルであっても、この機能がサポートされるように Cisco WLC を経由する必要があります。

### DNS ベースのアクセスコントロールリストの設定 (CLI)

**ステップ 1** ACL を作成するように指定します。最大 32 文字の英数字で IPv4 ACL の名前を入力できます。



例 :

```
(Cisco Controller) >> config acl create android
config acl create name
```

- ステップ 2** アクセスコントロールリストの新しい URL ドメインを追加するように指定します。URL ドメイン名は有効な形式（たとえば、Cisco.com、bbc.in、または play.google.com）で指定する必要があります。ホスト名比較は、一致するサブストリングです（ワイルドカードベース）。作成済みの ACL 名を使用する必要があります。

例 :

```
(Cisco Controller) >> config acl url-domain add cisco.com android
(Cisco Controller) >> config acl url-domain add play.google.com android
config acl url-domain add domain-name acl-name
```

- ステップ 3** アクセスコントロールリストの既存の URL ドメインを削除するように指定します。

例 :

```
(Cisco Controller) >> config acl url-domain delete cisco.com android
config acl url-domain delete domain-name acl-name
```

- ステップ 4** ACL を適用するように指定します。

例 :

```
(Cisco Controller) >> config acl apply android
config acl apply acl-name
```

- ステップ 5** 次のコマンドを入力して、DNS ベースの ACL 情報を表示します。

例 :

```
(Cisco Controller) >> show acl summary
```

ACL Counter Status	Disabled
-----	-----
IPv4 ACL Name	Applied
-----	-----
android	No
StoreACL	Yes
-----	-----
IPv6 ACL Name	Applied
-----	-----

**show acl summary**

- ステップ 6** 次のコマンドを入力して、DNS ベースの ACL 詳細情報を表示します。

例 :

```
(Cisco Controller) >> show acl detailed android
o rules are configured for this ACL.
DenyCounter : 0
URLs configured in this ACL

*.play.google.com
*.store.google.com
show acl detailed acl-name
```

**ステップ 7** 次のコマンドを入力して、DNS スヌーピング（DNS ベースの ACL）によって学習されたクライアントごとの IP アドレスを表示します。

例：  
(Cisco Controller) >> **show client detail mac-address**  
**show client detail mac-address**

**ステップ 8** DNS ベースの ACL に関連する情報のデバッグを有効にします。

例：  
(Cisco Controller) >> **debug aaa events enable**  
**debug aaa events enable**

---

## DNS ベースのアクセスコントロール リストの設定（GUI）

---

- ステップ 1** [Security] > [Access Control Lists] > [Access Control Lists] を選択して、[Access Control Lists] ページを開きます。
- ステップ 2** パケットがコントローラに設定された ACL のいずれかに一致するかどうかを確認する場合は、[Enable Counters] チェックボックスをオンにして [Apply] をクリックします。それ以外の場合、このチェックボックスはオフ（デフォルト値）のままにしておきます。この機能は、システムのトラブルシューティングを実行する際に役立ちます。
- （注） ACL のカウンタをクリアするには、その ACL の青いドロップダウンの矢印の上にカーソルを置いて、[Clear Counters] を選択します。
- ステップ 3** [New] をクリックして、新しい ACL を追加します。[Access Control Lists > New] ページが表示されます。
- ステップ 4** [Access Control List Name] テキスト ボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。
- ステップ 5** IPv4 として ACL タイプを選択します。
- ステップ 6** [Apply] をクリックします。
- ステップ 7** [Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。ACL に IP ルールはありません。青いドロップダウンの矢印の上にカーソルを置き、ドロップダウン リストから [Add-Remove URL] を選択して [URL List] ページを開きます。
- ステップ 8** ACL の新しい URL ドメインを追加するには、[URL String Name] テキスト ボックスにアクセスコントロール リストの新しい URL ドメインを入力します。URL ドメイン名は有効な形式（たとえば、Cisco.com、bbc.in、または play.google.com）で指定する必要があります。
- ステップ 9** URL ドメインを削除するには、削除する URL 名の下の子の青いドロップダウン矢印の上にカーソルを置いて [Delete] を選択します。
-



# 第 58 章

## 管理フレーム保護の設定

- [管理フレーム保護について](#), 541 ページ
- [管理フレーム保護の制約事項](#), 543 ページ
- [管理フレーム保護の設定 \(GUI\)](#), 544 ページ
- [管理フレーム保護の設定の表示 \(GUI\)](#), 544 ページ
- [管理フレーム保護の設定 \(CLI\)](#), 545 ページ
- [管理フレーム保護の設定の表示 \(CLI\)](#), 545 ページ
- [管理フレーム保護の問題のデバッグ \(CLI\)](#), 545 ページ

### 管理フレーム保護について

Management Frame Protection (MFP; 管理フレーム保護) では、アクセス ポイントとクライアント間で送受信される 802.11 管理メッセージを保護および暗号化することにより、セキュリティが確保されます。MFP は、インフラストラクチャとクライアント サポートの両方を実現します。

- **インフラストラクチャ MFP** : DoS 攻撃を引き起こしたり、ネットワーク上で過剰なアソシエーションやプローブを生じさせたり、不正なアクセスポイントとして介入したり、QoS と無線測定フレームへの攻撃によりネットワークパフォーマンスを低下させたりする敵対者を検出することにより、管理フレームを保護します。インフラストラクチャ MFP は、フィッシングインシデントを検出および報告するための迅速かつ効果的な手段を提供するグローバル設定です。

インフラストラクチャ MFP は特に、アクセスポイントによって送信され (クライアントによって送信されたのではなく)、次にネットワーク内の他のアクセスポイントによって検証される管理フレームに、Message Integrity Check Information Element (MIC IE; メッセージ整合性情報要素) を追加することによって、802.11 セッション管理機能を保護します。インフラストラクチャ MFP はパッシブです。侵入を検知し報告しますが、それを止めることはできません。

- クライアント MFP : 認証されたクライアントをスプーフィング フレームから保護し、無線 LAN に対する多くの一般化した攻撃が効力を発揮することのないようにします。認証解除攻撃などのほとんどの攻撃では、有効なクライアントとの競合により簡単にパフォーマンスを悪化させます。

具体的には、クライアント MFP は、アクセス ポイントと CCXv5 クライアント間で送受信される管理フレームを暗号化します。その結果、スプーフィングされたクラス 3 管理フレーム（つまり、アクセス ポイントと、認証およびアソシエートされたクライアントとの間でやり取りされる管理フレーム）をドロップすることにより、アクセス ポイントとクライアントの両方で予防措置をとることができます。クライアント MFP は、IEEE 802.11i によって定義されたセキュリティ メカニズムを利用し、アソシエーション解除、認証解除、および QoS (WMM) アクションといったタイプのクラス 3 ユニキャスト管理フレームを保護します。クライアント MFP は、最も一般的な種類のサービス拒否攻撃から、クライアントとアクセス ポイント間のセッションを保護します。また、セッションのデータ フレームに使用されているのと同じ暗号化方式を使用することにより、クラス 3 管理フレームを保護します。アクセス ポイントまたはクライアントにより受信されたフレームの暗号化解除に失敗すると、そのフレームはドロップされ、イベントがコントローラに報告されます。

クライアント MFP を使用するには、クライアントは CCXv5 MFP をサポートしており、TKIP または AES-CCMP のいずれかを使用して WPA2 をネゴシエートする必要があります。EAP または PSK は、PMK を取得するために使用されます。CCKM およびコントローラのモビリティ管理は、レイヤ 2 およびレイヤ 3 の高速ローミングのために、アクセス ポイント間でセッション キーを配布するのに使用されます。



- (注) 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（アソシエーション解除、認証解除、またはアクションなど）を送信しません。CCXv5 クライアントおよびアクセス ポイントは、ブロードキャスト クラス 3 管理フレームを破棄する必要があります。

インフラストラクチャ MFP は、クライアント MFP 対応でないクライアントに送信された無効なユニキャスト フレームと、無効なクラス 1 およびクラス 2 管理フレームを引き続き検出および報告するため、クライアント MFP は、インフラストラクチャ MFP を置き換えるのではなく、補足するものであると言えます。インフラストラクチャ MFP は、クライアント MFP によって保護されていない管理フレームにのみ適用されます。

インフラストラクチャ MFP は次の 3 つの主要なコンポーネントで構成されます。

- 管理フレーム保護 : アクセス ポイントは、送信される各管理フレームに MIC IE を追加することによってフレームを保護します。フレームのコピー、変更、再送が試みられた場合、MIC は無効となり、MFP フレームを検出するよう設定された受信アクセス ポイントは不具合を報告します。MFP は、Cisco Aironet Lightweight アクセス ポイントでの使用がサポートされています。

- 管理フレーム検証：インフラストラクチャ MFP では、アクセス ポイントによって、ネットワーク内の他のアクセス ポイントから受信する各管理フレームが検証されます。MIC IE が存在しており（送信側が MFP フレームを送信するよう設定されている場合）、管理フレームの中身に一致していることを確認します。MFP フレームを送信するよう設定されているアクセス ポイントに属する BSSID からの正当な MIC IE が含まれていないフレームを受信した場合、不具合をネットワーク管理システムに報告します。タイムスタンプが適切に機能するように、すべてのコントローラでネットワークタイムプロトコル（NTP）が同期されている必要があります。
- イベント報告：アクセス ポイントで異常が検出されるとコントローラに通知されます。コントローラでは、受信した異常イベントが集計され、その結果が SNMP トラップを使用してネットワーク管理システムに報告されます。



(注) クライアント MFP は、インフラストラクチャ MFP と同じイベント報告メカニズムを使用します。

インフラストラクチャ MFP は、デフォルトで有効化されており、システム全体で無効化できません。以前のソフトウェア リリースからアップグレードする場合、アクセス ポイント許可が有効になっているときは、これら 2 つの機能は相互に排他的であるため、インフラストラクチャ MFP はシステム全体で無効になります。インフラストラクチャ MFP がグローバルに有効化されると、選択した WLAN に対してシグニチャの生成（MIC を送信フレームに追加する）を無効にでき、選択したアクセス ポイントに対して検証を無効にできます。

クライアント MFP は、WPA2 に対して設定された WLAN 上でデフォルトで有効にされています。選択した WLAN 上で無効にすることも、必須にする（その場合、MFP をネゴシエートするクライアントのみがアソシエーションを許可されます）こともできます。

## 管理フレーム保護の制約事項

- Lightweight アクセス ポイントでは、インフラストラクチャ MFP はローカル モードおよび監視モードでサポートされます。アクセス ポイントがコントローラに接続しているときは、FlexConnect モードでサポートされます。クライアント MFP は、ローカル モード、FlexConnect モード、およびブリッジ モードでサポートされます。
- OEAP 600 シリーズのアクセス ポイントでは、MFP はサポートされません。
- クライアント MFP は、TKIP または AES-CCMP で WPA2 を使用する CCXv5 クライアントでの使用のみがサポートされています。
- クライアント MFP が無効にされているか、オプションである場合は、非 CCXv5 クライアントは WLAN にアソシエートできません。
- スタンドアロンモードの FlexConnect アクセス ポイントで生成されるエラー レポートは、コントローラに転送することはできず、ドロップされます。

## 管理フレーム保護の設定 (GUI)

- 
- ステップ 1** [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択して、[AP Authentication Policy] ページを開きます。
- ステップ 2** [Protection Type] ドロップダウンリストから [Management Frame Protection] を選択して、コントローラに対してインフラストラクチャ MFP をグローバルに有効にします。
- ステップ 3** [Apply] をクリックして、変更を確定します。  
 (注) 複数のコントローラがモビリティグループに含まれている場合は、インフラストラクチャ MFP に対して設定されているモビリティグループ内のすべてのコントローラ上で、ネットワークタイムプロトコル (NTP) サーバを設定する必要があります。
- ステップ 4** コントローラに対してインフラストラクチャ MFP をグローバルに有効にしたあと、次の手順を実行して、特定の WLAN にクライアント MFP を設定します。
- [WLANs] を選択します。
  - 目的の WLAN のプロファイル名をクリックします。[WLANs > Edit] ページが表示されます。
  - [Advanced] を選択します。[WLANs > Edit] ([Advanced]) ページが表示されます。
  - [MFP Client Protection] ドロップダウンリストから、[Disabled]、[Optional]、または [Required] を選択します。デフォルト値は [Optional] です。[Required] を選択した場合、MFP がネゴシエートされている場合 (つまり、WPA2 がコントローラ上で設定されており、クライアントが CCXv5 MFP をサポートしていて WPA2 に対して設定されている場合) のみ、クライアントはアソシエーションを許可されます。  
 (注) Cisco OEAP 600 では MFP はサポートされません。[Disabled] または [Optional] を選択してください。
  - [Apply] をクリックして、変更を確定します。
- ステップ 5** [Save Configuration] をクリックして設定を保存します。
- 

## 管理フレーム保護の設定の表示 (GUI)

コントローラの現在のグローバル MFP の設定を表示するには、[Security] > [Wireless Protection Policies] > [Management Frame Protection] の順に選択します。[Management Frame Protection Settings] ページが表示されます。

このページでは、次の MFP 設定が表示されます。

- [Management Frame Protection] フィールドは、インフラストラクチャ MFP がコントローラでグローバルに有効化されているかどうかを示します。
- [Controller Time Source Valid] フィールドは、コントローラの時刻が (時刻を手動で入力することにより) ローカルで設定されているか、外部ソース (NTP サーバなど) を通じて設定されているかを示します。時刻が外部ソースにより設定されている場合、このフィールドの値は「True」です。時刻がローカルで設定されている場合、このフィールドの値は「False」です。

す。時刻ソースは、モビリティグループ内の複数のコントローラのアクセスポイント間の管理フレーム上のタイムスタンプの検証に使用されます。

- [Client Protection] フィールドは、クライアント MFP が個別の WLAN に対して有効化されているかどうかと、オプションまたは必須のいずれであるかを示します。

## 管理フレーム保護の設定 (CLI)

- 次のコマンドを入力して、コントローラに対してインフラストラクチャ MFP をグローバルに有効または無効にします。  
**config wps mfp infrastructure {enable | disable}**
- 次のコマンドを入力して、特定の WLAN でクライアント MFP シグニチャを有効または無効にします。  
**config wlan mfp client {enable | disable} wlan\_id [required ]**

クライアント MFP を有効にしてオプションの **required** パラメータを使用すると、MFP がネゴシエートされている場合のみ、クライアントはアソシエーションを許可されます。

## 管理フレーム保護の設定の表示 (CLI)

- 次のコマンドを入力して、コントローラの現在の MFP の設定を表示します。  
**show wps mfp summary**
- 次のコマンドを入力して、特定の WLAN の現在の MFP の設定を表示します。  
**show wlan wlan\_id**
- 次のコマンドを入力して、特定のクライアントに対してクライアント MFP が有効になっているかどうかを表示します。  
**show client detail client\_mac**
- 次のコマンドを入力して、コントローラの MFP 統計情報を表示します。  
**show wps mfp statistics**



(注) 実際に攻撃が進行中でない限り、このレポートにデータは含まれません。ここに示すさまざまなエラーの種類は、図示のみを目的としています。この表は5分ごとにクリアされ、データはネットワーク管理ステーションに転送されます。

## 管理フレーム保護の問題のデバッグ (CLI)

- MFP に関する問題が発生した場合は、次のコマンドを使用します。  
**debug wps mfp ? {enable | disable}**  
ここで、? は、次のいずれかを示します。

**client** : クライアント MFP メッセージのデバッグについて設定します。

**capwap** : コントローラとアクセス ポイント間の MFP メッセージのデバッグについて設定します。

**detail** : MFP メッセージの詳細なデバッグについて設定します。

**report** : MFP レポートのデバッグについて設定します。

**mm** : MFP モビリティ (コントローラ間) メッセージのデバッグについて設定します。





# 第 59 章

## クライアント除外ポリシーの設定

- [クライアント除外ポリシーの設定 \(GUI\)](#) , 547 ページ
- [クライアント除外ポリシーの設定 \(CLI\)](#) , 548 ページ

### クライアント除外ポリシーの設定 (GUI)

**ステップ 1** [Security] > [Wireless Protection Policies] > [Client Exclusion Policies] を選択して、[Client Exclusion Policies] ページを開きます。

**ステップ 2** 指定された条件について、コントローラがクライアントを除外するように設定するには、次のチェックボックスのいずれかをオンにします。各除外ポリシーのデフォルトは有効です。

- [Excessive 802.11 Association Failures] : クライアントは、802.11 アソシエーションの試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.11 Authentication Failures] : クライアントは、802.11 認証の試行に 5 回連続して失敗すると、6 回目の試行で除外されます。
- [Excessive 802.1X Authentication Failures] : クライアントは、802.1X 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。
- [IP Theft or IP Reuse] : IP アドレスが他のデバイスにすでに割り当てられている場合、クライアントは除外されます。
- [Excessive Web Authentication Failures] : クライアントは、Web 認証の試行に 3 回連続して失敗すると、4 回目の試行で除外されます。

**ステップ 3** [Apply] をクリックします。

**ステップ 4** [Save Configuration] をクリックします。

## クライアント除外ポリシーの設定 (CLI)

**ステップ 1** 次のコマンドを入力して、802.11 アソシエーションを 5 回連続して失敗したあと、6 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

```
config wps client-exclusion 802.11-assoc {enable | disable}
```

**ステップ 2** 次のコマンドを入力して、802.11 認証を 5 回連続して失敗したあと、6 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

```
config wps client-exclusion 802.11-auth {enable | disable}
```

**ステップ 3** 次のコマンドを入力して、802.1X 認証を 3 回連続して失敗したあと、4 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

```
config wps client-exclusion 802.1x-auth {enable | disable}
```

**ステップ 4** 次のコマンドを入力して、IP アドレスが別のデバイスにすでに割り当てられている場合に、コントローラがクライアントを除外する設定を有効または無効にします。

```
config wps client-exclusion ip-theft {enable | disable}
```

**ステップ 5** 次のコマンドを入力して、Web 認証を 3 回連続して失敗したあと、4 回目の試行でコントローラがクライアントを除外する設定を有効または無効にします。

```
config wps client-exclusion web-auth {enable | disable}
```

**ステップ 6** 次のコマンドを入力して、上記のすべての理由でコントローラがクライアントを除外する設定を有効または無効にします。

```
config wps client-exclusion all {enable | disable}
```

**ステップ 7** 次のコマンドを使用して、クライアント除外エントリを追加または削除します。

```
config exclusionlist {add MAC [description] | delete MAC | description MAC [description]}
```

**ステップ 8** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 9** 次のコマンドを入力して、動的に除外されたクライアントのリストを表示します。

```
show exclusionlist
```

以下に類似した情報が表示されます。

```
Dynamically Disabled Clients
```

```

MAC Address Exclusion Reason Time Remaining (in secs)

00:40:96:b4:82:55 802.1X Failure 51
```

**ステップ 10** 次のコマンドを入力して、クライアント除外ポリシー構成の設定を表示します。

```
show wps summary
```

以下に類似した情報が表示されます。

```
Auto-Immune
Auto-Immune..... Disabled
```

## Client Exclusion Policy

```
Excessive 802.11-association failures..... Enabled
Excessive 802.11-authentication failures..... Enabled
Excessive 802.1x-authentication..... Enabled
IP-theft..... Enabled
Excessive Web authentication failure..... Enabled
```

## Signature Policy

```
Signature Processing..... Enabled
```

---





# 第 60 章

## Identity ネットワーキングの設定

- [Identity ネットワーキングについて, 551 ページ](#)
- [Identity ネットワーキングで使用する RADIUS 属性, 552 ページ](#)

### Identity ネットワーキングについて

ほとんどの無線 LAN システムの場合、各 WLAN に静的なポリシーがあり、SSID が設定されているすべてのクライアントに適用されます。これは強力な方式ですが、クライアントに複数の Quality of Service (QoS) およびセキュリティポリシーを適用するには、そのクライアントに複数の SSID を設定する必要があるために、限界がありました。

これに対し、Cisco Wireless LAN ソリューションは Identity ネットワーキングをサポートしており、ネットワークが 1 つの SSID をアドバタイズできると同時に、ユーザプロファイルに基づいて、個々のユーザに異なる QoS またはセキュリティポリシーを適用することができます。Identity ネットワーキングを使用して制御できるポリシーは次のとおりです。

- **ACL** : ACL 属性が RADIUS Access Accept で指定されている場合、システムは認証後に ACL 名をクライアントステーションに適用します。これにより、インターフェイスに当てられているすべての ACL は上書きされます。
- **VLAN** : VLAN Interface-Name または VLAN-Tag が RADIUS Access Accept で指定されている場合、システムはクライアントを特定のインターフェイスに割り当てます。



(注) VLAN 機能は、MAC フィルタリング、802.1X、および WPA のみをサポートします。VLAN 機能では Web 認証または IPSec はサポートされません。

- トンネル属性。



- (注) この項で後述する他の RADIUS 属性 (QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag) のいずれかを返す場合、トンネル属性も返す必要があります。

オペレーティング システムのローカル MAC フィルタ データベースは、インターフェイス名を含むように拡張されました。これにより、クライアントを割り当てるインターフェイスをローカル MAC フィルタで指定できるようになりました。別の RADIUS サーバも使用できますが、その RADIUS サーバは [Security] メニューを使用して定義する必要があります。

## Identity ネットワーキングで使用される RADIUS 属性

### QoS-Level

この項では、Identity ネットワーキングで使用される RADIUS 属性について説明します。

この属性は、スイッチングファブリック内、および無線経由のモバイルクライアントのトラフィックに適用される QoS レベルを示しています。この例は、QoS-Level 属性フォーマットの要約を示しています。テキスト ボックスは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| QoS Level |
+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – 3 オクテット :
  - 3 – Bronze (バックグラウンド)
  - 0 – Silver (ベストエフォート)
  - 1 – Gold (ビデオ)
  - 2 – Platinum (音声)

### ACL-Name

この属性は、クライアントに適用される ACL 名を示します。ACL-Name 属性形式の要約を次に示します。テキストボックスは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| ACL Name... |
+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – クライアントに対して使用する ACL の名前を含む文字列

### Interface Name

この属性は、クライアントが関連付けられる VLAN インターフェイスを示します。Interface-Name 属性形式の要約を次に示します。テキストボックスは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| Type | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont.) | Vendor type | Vendor length |
+-----+-----+-----+-----+-----+-----+-----+
| Interface Name... |
+-----+-----+-----+-----+-----+

```

- Type – 26 (ベンダー固有)
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – クライアントが割り当てられるインターフェイスの名前を含む文字列



(注) この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

## VLAN タグ

この属性は、特定のトンネルセッションのグループ ID を示し、Tunnel-Private-Group-ID 属性とも呼ばれます。

この属性は、トンネルの発信側が、特定の接続からグループを事前に判別できる場合は Access-Request パケットに含めることができ、このトンネルセッションを特定のプライベートグループに属するものとして処理する場合は Access-Accept パケットに含める必要があります。プライベートグループは、トンネルセッションを特定のユーザのグループと関連付けるために使用できます。たとえば、未登録の IP アドレスが特定のインターフェイスを通過するようにするルーティングを容易にするために使用できます。Start と Stop のいずれかの値を持つ Acct-Status-Type 属性を含み、かつトンネルセッションに関連する Accounting-Request パケットには、プライベートグループを含める必要があります。

Tunnel-Private-Group-ID 属性形式の要約を次に示します。テキストボックスは左から右に伝送されます。

```

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| | | | | | |
| Type | Length | Tag | String... | | |
+-----+-----+-----+-----+-----+-----+-----+

```

- Type – 81 (Tunnel-Private-Group-ID 用)
- Length –  $\geq 3$
- Tag : Tag テキストボックスは、長さが 1 オクテットで、同じパケット内で同じトンネルを示す属性をグループ化するために使用されます。Tag テキストボックスの値が 0x00 より大きく、0x1F 以下である場合、その値は (いくつかの選択肢のうち) この属性に関連しているトンネルを示すと解釈されます。Tag テキストボックスが 0x1F より大きい場合、その値は後続の String テキストボックスの最初のバイトであると解釈されます。
- String : これは必須のテキストボックスです。グループはこの String テキストボックスによって表されます。グループ ID の形式に制約はありません。



(注) この項の他の RADIUS 属性 (QoS-Level、ACL-Name、Interface-Name、または VLAN-Tag) のいずれかを返す場合、トンネル属性も返す必要があります。

## トンネル属性

RFC 2868 では、認証と許可に使用される RADIUS トンネル属性が定義されています。RFC2867 では、アカウントingに使用されるトンネル属性が定義されています。IEEE 802.1X Authenticator がトンネリングをサポートしている場合は、認証の結果としてサブリカントに対して強制的なトンネルを設定できます。

これは特に、認証の結果に基づいて IEEE8021Q で定義されている特定の VLAN にポートを配置できるようにする場合に適しています。たとえば、この設定を使用すると、ワイヤレスホストがキャンパスネットワーク内を移動するときに同じ VLAN 上にとどまれるようになります。



RADIUS サーバは、一般的に、Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。ただし IEEE 802.1X Authenticator も、Access-Request 内にトンネル属性を含めることによって、サブリカントに割り当てる VLAN に関するヒントを示すことができます。

VLAN 割り当てのために、次のトンネル属性が使用されます。

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

VLAN ID は、1～4094（両端の値を含む）の 12 ビットの値です。RFC 2868 で定義されているように、IEEE 802.1X で使用される Tunnel-Private-Group-ID は文字列型であるため、VLAN ID の整数値は文字列としてエンコードされます。

トンネル属性が送信される時は、Tag テキストボックスに値が含まれている必要があります。RFC 2868 の第 3.1 項には次のように明記されています。

- Tag テキストボックスは長さが 1 オクテットであり、同じパケット内で同じトンネルを示す属性をグループ化するために使用されます。このテキストボックスの有効な値は、0x01～0x1F（両端の値を含む）です。Tag テキストボックスが使用されない場合、値はゼロ（0x00）でなければなりません。
- Tunnel-Client-Endpoint、Tunnel-Server-Endpoint、Tunnel-Private-Group-ID、Tunnel-Assignment-ID、Tunnel-Client-Auth-ID、または Tunnel-Server-Auth-ID 属性（ただし Tunnel-Type、Tunnel-Medium-Type、Tunnel-Password、Tunnel-Preference は含まない）で使用する場合は、0x1F より大きい Tag テキストボックスは、次のテキストボックスの最初のオクテットであると解釈されます。
- 代替トンネルタイプが指定されていない場合（たとえば、トンネリングはサポートしているが VLAN はサポートしていない IEEE 802.1X Authenticator の場合）、トンネル属性は 1 つのトンネルのみを指定する必要があります。したがって、VLANID を指定することだけが目的の場合、すべてのトンネル属性の Tag テキストボックスをゼロ（0x00）に設定する必要があります。代替トンネルタイプが提供される場合は、0x01～0x1F のタグ値を選択する必要があります。





# 第 61 章

## AAA Override の設定

- [AAA Override](#) について, 557 ページ
- [AAA Override](#) の制約事項, 558 ページ
- [正しい QoS 値を取得するための RADIUS サーバディクショナリ ファイルの更新](#), 558 ページ
- [AAA Override](#) の設定 (GUI) , 560 ページ
- [AAA Override](#) の設定 (CLI) , 560 ページ

### AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

#### IPv6 ACL の AAA オーバーライド

Cisco Identity Services Engine (ISE)、ACS などの一元化された AAA サーバによるアクセス コントロールのサポートのために、AAA Override 属性を使用して、クライアントについて IPv6 ACL をプロビジョニングできます。この機能を使用するには、IPv6 ACL をコントローラで設定し、AAA Override 機能をイネーブルにして WLAN を設定する必要があります。ACL がコントローラで事前に設定されていない場合、クライアントは認証されません。IPv6 ACL の実際の名前付き AAA 属性は、IPv4 ベースの ACL をプロビジョニングするために使用される *Airespace ACL-Name* 属性に似た *Airespace-IPv6-ACL-Name* です。AAA 属性が返すコンテンツは、コントローラで設定された IPv6 ACL の名前に一致する文字列になるはずですが、



(注) リリース 7.5 から、アップストリーム AAA Override のレート制限値はダウンストリーム AAA Override のレート制限値と同じになりました。

## AAA Override の制約事項

- AAA Override のためにクライアントが新しいインターフェイスに移動したあと、そのインターフェイスに ACL を適用しても、クライアントが再認証されるまで ACL は有効になりません。この問題を回避するには、インターフェイス上ですでに設定済みの ACL にすべてのクライアントが接続するように、ACL を適用してから WLAN を有効にします。あるいは、クライアントが再認証されるように、インターフェイスを適用したあとで WLAN を一旦無効にし、再び有効にします。
- AAA サーバから返された ACL がコントローラ上にないか、ACL が間違った名前を設定されている場合、クライアントは認証されません。
- FlexConnect のローカルスイッチングを使用すると、マルチキャストは SSID がマッピングされた VLAN にのみ転送され、上書きされた VLAN には転送されません。
- インターフェイスグループが WLAN にマッピングされ、クライアントがその WLAN に接続した場合、クライアントはラウンドロビン方式で IP アドレスを取得しません。インターフェイスグループによる AAA Override はサポートされています。
- AAA Override を許可する設定の多くは、RADIUS サーバで実行されます。RADIUS サーバでは、コントローラに返すようにする上書きプロパティで、Access Control Server (ACS) を設定する必要があります。
- コントローラでは、GUI または CLI を使用して、Allow AAA Override 設定パラメータを有効にします。このパラメータを有効にすることにより、コントローラで RADIUS サーバから返される属性を受け入れるようになります。次にコントローラはそれらの属性をクライアントに適用します。
- レイヤ 2 認証中に AAA Override を有効にすると、ローカルポリシーは適用されず、Override が優先されます。

## 正しい QoS 値を取得するための RADIUS サーバディクショナリファイルの更新

Steel-Belted RADIUS (SBR)、FreeRadius、または同等の RADIUS サーバを使用している場合、AAA Override 機能を有効化した後、クライアントが正しい QoS 値を取得できないことがあります。ディクショナリファイルの編集を可能にするこれらのサーバについて、正しい QoS 値 (Silver = 0、Gold = 1、Platinum = 2、Bronze = 3) を反映させてファイルを更新する必要があります。RADIUS サーバのディクショナリ ファイルを更新するには、次の手順を実行します。



(注) この問題は、Cisco Secure Access Control Server (ACS) には適用されません。

RADIUS サーバのディクショナリ ファイルを更新するには、次の手順を実行します。

- 1 SBR サービス (または他の RADIUS サービス) を停止します。

- 2 次のテキストを、`ciscowlan.dct` として `Radius_Install_Directory\Service` フォルダに保存します。

```
#####
CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
(See README.DCT for more details on the format of this file)
#####

Dictionary - Cisco WLAN Controllers
#
Start with the standard Radius specification attributes
#
@radius.dct
#
Standard attributes supported by Airespace
#
Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE WLAN-Id Airespace-VSA(1, integer) cr
ATTRIBUTE Aire-QoS-Level Airespace-VSA(2, integer) r
VALUE Aire-QoS-Level Bronze 3
VALUE Aire-QoS-Level Silver 0
VALUE Aire-QoS-Level Gold 1
VALUE Aire-QoS-Level Platinum 2

ATTRIBUTE DSCP Airespace-VSA(3, integer) r
ATTRIBUTE 802.1P-Tag Airespace-VSA(4, integer) r
ATTRIBUTE Interface-Name Airespace-VSA(5, string) r
ATTRIBUTE ACL-Name Airespace-VSA(6, string) r

This should be last.

#####
CiscoWLAN.dct - Cisco WLC dictionary
#####
```

- 3 (同じディレクトリにある) `dictiona.dcm` ファイルを開いて、「`@ciscowlan.dct.`」行を追加します。
- 4 `dictiona.dcm` ファイルを保存して閉じます。
- 5 (同じディレクトリにある) `vendor.ini` ファイルを開いて、次のテキストを追加します。

```
vendor-product = Cisco WLAN Controller
dictionary = ciscowlan
ignore-ports = no
port-number-usage = per-port-type
help-id =
```

- 6 `vendor.ini` ファイルを保存して閉じます。
- 7 SBR サービス (または他の RADIUS サービス) を起動します。
- 8 SBR アドミニストレータ (または他の RADIUS アドミニストレータ) を起動します。
- 9 RADIUS クライアントを追加します (まだ追加されていない場合)。`[Make/Model]` ドロップダウンリストから `[Cisco WLAN Controller]` を選択します。

## AAA Override の設定 (GUI)

---

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
  - ステップ 2 設定する WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。
  - ステップ 3 [Advanced] タブを選択します。
  - ステップ 4 [Allow AAA Override] チェックボックスをオンにして AAA Override を有効にするか、オフにしてこの機能を無効にします。 デフォルト値はディセーブルです。
  - ステップ 5 [Apply] をクリックします。
  - ステップ 6 [Save Configuration] をクリックします。
- 

## AAA Override の設定 (CLI)

- 次のコマンドを入力して、WLAN 上の AAA を介したユーザ ポリシーのオーバーライドを設定します。  
**config wlan aaa-override {enable | disable} wlan-id**  
*wlan-id* には 1 ~ 16 の値を入力します。
- 次のコマンドを入力して、802.1X AAA インタラクションのデバッグを設定します。  
**debug dot1x aaa {enable | disable}**
- 次のコマンドを入力して、AAA QoS オーバーライドのデバッグを設定します。  
**debug ap aaaqos-dump {enable | disable}**



## 第 62 章

# 不正なデバイスの管理

- [不正なデバイスについて](#), 561 ページ
- [不正検出の設定 \(GUI\)](#), 565 ページ
- [不正検出の設定 \(CLI\)](#), 567 ページ

## 不正なデバイスについて

不正なアクセスポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセスポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド (CTS) フレームを送信できるようになります。アクセスポイントになりすまして、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービスプロバイダーは、空間からの不正なアクセスポイントの締め出しに強い関心を持っています。

不正なアクセスポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセスポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセスポイントは、企業のファイアウォールの内側にあるネットワークポートに接続可能であるため、重大なネットワークセキュリティ侵害となることがあります。通常、従業員は不正なアクセスポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセスポイントを使って、ネットワークトラフィックを傍受し、クライアントセッションをハイジャックすることは簡単です。さらに警戒すべきことは、セキュリティで保護されていないアクセスポイントの場所が無線ユーザにより頻繁に公開されるため、企業のセキュリティが侵害される可能性も増大します。

次に、不正なデバイスの管理に関する注意事項を示します。

- 許可とアソシエーションの検出後、ただちに阻止フレームが送信されます。強化された不正阻止アルゴリズムを使用すると、アドホッククライアントをより効果的に阻止することができます。

- 最も多くの不正アクセスポイント数が疑われる高密度な RF 環境では、ローカルおよび FlexConnect モードのアクセスポイントによってチャンネル 157 またはチャンネル 161 で不正なアクセスポイントが検出される可能性は、他のチャンネルの場合に比べて低くなります。この問題を緩和するために、専用の監視モードのアクセスポイントを使用することをお勧めします。
- および FlexConnect モードアクセスポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセスポイントは比較的短時間でオフチャンネル スキャンを実行します（各チャンネル約 50 ミリ秒）。高度な不正検出を実行するには、監視モードのアクセスポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 秒または 60 秒などに短縮して、無線がオフチャンネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセスポイントが各チャンネルに費やす時間は約 50 ミリ秒です。
- 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセスポイントでは不正検出はデフォルトでは無効です。
- クライアントカードの実装により、アドホックの抑制の効果が低下することがあります。
- 不正なアクセスポイントの分類および報告は、不正の状態と、不正なアクセスポイントの状態を自動的に移行できるようにする、ユーザ定義の分類規則に従って行うことができます。
- 各コントローラは、不正アクセスポイントの封じ込めを無線チャンネルごとに 3 台（監視モードアクセスポイントの場合、無線チャンネルごとに 6 台）に制限します。
- Rogue Location Discovery Protocol (RLDP) は、オープン認証に設定されている不正なアクセスポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier (BSSID) を使用する不正なアクセスポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセスポイント）を検出します。
- RLDP は、同じネットワークにある不正なアクセスポイントのみを検出します。ネットワークのアクセスリストによって不正なアクセスポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択 (DFS) チャンネルでは機能しません。ただし RLDP は、管理対象のアクセスポイントが DFS チャンネルの監視モードである場合には機能します。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP が監視モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 不正を手動で阻止すると、不正なエントリは期限切れになった後でも保持されます。
- 不正を自動、ルール、AwIPS などの他の防御方法で阻止すると、不正なエントリは期限切れになると削除されます。



- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[Validate Rogue Clients Against AAA] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。
- 7.4 以前のリリースでは、ルールによってすでに分類された不正は再分類されませんでした。7.5 リリースでは、不正ルールの優先順位に基づいて不正を再分類できるようにこの動作が強化されました。優先順位は、コントローラが受信する不正レポートを使用して決定されません。
- 接続モードの FlexConnect AP（不正検出が有効になっている）は、コントローラから不正阻止のリストを取得します。自動阻止 SSID および自動阻止アドホックがコントローラに設定されている場合、これらの設定は、接続モードのすべての FlexConnect AP に設定され、AP はこれをメモリに保存します。

FlexConnect AP がスタンドアロンモードに移行すると、次の処理が実行されます。

- コントローラによる阻止設定が継続されます。
- FlexConnect AP が、インフラ SSID と同じ SSID（FlexConnect AP が接続されているコントローラに設定された SSID）を持つ不正な AP を検出すると、スタンドアロンモードに移行する前に自動阻止 SSID がコントローラから有効にされていれば、阻止が開始されます。
- FlexConnect AP がアドホック不正を検出すると、接続モード時に自動阻止アドホックがコントローラから有効にされていれば、阻止が開始されます。

スタンドアロンの FlexConnect AP を接続モードに戻すと、次の処理が実行されます。

- すべての阻止はクリアされます。
- コントローラから開始された阻止が引き継ぎます。
- WLAN、LAN、11a 無線および 11bg 無線の不正な AP の MAC アドレスは、不正 BSSID の +/- 1 の差異で設定されているので、不正検出 AP は、5Mhz チャネルの不正な有線 AP の関連付けおよび阻止に失敗します。8.0 リリースでは、MAC アドレスの範囲を広げることで、この動作が強化されました。不正検出 AP は有線 ARP MAC と不正 BSSID を +/- 3 の差異で関連付けます。

### 不正なデバイスの検出

コントローラは、近くにあるすべてのアクセスポイントを継続的に監視し、不正なアクセスポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正なアクセスポイントを検出すると、Rogue Location Discovery Protocol (RLDP) を使用し、不正検出モードのアクセスポイントが接続されて、不正がネットワークに接続されているかどうかを特定しません。

コントローラは、オープン認証および設定された不正デバイスで RLDP を開始します。RLDP が Flexconnect またはローカルモードのアクセスポイントを使用すると、クライアントはその時点で接続を解除されます。RLDP のサイクルが終了すると、クライアントはアクセスポイントに再接

続します。不正なアクセスポイントが検出された時点で（自動設定）、RLDPのプロセスが開始されます。

すべてのアクセスポイント、または監視（リッスン専用）モードに設定されたアクセスポイントでのみRLDPを使用するようにコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセスポイント検出が実現され、不要な干渉を生じさせたり、正規のデータアクセスポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセスポイントでRLDPを使用するようにコントローラを設定した場合、モニタアクセスポイントとローカル（データ）アクセスポイントの両方が近くにあると、コントローラは常にRLDP動作に対してモニタアクセスポイントを選択します。ネットワーク上に不正があるとRLDPが判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行は **config rogue ap rldp retries** コマンドを使用して設定できます。

3種類の方法でコントローラからRLDPを開始またはトリガーできます。

- 1 コントローラのCLIからRLDP開始コマンドを手動で入力します。RLDPを開始するための同等のGUIオプションはサポートされていません。  
**config rogue ap rldp initiate mac-address**
- 2 コントローラのCLIからRLDPをスケジュールします。RLDPをスケジュールするための同等のGUIオプションはサポートされていません。  
**config rogue ap rldp schedule**
- 3 自動RLDP。コントローラのCLIまたはGUIから自動RLDPを設定できますが、次の注意事項を考慮してください。
  - 不正検出のセキュリティレベルが **custom** に設定されている場合にのみ、自動RLDPオプションを設定できます。
  - 自動RLDPおよびRLDPのスケジュールを同時に有効にすることはできません。

不正なアクセスポイントは、自動または手動で **Contained** 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセスポイントを選択し、そのアクセスポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセスポイントだけを使用するようにコントローラを設定できます。阻止動作は次の2つの方法で開始されます。

- コンテナアクセスポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャストアソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

## Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルールベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセスポイントが Friendly 状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正なエントリが削除されると、Malicious (Alert、Threat) または Unclassified (Alert) に分類された不正なアクセスポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

## 不正検出の設定 (GUI)

- ステップ 1** 該当するアクセスポイントで不正検出が有効になっていることを確認します。コントローラに join されたすべてのアクセスポイントに対し、不正の検出がデフォルトで有効にされます (OfficeExtend アクセスポイントを除く)。ただし、[All APs > Details for] ([Advanced]) ページで [Rogue Detection] チェックボックスをオンまたはオフにして、個々のアクセスポイントの不正検出を有効または無効にできます。
- ステップ 2** [Security] > [Wireless Protection Policies] > [Rogue Policies] > [General] を選択します。[Rogue Policies] ページが表示されます。
- ステップ 3** 次のオプションから [Rogue Detection Security Level] を選択します。
- Low : 小規模な導入向けの基本不正検出。
  - High : 中規模な展開向けの自動阻止を備えた基本不正検出。
  - Critical : 機密性の高い展開向けの自動阻止と RLDP を備えた基本不正検出。
  - Custom  
(注) 自動 RLDP の場合、セキュリティレベルを [Custom] モードに設定する必要があります。[Custom] モードの場合でも RLDP のスケジューリングはありません。
- ステップ 4** [Rogue Location Discovery Protocol] ドロップダウンリストから、次のオプションのいずれかを選択します。
- Disable : すべてのアクセスポイントで RLDP を無効にします。これは、デフォルト値です。
  - All APs : すべてのアクセスポイントで RLDP を有効にします。
  - Monitor Mode APs : 監視モードのアクセスポイントでのみ RLDP を有効にします。
- ステップ 5** [Expiration Timeout for Rogue AP and Rogue Client Entries] テキストボックスに、不正なアクセスポイントとクライアントエントリの期限が切れてリストから削除されるまでの秒数を入力します。有効な範囲は 240 ~ 3600 秒で、デフォルト値は 1200 秒です。

(注) 不正なアクセスポイントまたはクライアントのエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

**ステップ 6** AAA サーバまたはローカル データベースを使用して、不正なクライアントが有効なクライアントであるかどうかを検証するには、[Validate Rogue Clients Against AAA] チェックボックスをオンにします。デフォルトでは、チェックボックスはオフになっています。

**ステップ 7** 不正なクライアントの詳細を持っている Cisco Mobility Services Engine (MSE) を使用してクライアントを検証するには、[Validate Rogue Clients Against MSE] チェックボックスをオンにします。MSE は、不正なクライアントが有効で認識されたクライアントであるかどうかに関する情報とともに応答します。コントローラによって、不正なクライアントが脅威として含められるか、脅威と見なされる場合があります。

**ステップ 8** 必要に応じて、[Detect and Report Ad-Hoc Networks] チェックボックスをオンにして、アドホック不正検出および報告を有効にします。デフォルトでは、チェックボックスはオンになっています。

**ステップ 9** [Rogue Detection Report Interval] テキスト ボックスに、AP が不正検出レポートをコントローラに送信する間隔を秒単位で入力します。有効な範囲は 10 ~ 300 秒で、デフォルト値は 10 秒です。

**ステップ 10** [Rogue Detection Minimum RSSI] テキスト ボックスに、AP が不正を検出し、不正エントリがコントローラで作成されるために必要な受信信号強度表示 (RSSI) の最小値を入力します。有効な範囲は -128 ~ 0 dBm で、デフォルト値は 0 dBm です。

(注) この機能は、すべての AP モードに適用できます。RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

**ステップ 11** [Rogue Detection Transient Interval] テキスト ボックスに、不正が AP により最初にスキャンされた後、スキャンされる時間間隔を入力します。連続的に不正がスキャンされた後、更新情報が定期的にコントローラへ送信されます。したがって、非常に短い時間だけアクティブで、その後は活動を停止する一時的な不正が AP によってフィルタリングされます。有効な範囲は 120 ~ 1800 秒で、デフォルト値は 0 秒です。不正検出の一時的間隔は、モニタ モードの AP にのみ適用されます。

この機能には次の利点があります。

- AP からコントローラへの不正レポートが短くなる。
- 一時的不正エントリをコントローラで回避できる。
- 一時的不正への不要なメモリ割り当てを回避できる。

**ステップ 12** [Rogue Client Threshold] テキスト ボックスに、しきい値を入力します。値が 0 の場合、rogue client threshold パラメータは無効になります。

**ステップ 13** [Rogue Containment Automatic Rate Selection] チェックボックスを有効または無効にします。このオプションを使用して、ターゲットの不正に最良のレートを使用するためにレートを最適化できます。AP は不正 RSSI に基づいて最良のレートを選択します。

**ステップ 14** コントローラに自動的に特定の不正デバイスを阻止させる場合は、次のパラメータを有効にします。デフォルトでは、これらのパラメータは無効の状態です。

**注意** Auto Contain パラメータのいずれかを選択して [Apply] をクリックすると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz および 5 GHz の周波数は一般に開放されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

- **Auto Containment Level** : 自動阻止レベルを設定します。デフォルトで、自動阻止レベルは 1 に設定されています。

[Auto] を選択すると、コントローラは有効な阻止を必要とする AP を動的に選択します。

- **Auto Containment only for Monitor mode APs** : 自動阻止用のモニタ モード アクセス ポイントを設定します。
- **Auto Containment on FlexConnect Standalone** : 自動阻止に対して FlexConnect スタンドアロン モードのアクセス ポイントを設定します。

(注) AP が接続 FlexConnect モードのときに設定された場合、auto-containment は続行されます。スタンドアロン AP がコントローラに再アソシエートされると、自動阻止が停止し、以降のアクションは AP が関連付けられているコントローラの設定によって決まります。FlexConnect AP のアドホック SSID および管理対象 SSID で自動阻止を設定することもできます。

- **Rogue on Wire** : 有線ネットワークで検出される不正の自動阻止を設定します。
- **Using Our SSID** : ネットワークの SSID をアドバタイズする不正の自動阻止を設定します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
- **Valid Client on Rogue AP** : 信頼できるクライアントが関連付けられている不正なアクセス ポイントの自動阻止を設定します。このパラメータをオフにしておくと、該当する不正が検出されても警告が生成されるだけです。
- **AdHoc Rogue AP** : コントローラによって検出されたアドホック ネットワークの自動阻止を設定します。このパラメータをオフにしておくと、該当するネットワークが検出されても警告が生成されるだけです。

**ステップ 15** [Apply] をクリックします。

**ステップ 16** [Save Configuration] をクリックします。

## 不正検出の設定 (CLI)

**ステップ 1** 不正検出を目的のアクセス ポイントで有効にしてください。不正検出は、コントローラに関連付けられているすべてのアクセス ポイントに対してデフォルトで有効になっています。次のコマンドを入力して、個々のアクセス ポイントの不正検出を有効または無効にできます。

**config rogue detection {enable | disable} cisco-ap** コマンド。

- (注) 特定のアクセスポイントについて、不正の検出の現在の設定状態を確認するには、**show ap config general Cisco\_AP** コマンドを入力します。
- (注) 家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセスポイントでは不正検出はデフォルトでは無効です。

**ステップ 2** 次のコマンドを入力して、不正検出のセキュリティ レベルを設定します。

**config rogue detection security-level {critical | custom | high | low}**

- **critical** : 機密性の高い展開向けの自動阻止と RLDP を備えた基本不正検出。
- **high** : 中規模な展開向けの自動阻止を備えた基本不正検出。
- **low** : 小規模な導入向けの基本不正検出。

**ステップ 3** 次のコマンドを入力して、RLDP を有効化、無効化、または開始します。

- **config rogue ap rldp enable alarm-only** : すべてのアクセスポイント上で RLDP を有効にします。
- **config rogue ap rldp enable alarm-only monitor\_ap\_only** : 監視モードのアクセスポイント上でのみ RLDP を有効にします。
- **config rogue ap rldp initiate rogue\_mac\_address** : 特定の不正なアクセスポイントに対して RLDP を開始します。
- **config rogue ap rldp disable** : すべてのアクセスポイント上で RLDP を無効にします。
- **config rogue ap rldp retries** : 不正なアクセスポイントごとに試行される RLDP の回数を指定します。指定できる範囲は 1 ~ 5 で、デフォルトは 1 です。

**ステップ 4** 次のコマンドを入力して、不正なアクセスポイントとクライアントエントリの期限が切れてリストから削除されるまでの秒数を指定します。

**config rogue ap timeout seconds**

*seconds* パラメータの有効な範囲は 240 ~ 3600 秒 (両端の値を含む) です。デフォルト値は 1200 秒です。

- (注) 不正なアクセスポイントまたはクライアントエントリがタイムアウトすると、その不正の状態がいずれの分類タイプに対しても Alert または Threat である場合には、コントローラから削除されます。

**ステップ 5** 次のコマンドを入力して、アドホック不正検出および報告を有効または無効にします。

**config rogue adhoc {enable | disable}**

**ステップ 6** 次のコマンドを入力して AAA サーバまたはローカルデータベースを有効または無効にし、不正なクライアントが有効なクライアントかどうかを検証します。

**config rogue client aaa {enable | disable}**

**ステップ 7** 次のコマンドを入力して、不正なクライアントの詳細を持つ MSE の使用を有効または無効にし、クライアントを検証します。

**config rogue client mse {enable | disable}**

**ステップ 8** 次のコマンドを入力して、AP が不正検出レポートをコントローラに送信する間隔を秒単位で入力します。

**config rogue detection monitor-ap report-interval time in sec**

*time in sec* パラメータの有効な範囲は 10 秒～ 300 秒です。デフォルト値は 10 秒です。

(注) この機能は、モニタ モード AP にのみ適用されます。

**ステップ 9** 次のコマンドを入力して、AP が不正を検出し、不正エントリがコントローラで作成されるために必要な最小 RSSI 値を入力します。

**config rogue detection min-rssi rssi in dBm**

*rssi in dBm* パラメータに有効な範囲は -128 dBm ～ 0 dBm です。デフォルト値は 0 dBm です。

(注) この機能は、すべての AP モードに適用できます。RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

**ステップ 10** 次のコマンドを入力して、不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。

**config rogue detection monitor-ap transient-rogue-interval time in sec**

*time in sec* パラメータの有効な範囲は 120 秒～ 1800 秒です。デフォルト値は 0 です

(注) この機能は、モニタ モード AP にのみ適用されます。

一時的な間隔値を使用して、AP が不正をスキャンする間隔を制御できます。AP では、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。

この機能には次の利点があります。

- AP からコントローラへの不正レポートが短くなる。
- 一時的不正エントリをコントローラで回避できる。
- 一時的不正への不要なメモリ割り当てを回避できる。

**ステップ 11** 特定の不正なデバイスをコントローラで自動的に阻止するには、次のコマンドを入力します。

**注意** これらのコマンドのいずれかを入力すると、次のメッセージが表示されます。Using this feature may have legal consequences. Do you want to continue? 産業科学医療 (ISM) 帯域の 2.4 GHz および 5 GHz の周波数は一般に公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

- **config rogue ap rldp enable auto-contain** : 有線ネットワークで検出された不正を自動的に阻止します。
- **config rogue ap ssid auto-contain** : ネットワークの SSID をアドバタイズする不正を自動的に阻止します。  
(注) 該当する不正が検出されたときにコントローラで警告だけが生成されるようにするには、**config rogue ap ssid alarm** コマンドを入力します。
- **config rogue ap valid-client auto-contain** : 信頼できるクライアントのアソシエート先の不正なアクセスポイントを自動的に阻止します。

- (注) 該当する不正が検出されたときにコントローラで警告だけが生成されるようにするには、**config rogue ap valid-client alarm** コマンドを入力します。
- **config rogue adhoc auto-contain** : コントローラによって検出されたアドホック ネットワークを自動的に阻止します。
 

(注) 該当する不正が検出されたときにコントローラで警告だけが生成されるようにするには、**config rogue adhoc alert** コマンドを入力します。
  - **config rogue auto-contain level level monitor\_mode\_ap\_only** : モニタ モードアクセス ポイントに対して自動阻止レベルを設定します。デフォルト値は、1 です レベルに 0 を入力すると、コントローラは有効な阻止に必要な AP の数を動的に選択します。
  - **config rogue containment flexconnect {enable | disable}** : スタンドアロンの FlexConnect アクセス ポイントに対して自動阻止オプションを設定します。
 

(注) AP が接続 FlexConnect モードのときに自動阻止を設定した場合、自動阻止は継続されます。スタンドアロン AP がコントローラに再アソシエートされると、自動阻止が停止して、以降のアクションは AP が関連付けられているコントローラの設定によって決まります。FlexConnect AP のアドホック SSID、および管理対象 SSID で自動阻止を設定することもできます。
  - **config rogue containment auto-rate {enable | disable}** : 不正の阻止の自動レートを設定します。

**ステップ 12** 次のコマンドを入力して、アドホックの不正分類を設定します。

- **config rogue adhoc classify friendly state {internal | external} mac-addr**
- **config rogue adhoc classify malicious state {alert | contain} mac-addr**
- **config rogue adhoc classify unclassified state {alert | contain} mac-addr**

次に、パラメータを簡単に説明します。

- **internal** : 外部アドホック不正を信頼します。
- **external** : アドホック不正の存在を承認します。
- **alert** : アドホック不正が検出された場合に、トラップを生成します。
- **contain** : 不正アドホックの阻止を開始します。

**ステップ 13** 次のコマンドを入力して、RLDP のスケジュールを設定します。

**config rogue ap rldp schedule { add | delete | disable | enable }**

- **add** : 指定した曜日に RLDP をスケジュールできるようにします。RLDP をスケジュールする曜日 (**mon**、**tue**、**wed** など) を入力し、開始時刻と終了時刻を HH:MM:SS 形式で指定する必要があります。例 : **config rogue ap rldp schedule add mon 22:00:00 23:00:00**。
- **delete** : RLDP のスケジュールを削除できるようにします。日数を入力する必要があります。
- **disable** : RLDP のスケジューリングを無効にするように設定します。
- **enable** : RLDP のスケジューリングを有効にするように設定します。



(注) RLDP スケジュールを設定すると、それ以降、つまり設定の保存後にそのスケジュールが実行されるとみなされます。

**ステップ 14** 次のコマンドを入力して、変更を保存します。

**save config**

---





## 第 63 章

# 不正なアクセス ポイントの分類

- [不正なアクセス ポイントの分類について](#), 573 ページ
- [不正なアクセス ポイントの分類の制限](#), 576 ページ
- [不正分類ルールの設定 \(GUI\)](#), 577 ページ
- [不正なデバイスの表示および分類 \(GUI\)](#), 580 ページ
- [不正分類ルールの設定 \(CLI\)](#), 584 ページ
- [不正なデバイスの表示および分類 \(CLI\)](#), 586 ページ

## 不正なアクセス ポイントの分類について

コントローラソフトウェアでは、不正なアクセス ポイントを Friendly、Malicious、Custom または Unclassified に分類して表示するルールを作成できます。カスタム タイプの場合、重大度スコアと分類の名前を指定する必要があります。



(注) 手動分類と、auto-containment または rogue-on-wire の結果行われた分類は、不正ルールをオーバーライドします。不正な AP のクラスおよび/または状態を手動で変更し、不正ルールを AP に適用する場合、それを Unclassified および Alert 状態に変更する必要があります。

デフォルトでは、いずれの分類ルールも有効になっていません。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成し、その条件を設定して、ルールを有効にすると、Unclassified のアクセス ポイントは分類し直されます。ルールを変更するたびに、Alert 状態にあるすべてのアクセス ポイント（Friendly、Malicious、Custom および Unclassified）にそのルールが適用されます。

1 台のコントローラにつき最大 64 の不正分類ルールを設定できます。

また、クライアントカウント状態を除くアドホック不正に、不正ルールを適用できます。

不正アクセス ポイントのデータベース テーブルに格納できる不正クライアントの最大数は 256 です。

RSSI 不正ルール状態によって不正な AP またはアドホック不正が分類される場合、トリガーを生じた RSSI 値がコントローラの GUI/CLI に表示されます。コントローラには、トラップにある分類された RSSI、分類された AP MAC アドレス、およびルール名が含まれます。新しいトラップは、新しい分類が作成されるか、不正ルールによって状態が変更するたびに生成されますが、そのレートは不正な AP またはアドホック不正に対して 30 分ごとに制限されています。ただし、不正ルールによる阻止で状態が変更した場合、トラップは即座に送信されます。デフォルト以外の分類タイプ (Friendly、Malicious、および Custom 分類) に有効な値は、「classified by」、「classified at」、および「classified by rule name」です。未分類のタイプの場合、これらのフィールドは表示されません。



(注) 不正ルールの RSSI 状態の場合、再分類は RSSI の変動が設定された RSSI 値の 2 dBm よりも多い場合にのみ行われます。

コントローラは、管理対象のアクセスポイントの 1 つから不正レポートを受信すると、次のように応答します。

- 1 コントローラは未知 (管理対象外) のアクセスポイントが危険性のない MAC アドレスのリストに含まれているか確認します。そのリストに含まれている場合、コントローラはそのアクセスポイントを Friendly として分類します。
- 2 未知 (管理対象外) のアクセスポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラは、不正状態の分類ルール適用処理を開始します。
- 3 不正なアクセスポイントが Malicious、Alert または Friendly、Internal または External にすでに分類されている場合は、コントローラはそのアクセスポイントを自動的に分類しません。不正なアクセスポイントがそれ以外に分類されており、Alert 状態にある場合に限り、コントローラはそのアクセスポイントを自動的に分類し直します。
- 4 コントローラは、優先度の一番高いルールを適用します。不正なアクセスポイントがルールで指定された条件に一致すると、コントローラはそのアクセスポイントをルールに設定された分類タイプに基づいて分類します。
- 5 不正なアクセスポイントが設定されたルールのいずれにも一致しないと、コントローラはそのアクセスポイントを Unclassified に分類します。
- 6 コントローラは、すべての不正なアクセスポイントに対して上記の手順を繰り返します。
- 7 不正なアクセスポイントが社内ネットワーク上にあると RLDP で判断されると、ルールが設定されていない場合でも、コントローラは不正の状態を Threat とマークし、そのアクセスポイントを自動的に Malicious に分類します。その後、不正なアクセスポイントに対して手動で封じ込め処理を行うことができますが (不正を自動的に封じ込めるよう RLDP が設定されていない限り)、その場合は不正の状態が Contained に変更されます。不正なアクセスポイントがネットワーク上にないと、コントローラによって不正の状態が Alert とマークされ、そのアクセスポイントを手動で封じ込め処理を行うことができますようになります。
- 8 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。

表 16: 分類マッピング

ルールベースの分類タイプ	不正の状態
Friendly	<ul style="list-style-type: none"> <li>• <b>Internal</b> : 未知 (管理対象外) のアクセスポイントがネットワーク内に存在し、WLANのセキュリティに脅威を与えない場合、手動で<b>Friendly</b>、<b>Internal</b>に設定します。たとえば、ラボネットワーク内のアクセスポイントなどです。</li> <li>• <b>External</b> : 未知 (管理対象外) のアクセスポイントがネットワーク外に存在し、WLANのセキュリティに脅威を与えない場合、手動で<b>Friendly</b>、<b>External</b>に設定します。たとえば、近隣のコーヒーショップに属するアクセスポイントなどです。</li> <li>• <b>Alert</b> : 不明なアクセスポイントがネイバーリストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセスポイントは<b>Alert</b>に移動されます。</li> </ul>
Malicious	<ul style="list-style-type: none"> <li>• <b>Alert</b> : 不明なアクセスポイントがネイバーリストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセスポイントは<b>Alert</b>に移動されます。</li> <li>• <b>Contained</b> : 未知 (管理対象外) のアクセスポイントが封じ込められています。</li> </ul>
Custom	<ul style="list-style-type: none"> <li>• <b>Alert</b> : 不明なアクセスポイントがネイバーリストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセスポイントは<b>Alert</b>に移動されます。</li> <li>• <b>Contained</b> : 未知 (管理対象外) のアクセスポイントが封じ込められています。</li> </ul>

ルールベースの分類タイプ	不正の状態
Unclassified	<ul style="list-style-type: none"> <li>• <b>Pending</b> : 最初の検出で、未知（管理対象外）のアクセスポイントは3分間 <b>Pending</b> 状態に置かれます。この間に、管理対象のアクセスポイントでは、未知（管理対象外）のアクセスポイントがネイバーアクセスポイントであるかどうか判定されます。</li> <li>• <b>Alert</b> : 不明なアクセスポイントがネイバーリストまたはユーザが設定した危険性のないMACのリストに記載されていない場合、そのアクセスポイントは <b>Alert</b> に移動されます。</li> <li>• <b>Contained</b> : 未知（管理対象外）のアクセスポイントが封じ込められています。</li> <li>• <b>Contained Pending</b> : 未知（管理対象外）のアクセスポイントが <b>Contained</b> とマークされましたが、リソースを使用できないため対処が遅れています。</li> </ul>

不正なアクセスポイントの分類と状態は、次のように設定されています。

- **Known** から **Friendly**、**Internal**
- **Acknowledged** から **Friendly**、**External**
- **Contained** から **Malicious**、**Contained**

不正の状態が **Contained** の場合、不正なアクセスポイントの分類タイプを変更する前に、そのアクセスポイントが封じ込められないようにする必要があります。不正なアクセスポイントを **Malicious** から **Unclassified** に変更する場合は、そのアクセスポイントを削除して、コントローラで分類し直せるようにする必要があります。

## 不正なアクセスポイントの分類の制限

いくつかの不正なルールがあります。その内容は次のとおりです。

- カスタムタイプの不正の分類は、不正ルールに関連付けられています。このため、不正を手動で **Custom** として分類することはできません。カスタムクラスの変更は不正ルールを使用する場合にのみ行えます。
- 不正分類の変更に対して、ルールによって30分ごとに阻止用のトラップが送信されます。カスタム分類の場合、最初のトラップはカスタム分類よりも前に存在していたため、そのトラップに重大度スコアは含まれません。不正が分類されると、30分後に生成される後続のトラップから重大度スコアが取得されます。
- 不正ルールは、優先順位に従って、コントローラ内の新しい着信不正レポートごとに適用されます。

- 不正がより高い優先度ルールを満たし、分類されると、同じレポートの優先順位リスト内で下位に下がることはありません。
- 以前に分類された不正は、次の制限に従って、新しい不正レポートが作成されるたびに、再分類されます。
  - ルールによって Friendly に分類され、状態が ALERT に設定されている不正は、新しい不正レポートを受け取ると再分類が開始されます。
  - 不正が管理者によって Friendly に手動で分類されると、状態は INTERNAL になり、次に続く不正レポートで再分類されません。
  - 不正が Malicious に分類されると、その状態に関係なく、後続の不正レポートで再分類されません。
- 一部の属性が新しい不正レポートで欠落している場合、複数の不正ルールによって、Friendly から Malicious に不正の状態が遷移する可能性があります。
- どの不正ルールによっても、Malicious から他の分類に不正の状態が遷移することはありません。

## 不正分類ルールの設定 (GUI)

**ステップ 1** [Security] > [Wireless Protection Policies] > [Rogue Policies] > [Rogue Rules] を選択して、[Rogue Rules] ページを開きます。

すでに作成されているすべてのルールが優先順位に従って一覧表示されます。各ルールの名前、タイプ、およびステータスが表示されます。

(注) ルールを削除するには、そのルールの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。

**ステップ 2** 次の手順を実行して、新しいルールを作成します。

- [Add Rule] をクリックします。[Add Rule] セクションがページ上部に表示されます。
- [Rule Name] テキスト ボックスに、新しいルールの名前を入力します。名前にスペースが含まれていないことを確認します。
- [Rule Type] ドロップダウン リストで、次のオプションから選択し、このルールとマッチする不正アクセス ポイントを Friendly または Malicious に分類します。
  - Friendly
  - Malicious
  - Custom
- [Notify] ドロップダウン リストから、ルールがマッチする場合の通知を [All]、[Global]、[Local]、または [None] に設定します。
- [State] ドロップダウン リストから、ルールがマッチする場合の不正な AP の状態を構成します。

- f) [Rule Type] を [Custom] に選択する場合、[Severity Score] と [Classification Name] に入力します。
- g) [Add] をクリックして既存のルールリストにこのルールを追加するか、[Cancel] をクリックしてこの新しいルールを破棄します。

**ステップ 3** 次の手順を実行して、ルールを編集します。

- a) 編集するルールの名前をクリックします。[Rogue Rule > Edit] ページが表示されます。
- b) [Type] ドロップダウンリストで、次のオプションから選択し、このルールとマッチする不正アクセスポイントを分類します。
  - Friendly
  - Malicious
  - Custom
- c) [Notify] ドロップダウンリストから、ルールがマッチする場合の通知を [All]、[Global]、[Local]、または [None] に設定します。
- d) [State] ドロップダウンリストから、ルールがマッチする場合の不正な AP の状態を構成します。
- e) [Match Operation] テキストボックスから、次のいずれかを選択します。
 

[Match All] : このルールが有効な場合、検出された不正なアクセスポイントは、ルールで指定されたすべての条件を満たしている場合にルールと一致し、その不正に対してルールの分類タイプが適用されます。

[Match Any] : このルールが有効な場合、検出された不正なアクセスポイントは、ルールで指定された条件のいずれかを満たす場合にルールと一致し、その不正に対してルールの分類タイプが適用されます。これは、デフォルト値です。
- f) このルールを有効にするには、[Enable Rule] チェックボックスをオンにします。デフォルト値はオフです。
- g) [Rule Type] を [Custom] に選択する場合、[Severity Score] と [Classification Name] に入力します。
- h) [Add Condition] ドロップダウンリストで、不正なアクセスポイントが満たす必要がある次の条件から 1 つまたは複数を選択し、[Add Condition] をクリックします。
  - [SSID] : 不正なアクセスポイントには、特定のユーザ設定 SSID が必要です。このオプションを選択する場合は、[User Configured SSID] テキストボックスに SSID を入力し、[Add SSID] をクリックします。
 

(注) SSID を削除するには、SSID を強調表示して [Remove] をクリックします。
  - [RSSI] : 不正なアクセスポイントには、最小の受信信号強度インジケータ (RSSI) 値が必要です。たとえば、不正なアクセスポイントが設定値より大きい RSSI を持つ場合、そのアクセスポイントは Malicious に分類されます。このオプションを選択する場合は、[Minimum RSSI] テキストボックスに最小 RSSI 値を入力します。有効な値の範囲は -95 ~ -50 dBm (両端の値を含む) で、デフォルト値は 0 dBm です。
  - [Duration] : 不正なアクセスポイントが最小期間検出される必要があります。このオプションを選択する場合は、[Time Duration] テキストボックスに最小検出期間の値を入力します。有効な値の範囲は 0 ~ 3600 秒 (両端の値を含む) で、デフォルト値は 0 秒です。



- [Client Count] : 不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、[Minimum Number of Rogue Clients] テキスト ボックスに、不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ~ 10 (両端の値を含む) で、デフォルト値は 0 です。
- [No Encryption] : 不正なアクセス ポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。不正なアクセス ポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセス ポイントに対してアソシエートを試行します。このオプションに関して、これ以外の設定を行う必要はありません。
  - (注) Cisco Prime Infrastructure では、このオプションを「オープン認証」と呼んでいます。
- [Managed SSID] : 不正なアクセス ポイントの管理対象 SSID (WLAN に設定された SSID) がコントローラで認識される必要があります。このオプションに関して、これ以外の設定を行う必要はありません。
  - (注) SSID および管理対象 SSID の 2 つのリストは相互に排他的であるため、[SSID] および [Managed SSID] の条件を [Match All] 操作で使用することはできません。[Match All] を使用してルールを定義し、これら 2 つの条件を設定した場合は、いずれかの条件が満たされないため、不正なアクセス ポイントが Friendly または Malicious に分類されることはありません。
 

1 つのルールにつき最大 6 つの条件を追加できます。条件を追加すると、[Conditions] セクションにその条件が表示されます。
  - (注) 条件を削除するには、その条件の青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。
- SSID Wildcard : 不正なアクセス ポイントに特定のユーザ設定 SSID のサブストリングが存在する必要があります。コントローラは同じ発生パターンのサブストリングを検索し、SSID のすべてのストリングでサブストリングが見つかった場合、マッチを返します。

i) [Apply] をクリックします。

**ステップ 4** [Save Configuration] をクリックします。

**ステップ 5** 不正分類ルールを適用する順序を変更する場合の手順は、次のとおりです。

- 1 [Back] をクリックして、[Rogue Rules] ページに戻ります。
- 2 [Change Priority] をクリックして、[Rogue Rules > Priority] ページにアクセスします。  
不正ルールが優先順位に従って [Change Rules Priority] テキスト ボックスに表示されます。
- 3 優先順位を変更するルールを強調表示し、[Up] をクリックしてリスト内の順位を上げるか、[Down] をクリックしてリスト内の順位を下げます。
- 4 目的の順位になるまで、ルールを上または下に移動します。
- 5 [Apply] をクリックします。

**ステップ 6** 次の手順を実行して、任意の不正なアクセス ポイントを Friendly に分類し、危険性のない MAC アドレス リストに追加します。

- [Security] > [Wireless Protection Policies] > [Rogue Policies] > [Friendly Rogue] の順に選択して、[Friendly Rogue > Create] ページにアクセスします。
- [MAC Address] テキスト ボックスに、危険性のない不正なアクセス ポイントの MAC アドレスを入力します。
- [Apply] をクリックします。
- [Save Configuration] をクリックします。このアクセス ポイントは、コントローラの、危険性のないアクセス ポイントのリストに追加され、[Friendly Rogue APs] ページに表示されます。

## 不正なデバイスの表示および分類 (GUI)

はじめる前に



注意

不正なデバイスを封じ込めることを選択すると、「There may be legal issues following this containment. Are you sure you want to continue?」という警告メッセージが表示されます。工業、科学、医療用 (ISM) 帯域の 2.4 GHz および 5 GHz の周波数は一般に解放されているので、ライセンスなしで使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

**ステップ 1** [Monitor] > [Rogues] の順に選択します。

**ステップ 2** 次のオプションを選択すると、コントローラで検出された各タイプの不正なアクセス ポイントを表示できます。

- Friendly APs
- Malicious APs
- Unclassified APs
- Custom APs

不正な AP の各ページには、不正アクセス ポイントの MAC アドレスと SSID、チャンネル番号、不正なアクセス ポイントが検出された無線の数、不正アクセス ポイントに接続しているクライアントの数、および不正アクセス ポイントの現在のステータスの情報が含まれます。

(注) データベースから認識済みの不正を削除するには、不正状態を Alert に変更します。不正が存在しなくなれば、不正データが 20 分以内にデータベースから削除されます。

(注) これらのいずれかのページから不正なアクセス ポイントを削除するには、青いドロップダウンの矢印の上にカーソルを置いて、[Remove] をクリックします。複数の不正なアクセス ポイントを削除するには、削除対象の行に該当するチェックボックスをオンにし、[Remove] をクリックします。

(注) それぞれのページで [Move to Alert] ボタンをクリックして、阻止されているまたは阻止された悪意のある未分類の不正 AP を Alert 状態に戻すことができます。

**ステップ 3** 不正なアクセス ポイントの詳細を取得するには、アクセス ポイントの MAC アドレスをクリックします。[Rogue AP Detail] ページが表示されます。

このページには、不正なデバイスの MAC アドレス、不正なデバイスのタイプ (アクセス ポイントなど)、不正なデバイスが有線ネットワーク上にあるかどうか、不正なデバイスが最初および最後に報告された日時、デバイスの現在のステータスといった情報が表示されます。

[Class Type] テキスト ボックスには、この不正なアクセス ポイントの現在の分類が表示されます。

- [Friendly] : ユーザ定義の Friendly ルールと一致した不明なアクセス ポイント、または既知の不正なアクセス ポイント。危険性のないアクセス ポイントは阻止することができません。
- [Malicious] : ユーザ定義の Malicious ルールと一致した不明なアクセス ポイント、またはユーザが Friendly または Unclassified 分類タイプから手動で移動した不明なアクセス ポイント。
  - (注) アクセス ポイントが Malicious に分類されると、その後でそのアクセス ポイントにルールを適用することはできなくなります。また、別の分類タイプに移動することもできません。危険性のあるアクセス ポイントを Unclassified 分類タイプに移動する場合は、そのアクセス ポイントを削除して、コントローラで分類し直せるようにする必要があります。
- [Unclassified] : ユーザ定義の Friendly または Malicious ルールと一致しない不明なアクセス ポイント。Unclassified のアクセス ポイントは阻止することができます。また、このアクセス ポイントは、ユーザ定義のルールに従って自動的に、またはユーザが手動で、Friendly または Malicious 分類タイプに移動できます。
- [Custom] : 不正ルールに関連付けられている、ユーザ定義の分類タイプ。手動で不正を Custom に分類することはできません。カスタム クラスの変更は不正ルールを使用する場合にのみ行えます。

**ステップ 4** このデバイスの分類を変更するには、[Class Type] ドロップダウン リストから別の分類を選択します。

(注) 不正なアクセス ポイントの現在の状態が [Contain] である場合、そのアクセス ポイントは移動できません。

**ステップ 5** [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、この不正なアクセス ポイントに対するコントローラの応答方法を指定します。

- [Internal] : コントローラはこの不正なアクセス ポイントを信頼します。このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [External] : コントローラはこの不正なアクセス ポイントの存在を認識します。このオプションは、[Class Type] が [Friendly] に設定されている場合に使用できます。
- [Contain] : コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。

- [Alert] : コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。このオプションは、[Class Type] が [Malicious] または [Unclassified] に設定されている場合に使用できます。

ページの下部には、この不正なアクセス ポイントが検出されたアクセス ポイントと、不正なアクセス ポイントにアソシエートされたすべてのクライアントの両方に関する情報が提供されます。クライアントの詳細を表示するには、[Edit] をクリックして [Rogue Client Detail] ページを開きます。

**ステップ 6** [Apply] をクリックします。

**ステップ 7** [Save Configuration] をクリックします。

**ステップ 8** コントローラに接続された不正なクライアントを表示するには、[Rogue Clients] を選択します。[Rogue Clients] ページが表示されます。このページには、不正なクライアントの MAC アドレス、不正なクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID、不正なクライアントが検出された無線の数、不正なクライアントが最後に報告された日時、不正なクライアントの現在のステータスといった情報が表示されます。

**ステップ 9** 不正なクライアントの詳細情報を取得するには、そのクライアントの MAC アドレスをクリックします。[Rogue Client Detail] ページが表示されます。このページには、不正なクライアントの MAC アドレス、このクライアントがアソシエートされているアクセス ポイントの MAC アドレス、不正なクライアントの SSID および IP アドレス、不正なクライアントが最初および最後に報告された日時、不正なクライアントの現在のステータスといった情報が表示されます。

**ステップ 10** [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、この不正なクライアントに対するコントローラの応答方法を指定します。

- [Contain] : コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert] : コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。

ページの下部には、この不正なクライアントが検出されたアクセス ポイントに関する情報が提供されません。

**ステップ 11** [Apply] をクリックします。

**ステップ 12** 必要に応じて [Ping] をクリックすると、このクライアントへのコントローラの接続をテストできます。

**ステップ 13** [Save Configuration] をクリックします。

**ステップ 14** コントローラで検出されたアドホック不正を確認するには、[Adhoc Rogues] を選択します。[Adhoc Rogues] ページが表示されます。

このページには、MAC アドレス、BSSID、アドホック不正の SSID、アドホック不正が検出された無線の数、アドホック不正の現在のステータスといった情報が表示されます。

**ステップ 15** アドホック不正の詳細情報を取得するには、その不正の MAC アドレスをクリックします。[Adhoc Rogue Detail] ページが表示されます。

このページには、アドホック不正の MAC アドレスおよび BSSID、不正が最初および最後に報告された日時、不正の現在のステータスといった情報が表示されます。

**ステップ 16** [Update Status] ドロップダウン リストから次のオプションのいずれかを選択して、このアドホック不正に対するコントローラの応答方法を指定します。

- [Contain] : コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。
- [Alert] : コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。
- [Internal] : コントローラはこの不正なアクセス ポイントを信頼します。
- [External] : コントローラはこの不正なアクセス ポイントの存在を認識します。

**ステップ 17** [Maximum number of APs to contain the rogue] ドロップダウン リストから、[1]、[2]、[3]、[4] のオプションのいずれかを選択して、このアドホック不正を阻止するために使用するアクセス ポイントの最大数を指定します。

ページの下部には、このアドホック不正が検出されたアクセス ポイントに関する情報が提供されます。

- 1 : 対象の不正なアクセス ポイントが 1 つのアクセス ポイントで阻止されることを指定します。これは最も低い阻止レベルです。
- 2 : 対象の不正なアクセス ポイントが 2 つのアクセス ポイントで阻止されることを指定します。
- 3 : 対象の不正なアクセス ポイントが 3 つのアクセス ポイントで阻止されることを指定します。
- 4 : 対象の不正なアクセス ポイントが 4 つのアクセス ポイントで阻止されることを指定します。これは最も高い阻止レベルです。

**ステップ 18** [Apply] をクリックします。

**ステップ 19** [Save Configuration] をクリックします。

**ステップ 20** 無視するように設定されている任意のアクセス ポイントを表示するには、[Rogue AP Ignore-List] を選択します。[Rogue AP Ignore-List] ページが表示されます。

このページには、無視するように設定されている任意のアクセス ポイントの MAC アドレスが表示されます。不正無視リストには、ユーザによって手動で Cisco Prime Infrastructure マップに追加された任意の自律アクセス ポイントのリストが含まれています。コントローラでは、これらの自律アクセス ポイントが Prime Infrastructure によって管理されていても、不正と見なされます。不正無視リストを使用すると、コントローラでこれらのアクセス ポイントを無視できます。このリストは次のように更新されます。

- コントローラは、不正レポートを受信すると、不明なアクセス ポイントが不正無視アクセス ポイント リストに存在するかどうかを確認します。
- 不明なアクセス ポイントが不正無視リストに存在する場合、コントローラはこのアクセス ポイントを無視して他の不正なアクセス ポイントの処理を続けます。
- 不明なアクセス ポイントが不正無視リストにない場合、コントローラは Prime Infrastructure にトラップを送信します。Prime Infrastructure によって、このアクセス ポイントがその自律アクセス ポイントで検出されると、Prime Infrastructure はコマンドをコントローラに送信し、このアクセス ポイントを rogue-ignore リストに追加します。このアクセス ポイントは、今後の不正レポートで無視されるようになります。

- ユーザが Prime Infrastructure から自律アクセス ポイントを削除すると、Prime Infrastructure はコマンドをコントローラに送信し、このアクセス ポイントを `rogue-ignore` リストから削除します。

## 不正分類ルールの設定 (CLI)

**ステップ 1** 次のコマンドを入力して、ルールを作成します。

```
config rogue rule add ap priority priority classify {friendly | malicious} rule-name
```

後でこのルールの優先順位を変更し、それに従ってリスト内の他の順番も変更する場合は、**config rogue rule priority *priority* *rule-name*** コマンドを入力します。

後でこのルールの分類を変更する場合は、**config rogue rule classify {friendly | malicious} *rule-name*** コマンドを入力します。

すべての不正分類ルールまたは特定のルールを削除するには、**{config rogue rule delete {all | *rule-name*}** コマンドを入力します。

**ステップ 2** 次のコマンドを入力して、ルールを作成します。

- 次のコマンドを入力して、Friendly 不正のルールを設定します。

```
config rogue rule add ap priority priority classify friendly notify {all | global | local | none} state {alert | internal | external | delete} rule-name
```

- 次のコマンドを入力して、Malicious 不正のルールを設定します。

```
config rogue rule add ap priority priority classify malicious notify {all | global | local | none} state {alert | contain} rule-name
```

- 次のコマンドを入力して、Custom 不正のルールを設定します。

```
config rogue rule add ap priority priority classify custom severity-score classification-name notify {all | global | local | none} state {alert | contain} rule-name
```

後でこのルールの優先順位を変更し、それに従ってリスト内の他の順番も変更する場合は、**config rogue rule priority *priority* *rule-name*** コマンドを入力します。

後でこのルールの分類を変更する場合は、**config rogue rule classify {friendly | malicious | custom *severity-score* *classification-name*} *rule-name*** コマンドを入力します。

すべての不正分類ルールまたは特定のルールを削除するには、**{config rogue rule delete {all | *rule-name*}** コマンドを入力します。

**ステップ 3** 次のコマンドを入力して、ルールに基づき、不正 AP の状態を設定します。

```
config rogue rule state {alert | contain | internal | external} rule-name
```

**ステップ 4** 次のコマンドを入力して、ルール マッチの通知を設定します。

```
config rogue rule notify {all | global | local | none} rule-name
```

**ステップ 5** 次のコマンドを入力して、すべてのルールまたは特定のルールを無効にします。

```
config rogue rule disable {all | rule_name}
```

(注) ルールの属性を変更する前にルールを無効にする必要があります。

**ステップ 6** 次のコマンドを入力して、不正なアクセス ポイントが満たす必要があるルールに条件を追加します。

```
config rogue rule condition ap set condition_type condition_value rule_name
```

利用可能な状態の種類は、次のとおりです。

- **ssid** : 不正なアクセス ポイントには、特定の SSID が必要です。コントローラによって管理されない SSID を追加する必要があります。このオプションを選択する場合は、*condition\_value* パラメータに SSID を入力します。SSID はユーザ設定の SSID リストに追加されます。

(注) ユーザ設定の SSID リストからすべての SSID または特定の SSID を削除するには、**config rogue rule condition ap delete ssid** {all | ssid} rule\_name コマンドを入力します。

- **rssi** : 不正なアクセス ポイントには、最小の RSSI 値が必要です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition\_value* パラメータに最小 RSSI 値を入力します。有効な値の範囲は -95 ~ -50 dBm (両端の値を含む) で、デフォルト値は 0 dBm です。

- **duration** : 不正なアクセス ポイントが最小期間検出される必要があります。このオプションを選択する場合は、*condition\_value* パラメータに最小検出期間の値を入力します。有効な値の範囲は 0 ~ 3600 秒 (両端の値を含む) で、デフォルト値は 0 秒です。

- **client-count** : 不正なアクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、*condition\_value* パラメータに、不正なアクセス ポイントにアソシエートされたクライアントの最小数を入力します。有効な値の範囲は 1 ~ 10 (両端の値を含む) で、デフォルト値は 0 です。

- **managed-ssid** : 不正なアクセス ポイントの SSID がコントローラで認識される必要があります。このオプションには *condition\_value* パラメータは必要ありません。

(注) 1 つのルールにつき最大 6 つの条件を追加できます。ルールからすべての条件または特定の条件を削除するには、**config rogue rule condition ap delete all** condition\_type condition\_value rule\_name コマンドを入力します。

- **wildcard-ssid** : 不正なアクセス ポイントに特定のユーザ設定 SSID のワイルドカードが存在する必要があります。サブストリングが SSID の全文字列内で検出されると、コントローラは同じ発生パターンのワイルドカードを検索して一致を返します。

**ステップ 7** 検出された不正なアクセス ポイントがルールに一致しているとみなされ、そのルールの分類タイプが適用されるためには、ルールで指定されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。

```
config rogue rule match {all | any} rule_name
```

**ステップ 8** 次のコマンドを入力して、すべてのルールまたは特定のルールを有効にします。

```
config rogue rule enable {all | rule_name}
```

(注) 変更を有効にするには、ルールを有効にする必要があります。

**ステップ 9** 次のコマンドを入力して、新しい危険性のないアクセスポイントエントリを危険性のないMACアドレスのリストに追加したり、リストから既存の危険性のないアクセスポイントエントリを削除したりします。

**config rogue ap friendly {add | delete} ap\_mac\_address**

**ステップ 10** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 11** 次のコマンドを入力して、コントローラ上に設定されている不正分類ルールを表示します。

**show rogue rule summary**

**ステップ 12** 次のコマンドを入力して、特定の不正分類ルールの詳細情報を表示します。

**show rogue rule detailed rule\_name**

## 不正なデバイスの表示および分類 (CLI)

- 次のコマンドを入力して、コントローラによって検出されたすべての不正なアクセスポイントのリストを表示します。  
**show rogue ap summary**
- 次のコマンドを入力して、コントローラによって検出された危険性のない不正なアクセスポイントのリストを表示します。  
**show rogue ap friendly summary**
- 次のコマンドを入力して、コントローラによって検出された危険性のある不正なアクセスポイントのリストを表示します。  
**show rogue ap malicious summary**
- 次のコマンドを入力して、コントローラによって検出された未分類の不正なアクセスポイントのリストを表示します。  
**show rogue ap unclassified summary**
- 次のコマンドを入力して、特定の不正なアクセスポイントに関する詳細情報を表示します。  
**show rogue ap detailed ap\_mac\_address**
- 次のコマンドを入力して、特定の 802.11a/n/ac 無線に関する不正レポート（各種チャネル幅で検出された不正なデバイスの数を示す）を表示します。  
**show ap auto-rf 802.11a Cisco\_AP**
- 次のコマンドを入力して、不正なアクセスポイントにアソシエートされているすべての不正なクライアントのリストを表示します。  
**show rogue ap clients ap\_mac\_address**
- 次のコマンドを入力して、コントローラによって検出されたすべての不正なクライアントのリストを表示します。  
**show rogue client summary**



- 次のコマンドを入力して、特定の不正なクライアントに関する詳細情報を表示します。  
**show rogue client detailed *client\_mac\_address***
- 次のコマンドを入力して、コントローラによって検出されたすべてのアドホック不正のリストを表示します。  
**show rogue adhoc summary**
- 次のコマンドを入力して、特定のアドホック不正に関する詳細情報を表示します。  
**show rogue adhoc detailed *rogue\_mac\_address***
- 次のコマンドを入力して、分類に基づいてアドホック不正の要約を表示します。  
**show rogue adhoc {friendly | malicious | unclassified} summary**
- 次のコマンドを入力して、無視するように設定されている不正なアクセスポイントのリストを表示します。  
**show rogue ignore-list**



(注) 不正無視アクセスポイントリストの詳細については、「不正なデバイスの表示および分類 (GUI)」を参照してください。

- 次のコマンドを入力して、不正なアクセスポイントを Friendly に分類します。  
**config rogue ap classify friendly state {internal | external} *ap\_mac\_address***  
値は次のとおりです。  
**internal** は、コントローラがこの不正なアクセスポイントを信頼することを表しています。  
**external** は、コントローラがこの不正なアクセスポイントの存在を認識することを表しています。



(注) 不正なアクセスポイントの現在の状態が Contain である場合、そのアクセスポイントを Friendly クラスに移動することはできません。

- 次のコマンドを入力して、不正なアクセスポイントに Malicious のマークを付けます。  
**config rogue ap classify malicious state {alert | contain} *ap\_mac\_address***  
値は次のとおりです。  
**alert** は、コントローラからシステム管理者に、更なる処理を行うよう即時に警告が転送されることを表しています。  
**contain** は、コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになることを表しています。



(注) 不正なアクセスポイントの現在の状態が Contain である場合、そのアクセスポイントを Malicious クラスに移動することはできません。

- 次のコマンドを入力して、不正なアクセス ポイントに **Unclassified** のマークを付けます。  
**config rogue ap classify unclassified state {alert | contain} ap\_mac\_address**



(注) 現在の状態が **Contain** の場合、不正なアクセス ポイントは **Unclassified** クラスに移動できません。

**alert** は、コントローラからシステム管理者に、更なる処理を行うよう即時に警告が転送されることを表しています。

**contain** は、コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになることを表しています。

- 次のコマンドを入力して、アドホック不正の阻止に使用するアクセスポイントの最大数を選択します。

**config rogue ap classify unclassified state contain rogue\_ap\_mac\_address 1, 2, 3, or 4**

- 1 : 対象の不正なアクセス ポイントが1つのアクセスポイントで阻止されることを指定します。これは最も低い阻止レベルです。
- 2 : 対象の不正なアクセス ポイントが2つのアクセスポイントで阻止されることを指定します。
- 3 : 対象の不正なアクセス ポイントが3つのアクセスポイントで阻止されることを指定します。
- 4 : 対象の不正なアクセス ポイントが4つのアクセスポイントで阻止されることを指定します。これは最も高い阻止レベルです。

- 次のコマンドのいずれかを入力して、不正なクライアントに対するコントローラの応答方法を指定します。

**config rogue client alert client\_mac\_address** : コントローラからシステム管理者に対し、さらなる処理を行うよう即時に警告が転送されます。

**config rogue client contain client\_mac\_address** : コントローラによって危険性のあるデバイスが阻止されます。これにより、そのデバイスの信号は、認証されたクライアントに干渉しなくなります。

- 次のコマンドのいずれかを入力して、アドホック不正に対するコントローラの応答方法を指定します。

**config rogue adhoc alert rogue\_mac\_address** : コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。

**config rogue adhoc contain rogue\_mac\_address** : コントローラによって危険性のあるデバイスが阻止されます。これにより、そのデバイスの信号は、認証されたクライアントに干渉しなくなります。

**config rogue adhoc external rogue\_mac\_address** : コントローラによって、このアドホック不正の存在が認識されます。

- これらのコマンドのいずれかを入力して、アドホック不正の分類を設定します。

- [Friendly] 状態 : **config rogue adhoc classify friendly state {internal | external} mac-addr**
  - [Malicious] 状態 : **config rogue adhoc classify malicious state {alert | contain} mac-addr**
  - [Unclassified] 状態 : **config rogue adhoc classify unclassified state {alert | contain} mac-addr**
- 次のコマンドを入力して、カスタム不正 AP 情報の要約を表示します。  
**show rogue ap custom summary**
  - 次のコマンドを入力して、カスタム アドホック不正情報を表示します。  
**show rogue adhoc custom summary**
  - 次のコマンドを入力して、不正な AP を削除します。  
**config rogue ap delete {class | all | mac-addr}**
  - 次のコマンドを入力して、不正なクライアントを削除します。  
**config rogue client delete {state | all | mac-addr}**
  - 次のコマンドを入力して、アドホック不正を削除します。  
**config rogue adhoc delete {class | all | mac-addr}**
  - 次のコマンドを入力して、変更を保存します。  
**save config**





# 第 64 章

## Cisco TrustSec SXP の設定

- [Cisco TrustSec SXP について](#), 591 ページ
- [Cisco TrustSec SXP の制約事項](#), 593 ページ
- [Cisco TrustSec SXP の設定 \(GUI\)](#), 593 ページ
- [新規 SXP 接続の作成 \(GUI\)](#), 594 ページ
- [Cisco TrustSec SXP の設定 \(CLI\)](#), 594 ページ

### Cisco TrustSec SXP について

Cisco TrustSec を使用すると、組織はアイデンティティベースのアクセスコントロールを通じて、人、場所、時を問わずネットワークとサービスをセキュリティで保護できます。このソリューションでは、データの整合性および機密保持サービス、ポリシーベースの管理、中央集中型のモニタリング、トラブルシューティング、およびレポートサービスも提供されます。TrustSec をカスタマイズされたプロフェッショナルサービスと組み合わせると、ソリューションの導入と管理を簡素化できます。CTS は、Cisco ボードレス ネットワークの基盤となるセキュリティ コンポーネントです。

Cisco TrustSec のセキュリティアーキテクチャは、信頼できるネットワーク デバイスのドメインを確立することによってセキュアネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。Cisco TrustSec は、ネットワークに入るようにセキュリティグループ (SG) がパケットを分類するために認証中に取得したデバイスおよびユーザークレデンシャルを使用します。このパケット分類は、Cisco TrustSec ネットワークへの進入時にパケットにタグを付けることで維持されます。これにより、パケットはデータパス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグはセキュリティグループタグ (SGT) と呼ばれ、エンドポイントデバイスはこの SGT に基づいてトラフィックをフィルタリングできるので、ネットワークへのアクセス コントロール ポリシーの適用が可能になります。

Cisco TrustSec アーキテクチャのコンポーネントの1つが、セキュリティグループベースのアクセスコントロールです。セキュリティグループベースのアクセスコントロールコンポーネント

で、Cisco TrustSec ドメインのアクセス ポリシーは、トポロジとは無関係で、ネットワーク アドレスではなく送信元デバイスおよび宛先デバイスのロール（セキュリティグループ番号で指定）に基づいています。個々のパケットには、送信元のセキュリティグループ番号のタグが付けられます。

シスコ デバイスは SGT 交換プロトコル（SXP）を使用して、Cisco TrustSec 向けのハードウェア サポートがないネットワーク デバイスに SGT を伝播します。SXP は、すべてのスイッチで CTS ハードウェアがアップグレードされるのを防ぐためのソフトウェア ソリューションです。WLC では、TrustSec アーキテクチャの一部として SXP がサポートされます。SXP は、CTS 対応のスイッチに SGT 情報を送信します。SGT で示されたロール情報に従って、適切なロールベース アクセス コントロール リスト（RBACL）をアクティブにすることができます。デフォルトでは、コントローラは常にスピーカー モードで動作します。ネットワーク上で SXP を実装するには、出口のディストリビューションスイッチのみを CTS 対応にすればよく、他のすべてのスイッチは CTS 非対応でかまいません。

SXP は、任意のアクセス レイヤとディストリビューションスイッチ間、または2つのディストリビューション スイッチ間で動作します。SXP は TCP をトランスポート層として使用します。アクセス レイヤスイッチ上でネットワークに join している任意のホスト（クライアント）に対する CTS-enabled 認証は、CTS 対応ハードウェアを備えたアクセス スイッチの場合と同様に実行されます。アクセス レイヤスイッチは CTS 対応ハードウェアではありません。したがって、データトラフィックがアクセス レイヤスイッチを通過するとき、そのトラフィックの暗号化または暗号による認証は行われません。SXP は、認証されたデバイス（つまりワイヤレスクライアント）の IP アドレスと、対応する SGT をディストリビューション スイッチに渡すために使用されます。ディストリビューションスイッチが CTS 対応ハードウェアの場合は、そのディストリビューション スイッチがアクセス レイヤ スイッチに代わってパケットに SGT を挿入します。ディストリビューション スイッチが CTS 対応ハードウェアでない場合は、ディストリビューション スイッチの SXP が、CTS ハードウェアを備えたすべてのディストリビューション スイッチに IP-SGT マッピングを渡します。出口側では、ディストリビューション スイッチの出力 L3 インターフェイスで RBACL が適用されます。

次に、Cisco TrustSec SXP に関する注意事項を示します。

- SXP は次のセキュリティ ポリシーでのみサポートされます。
  - WPA2-dot1x
  - WPA-dot1x
  - 802.1x (Dynamic WEP)
  - RADIUS サーバを使用した MAC フィルタリング
  - RADIUS サーバを使用した Web 認証によるユーザ認証
- SXP は IPv4 クライアントと IPv6 クライアントの両方でサポートされます。
- コントローラは常にスピーカー モードで動作します。

Cisco TrustSec の詳細については、<http://www.cisco.com/en/US/netsol/ns1051/index.html> を参照してください。

## Cisco TrustSec SXP の制約事項

- SXP は FlexConnect アクセス ポイントではサポートされません。
- SXP がサポートされるのは、中央認証を使用し、中央でスイッチされるネットワークだけです。
- デフォルトでは、SXP はローカル モードのみで動作する AP 向けにサポートされています。
- デフォルトパスワードの設定は、コントローラとスイッチの両方で一致している必要があります。
- 耐障害性は AP でのローカル スイッチングが必要になるため、この機能はサポートされません。
- ユーザをローカル認証するための静的 IP-SGT マッピングはサポートされません。
- IP-SGT マッピングでは、外部 ACS サーバを使用した認証が必要です。
- 自動アンカー モビリティ モードのコントローラはモビリティ メッセージを介してクライアント IP-SGT 情報を更新しません。両方のコントローラの接続スイッチ間には、IP-SGT マッピングを更新するために、SXP 接続が確立されている必要があります。

## Cisco TrustSec SXP の設定 (GUI)

**ステップ 1** [Security] > [TrustSec SXP] の順に選択して、[SXP Configuration] ページを開きます。このページでは、次の SXP 設定の詳細が表示されます。

- [Total SXP Connections] : 設定されている SXP 接続の数。
- [SXP State] : SXP 接続のステータス (有効または無効)。
- [SXP Mode] : コントローラの SXP モード。 SXP 接続では、コントローラは常にスピーカー モードに設定されています。
- [Default Password] : SXP メッセージの MD5 認証用パスワード。パスワードには 6 文字以上を含めることをお勧めします。
- [Default Source IP] : 管理インターフェイスの IP アドレス。 SXP は、すべての新規 TCP 接続に対してデフォルトの送信元 IP アドレスを使用します。
- [Retry Period] : SXP 再試行タイマー。デフォルト値は 120 秒 (2 分) です。有効な範囲は 0 ~ 64000 秒です。SXP 再試行期間によって、コントローラが SXP 接続を再試行する間隔が決まります。SXP 接続が正常に確立されなかった場合、コントローラは SXP 再試行期間タイマーの終了後に、新しい接続の確立を試行します。SXP 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

このページでは、SXP 接続について次の情報も表示されます。

- [Peer IP Address] : ピアの IP アドレス、つまりコントローラが接続するネクスト ホップ スイッチの IP アドレス。新しいピア接続を設定しても、既存の TCP 接続に影響はありません。
- [Source IP Address] : 送信元の IP アドレス、つまりコントローラの管理 IP アドレス。
- [Connection Status] : SXP 接続のステータス。

ステップ 2 [SXP State] ドロップダウン リストで、[Enabled] を選択して Cisco TrustSec SXP を有効にします。

ステップ 3 SXP 接続に使用するデフォルト パスワードを入力します。パスワードには 6 文字以上を含めることをお勧めします。

ステップ 4 [Retry Period] ボックスに、Cisco TrustSec ソフトウェアが SXP 接続を再試行する間隔を秒単位で入力します。

ステップ 5 [Apply] をクリックします。

## 新規 SXP 接続の作成 (GUI)

ステップ 1 [SECURITY] > [TrustSec SXP] の順に選択し、[New] をクリックして [SXP Connection > New] ページを開きます。

ステップ 2 [Peer IP Address] テキスト ボックスに、コントローラが接続するネクスト ホップ スイッチの IP アドレスを入力します。

ステップ 3 [Apply] をクリックします。

## Cisco TrustSec SXP の設定 (CLI)

- 次のコマンドを入力して、コントローラ上で SXP を有効または無効にします。  
**config cts sxp {enable | disable}**
- 次のコマンドを入力して、SXP メッセージの MD5 認証のデフォルト パスワードを設定します。  
**config cts sxp default password password**
- 次のコマンドを入力して、コントローラが接続するネクスト ホップ スイッチの IP アドレスを設定します。  
**config cts sxp connection peer ip-address**
- 次のコマンドを入力して、接続を試みる間隔を設定します。  
**config cts sxp retry period time-in-seconds**



- 次のコマンドを入力して、SXP 接続を削除します。

```
config cts sxp connection delete ip-address
```

- 次のコマンドを入力して、SXP の設定の概要を確認します。

```
show cts sxp summary
```

以下に類似した情報が表示されます。

```
SXP State..... Enable
SXP Mode..... Speaker
Default Password..... ****
Default Source IP..... 209.165.200.224
Connection retry open period 120
```

- 次のコマンドを入力して、設定された SXP 接続のリストを参照します。

```
show cts sxp connections
```

以下に類似した情報が表示されます。

```
Total num of SXP Connections..... 1
SXP State..... Enable
Peer IP Source IP Connection Status

209.165.200.229 209.165.200.224 On
```

- 次の手順のいずれかに従って、コントローラと Cisco Nexus 7000 シリーズ スイッチ間に接続を確立します。

- 次のコマンドを入力します。

- 1 config cts sxp version sxp version 1 または 2 /**

- 2 config cts sxp disable**

- 3 config cts sxp enable**

- コントローラで SXP バージョン 2 が使用され、Cisco Nexus 7000 シリーズ スイッチでバージョン 1 が使用されている場合、接続を確立するために再試行間隔を設定する必要があります。始めは短い試行間隔を設定することを推奨します。デフォルトは 120 秒です。





# 第 65 章

## ローカル ポリシーの設定

---

- [ローカル ポリシーについて](#), 597 ページ
- [ローカル ポリシー分類の制約事項](#), 598 ページ
- [ローカル ポリシーの設定 \(GUI\)](#), 600 ページ
- [ローカル ポリシーの設定 \(CLI\)](#), 601 ページ

### ローカル ポリシーについて

コントローラは、HTTP、DHCPなどのプロトコルに基づいてデバイスのプロファイリングを実行して、クライアントを識別できます。デバイスベースのポリシーを設定し、ネットワークにユーザごとまたはデバイスごとのポリシーを適用できます。コントローラは、ユーザごとまたはデバイスごとのエンドポイント、およびデバイスごとに適用できるポリシーに基づく統計情報を表示します。設定できるポリシーの最大数は64です。

ポリシーは、次の属性に基づいて定義されます。

- ユーザ グループまたはユーザ ロール
- Windows クライアント、スマートフォン、タブレットなどのデバイス タイプ
- SSID (Service Set Identifier)
- エンドポイントが接続されているアクセス ポイント グループに基づく場所
- 時刻
- クライアントが接続されているEAP方式をチェックするための拡張認証プロトコル (EAP) タイプ。

これらのポリシー属性が一致する場合は、次のアクションを定義できます。

- 仮想ローカルエリア ネットワーク (VLAN)
- アクセス コントロール リスト (ACL)

- Quality of Service (QoS) レベル
- セッションタイムアウト値
- スリープ状態にあるクライアントのタイムアウト値
- AAA サーバに定義されたローカル ポリシー属性に基づいて、AVC プロファイル、ロール、またはその両方を選択します。

次に、AAA サーバに定義された AVC プロファイルとロールの組み合わせに基づいて適用されるローカル ポリシーによる別の方法を示します。

- AVC プロファイルとロールの両方が AAA サーバから取得される場合、次のオプションを使用できます。
  - AAA Override が有効である場合、AVC プロファイルは優先順位付けされて適用されます。
  - AAA Override が無効である場合、ロール マッチングが適用されます。
- ロールのみを AAA サーバから取得してロール マッチングを行う場合、次のオプションを使用できます。
  - プロファイルがポリシー内で定義されている場合、ロール ポリシーが適用されません。
  - プロファイルがポリシーで定義されていない場合、WLAN で定義された AVC プロファイルが適用されます。
- AVC プロファイルのみを AAA サーバから取得する場合、次のオプションを使用できます。
  - AAA Override が有効である場合、AAA サーバから受け取った AVC プロファイルが適用されます。
  - AAA Override が無効である場合、WLAN で定義された AVC プロファイルが適用されます。

## ローカル ポリシー分類の制約事項

- AAA Override が有効で、AAA 属性が AAA サーバのロール タイプ以外である場合、設定されたポリシーのアクションは適用されません。AAA Override 属性が優先されます。
- WLAN では、ローカル プロファイルが有効になっている場合、RADIUS プロファイルは許可されません。
- クライアント プロファイルではコントローラの既存のプロファイルが使用されます。
- カスタム プロファイルを作成することはできません。

- ワークグループブリッジ (WGB) の背後の有線クライアントはプロファイルされず、ポリシーアクションは実行されません。
- ポリシープロファイルと一致する最初のポリシールールのみが優先されます。各ポリシープロファイルには、ポリシーとの一致に使用されるポリシールールが関連付けられています。
- 最大 64 のポリシーを設定することができ、これらのポリシーを WLAN ごとに最大 16 設定できます。
- レイヤ 2 認証またはレイヤ 3 認証の完了後、またはデバイスが HTTP トラフィックを送信して、デバイスがプロファイルされた場合、ポリシーアクションが実行されます。したがって、プロファイルおよびポリシーアクションはクライアントごとに複数回実行されます。
- VLAN、ACL、Session Timeout および QoS のみがポリシーアクション属性としてサポートされます。
- プロファイルは、IPv4 クライアントでのみ行われます。
- モビリティグループのすべてのコントローラについて、ローカルポリシー設定に同じ一致基準属性とアクション属性が必要です。これ以外の場合、コントローラ間でローミングが発生すると、ローカルポリシー設定は無効になります。

表 17: Cisco Identity Services Engine (ISE) とコントローラでのプロファイルサポートの違い

ISE	コントローラ
RADIUS プロープ、DHCP プロープ、HTTP およびクライアントタイプの識別に使用するその他のプロトコルを使用したプロファイルをサポートします。	MAC OUI、DHCP、および HTTP ベースのプロファイルをサポートします。
ポリシーアクションの複数の異なる属性をサポートし、各属性を選択するためのインターフェイスがあります。	ポリシーアクション属性として VLAN、ACL、Session-Timeout および QoS をサポートします。
ユーザ定義属性によるプロファイルルールのカスタマイズをサポートします。	デフォルトのプロファイルルールのみをサポートします。

## ローカルポリシーの設定 (GUI)

- ステップ1 [Security] > [Local Policies] を選択します。
- ステップ2 新しいポリシーを作成するには、[New] をクリックします。
- ステップ3 ポリシー名を入力し、[Apply] をクリックします。
- ステップ4 [Policy List] ページで、設定するポリシー名をクリックします。
- ステップ5 [Policy > Edit] ページで、次の手順を実行します。
- [Match Criteria] 領域で、[Match Role String] の値を入力します。これはユーザーのユーザタイプまたはユーザグループです（たとえば、学生、教員など）。
  - [Match EAP Type] ドロップダウンリストから、クライアントが使用する EAP 認証方式を選択します。
  - [Device Type] ドロップダウンリストから、デバイスタイプを選択します。
  - ポリシーのデバイスリストにデバイスタイプを追加するには、[Add] をクリックします。選択したデバイスタイプは、[Device List] に表示されます。
  - [Action] 領域で、適用させるポリシーを指定します。[IPv4 ACL] ドロップダウンリストから、ポリシーの IPv4 ACL を選択します。
  - ポリシーに関連付ける必要がある VLAN ID を入力します。
  - [QoS Policy] ドロップダウンリストから、適用する QoS ポリシーを選択します。
  - [Session Timeout] の値を入力します。これは、クライアントに再認証を強制するまでの最大時間（秒単位）です。
  - [Sleeping Client Timeout] の値を入力します。これはスリープ状態にあるクライアントのタイムアウトです。スリープ状態にあるクライアントとは、Web 認証に成功したゲストアクセスを持つクライアントであり、スリープおよび再起動のためにログインページからの別の認証プロセスを必要としません。この設定は、WLAN 固有のスリープ状態のクライアントタイムアウト設定に優先します。
  - [AVC Profile] ドロップダウンリストから、AAA に定義されたルールに基づいて適用される AVC プロファイルを選択します。
  - [Active Hours] 領域の [Day] ドロップダウンリストから、ポリシーをアクティブにする曜日を選択します。
  - ポリシーの開始時間と終了時間を入力します。
  - [Add] をクリックします。指定した曜日および開始時刻と終了時刻が表示されます。
  - [Apply] をクリックします。

### 次の作業

次の手順に従って、作成したローカルポリシーを WLAN に適用します。

- 1 [WLANs] を選択します。

- 2 対応する WLAN ID をクリックします。  
[WLANs > Edit] ページが表示されます。
- 3 [Policy-Mapping] タブをクリックします。
- 4 ポリシーのプライオリティ インデックスを入力します。
- 5 [Local Policy] ドロップダウン リストから、WLAN に適用させるポリシーを選択します。
- 6 [Add] をクリックします。  
選択したプライオリティ インデックスおよびポリシーが表示されます。 WLAN に対して最大 16 のポリシーを適用できます。

## ローカルポリシーの設定 (CLI)

- 次のコマンドを入力して、ローカル ポリシーを作成または削除します。  
**config policy *policy-name* {create | delete}**
- 次のコマンドを入力して、ポリシーに一致タイプを設定します。
  - **config policy *policy-name* match device-type {add | delete} *device-type***
  - **config policy *policy-name* match eap-type {add | delete} {eap-fast | eap-tls | leap | peap}**
  - **config policy *policy-name* match role {*role-name* | none}**
- 次のコマンドを入力して、ポリシーの一部として実行させるアクションを設定します。
  - ポリシーに対する ACL アクション : **config policy *policy-name* action acl {enable | disable} *acl-name***
  - QoS 平均データ レート : **config policy *policy-name* action average-data-rate {enable | disable} *rate***
  - QoS 平均リアルタイムデータ レート : **config policy *policy-name* action average-realtime-rate {enable | disable} *rate***
  - QoS バースト データ レート : **config policy *policy-name* action burst-data-rate {enable | disable} *rate***
  - QoS バースト リアルタイム データ レート : **config policy *policy-name* action burst-realtime-rate {enable | disable} *rate***
  - QoS アクション : **config policy *policy-name* action qos {enable | disable} {bronze | gold | platinum | silver}**
  - セッション タイムアウト アクション : **config policy *policy-name* action session-timeout {enable | disable} *timeout-in-seconds***
  - スリープ状態のクライアント タイムアウト アクション : **config policy *policy-name* action sleeping-client-timeout {enable | disable} *timeout-in-hours***

- AVC プロファイルの有効化 : **config policy policy-name action avc-profile-name enable avc-profile-name**
- AVC プロファイルの無効化 : **config policy policy-name action avc-profile-name disable**
- VLAN アクション : **config policy policy-name action vlan {enable | disable} wlan-id**



(注) バースト データ レートを設定する前に平均データ レートを設定してください。

- 次のコマンドを入力して、ポリシーのアクティブ タイムを設定します。  
**config policy policy-name active {add | delete} hours start-time end-time days {mon | tue | wed | thu | fri | sat | sun | daily | weekdays}**
- 次のコマンドを入力して、WLAN にローカル ポリシーを適用します。  
**config wlan policy {add | delete} priority-index policy-name wlan-id**
- 次のコマンドを入力して、HTTP と DHCP の両方またはいずれかに基づいて、WLAN に対してローカル モードのクライアント プロファイルを有効または無効にします。  
**config wlan profiling local {dhcp | http | all} {enable | disable} wlan-id**
- 次のコマンドを入力して、WLAN の AP グループにローカル ポリシーを適用します。  
**config wlan apgroup policy {add | delete} priority-index policy-name ap-group-name wlan-id**
- 次のコマンドを入力して、ポリシーに関する情報を表示します。  
**show policy {summary | policy-name} statistics**
- 次のコマンドを入力して、ローカル デバイス分類プロファイルの概要を表示します。  
**show profiling policy summary**
- 次のコマンドを入力して、すべてのクライアントとデバイス タイプを表示します。  
**show client wlan wlan-id device-type device-type**
- 次のコマンドを入力して、RADIUS サーバおよびコントローラによって行われたプロファイルを含むクライアントのプロファイル ステータスを表示します。  
**show wlan wlan-id**
- 次のコマンドを入力して、AP グループに関するポリシーの詳細を表示します。  
**show wlan apgroups**
- 次のコマンドを入力して、ポリシーのデバッグ タスクを設定します。  
**debug policy {error | event} {enable | disable}**





## 第 66 章

# Cisco Intrusion Detection System の設定

- [Cisco Intrusion Detection System](#) について, 603 ページ
- その他の情報, 604 ページ
- IDS センサーの設定 (GUI) , 604 ページ
- 回避クライアントの表示 (GUI) , 605 ページ
- IDS センサーの設定 (CLI) , 605 ページ
- 回避クライアントの表示 (CLI) , 607 ページ

## Cisco Intrusion Detection System について

Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/IPS) は、特定のクライアントに関わる攻撃がレイヤ 3 ~ レイヤ 7 で検出されたとき、これらのクライアントによるワイヤレスネットワークへのアクセスをブロックするよう、コントローラに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワークウイルス、およびアプリケーションの不正使用などの脅威の検出、分類、阻止を支援することにより、強力なネットワーク保護を提供します。潜在的な攻撃を検出するには 2 つの方法があります。

- IDS センサー
- IDS シグニチャ

ネットワークのさまざまなタイプの IP レベル攻撃を検出するように、IDS センサーを設定することができます。センサーで攻撃が特定されたら、違反クライアントを回避 (shun) するよう、コントローラに警告することができます。新しく IDS センサーを追加したときは、コントローラをその IDS センサーに登録し、回避クライアントのリストをセンサーから取得できるようにします。

## 回避クライアント

IDS センサーは、疑わしいクライアントを検出すると、コントローラにこのクライアントを回避するよう警告します。回避エントリは、同じモビリティグループ内のすべてのコントローラに配

信されます。回避すべきクライアントが現在、このモビリティグループ内のコントローラに join している場合、アンカーコントローラはこのクライアントを動的除外リストに追加し、外部コントローラはクライアントを切り離します。次回、このクライアントがコントローラに接続を試みた場合、アンカーコントローラはハンドオフを拒否し、外部コントローラにクライアントを除外することを通知します。

## その他の情報

コントローラでは Cisco Prime Infrastructure を介して Cisco Wireless Intrusion Prevention System (wIPS) もサポートされています。詳細については、「wIPS の設定」の項を参照してください。

## IDS センサーの設定 (GUI)

- 
- ステップ 1** [Security] > [Advanced] > [CIDs] > [Sensors] の順に選択して、[CIDS Sensors List] ページを開きます。  
(注) 既存のセンサーを削除するには、そのセンサーの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- ステップ 2** リストに新しい IDS センサーを追加するには、[New] をクリックします。[CIDS Sensor Add] ページが表示されます。
- ステップ 3** [Index] ドロップダウンリストから数字 (1 ~ 5) を選択し、コントローラで IDS センサーが検索される順序を決定します。たとえば、1 を選択した場合には、コントローラは最初にこの IDS センサーを検索します。  
コントローラでは最大 5 つの IDS センサーをサポートします。
- ステップ 4** [Server Address] テキストボックスに、IDS サーバの IP アドレスを入力します。
- ステップ 5** [Port] テキストボックスに、コントローラが IDS センサーとの通信に使用する必要がある HTTPS ポートの番号を入力します。  
センサーはデフォルトで 443 を使用して通信するので、このパラメータを 443 に設定することをお勧めします。デフォルト値は 443 で、範囲は 1 ~ 65535 です。
- ステップ 6** [Username] テキストボックスに、コントローラが IDS センサーの認証に使用するユーザ名を入力します。
- 例：  
(注) このユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。
- ステップ 7** [Password] テキストボックスと [Confirm Password] テキストボックスに、コントローラが IDS センサーの認証に使用するパスワードを入力します。
- ステップ 8** [Query Interval] テキストボックスに、コントローラが IDS サーバで IDS イベントをクエリーする間隔 (秒単位) を入力します。  
デフォルトは 60 秒で、範囲は 10 ~ 3600 秒です。

- ステップ 9** [State] チェックボックスをオンにしてコントローラをこの IDS センサーに登録するか、このチェックボックスをオフにして登録を解除します。デフォルト値はディセーブルです。
- ステップ 10** [Fingerprint] テキストボックスに、40 桁の 16 進数文字のセキュリティ キーを入力します。このキーは、センサーの有効性の確認、およびセキュリティ攻撃の防止に使用されます。  
(注) キー内にコロンが 2 バイト間隔で表記されるようにしてください。たとえば AA:BB:CC:DD のように入力します。
- ステップ 11** [Apply] をクリックします。[CIDS Sensors List] ページのセンサーのリストに新しい IDS センサーが表示されます。
- ステップ 12** [Save Configuration] をクリックします。

## 回避クライアントの表示 (GUI)

- ステップ 1** [Security] > [Advanced] > [CIDS] > [Shunned Clients] の順に選択して、[CIDS Shun List] ページを開きます。このページには、各回避クライアントの IP アドレスと MAC アドレス、IDS センサーの要求に応じてコントローラがクライアントのデータ パケットをブロックする期間、およびクライアントを検出した IDS センサーの IP アドレスが表示されます。
- ステップ 2** 必要に応じて [Re-sync] をクリックし、リストを削除およびリセットします。  
(注) コントローラは、対応するタイマーが期限切れになっても、回避エントリに何も処理を行いません。回避エントリタイマーは、表示用としてのみ保持されます。回避エントリはコントローラが IPS サーバをポーリングするたびにクリーンアップされます。CIDS IPS サーバに接続できない場合、回避エントリはコントローラでタイムアウトが生じても削除されません。回避エントリは、CIDS IPS サーバが再び動作し、コントローラが CIDS IPS サーバをポーリングするときのみクリーンアップされます。

## IDS センサーの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、IDS センサーを追加します。  
**config wps cids-sensor add index ids\_ip\_address username password.** index パラメータは、コントローラで IDS センサーが検索される順序を決定します。コントローラでは最大 5 つの IDS センサーをサポートします。数字 (1~5) を入力してこのセンサーの優先順位を決定します。たとえば、1 を入力した場合には、コントローラは最初にこの IDS センサーを検索します。  
(注) ユーザ名は IDS センサーに設定されており、少なくとも読み取り専用権限を持っている必要があります。

**ステップ 2** (任意) 次のコマンドを入力して、コントローラが IDS センサーとの通信に使用する HTTPS ポートの番号を指定します。

**config wps cids-sensor port index port**

port-number パラメータには、1 ~ 65535 の値を入力することができます。デフォルト値は 443 です。この手順は任意であり、デフォルト値の 443 を使用することをお勧めします。デフォルトでは、センサーはこの値を使用して通信します。

**ステップ 3** 次のコマンドを入力して、コントローラが IDS センサーで IDS イベントをクエリーする間隔を指定します。

**config wps cids-sensor interval index interval**

interval パラメータには、10 ~ 3600 秒の値を入力することができます。デフォルト値は 60 秒です。

**ステップ 4** 次のコマンドを入力して、センサーの有効性の確認に使用する 40 桁の 16 進数文字から成るセキュリティキーを入力します。

**config wps cids-sensor fingerprint index sha1 fingerprint**

センサーのコンソール上で **show tls fingerprint** と入力すると、フィンガープリントの値を取得できます。

(注) キー内にコロン (:) が 2 バイト間隔で表記されるようにしてください (たとえば、AA:BB:CC:DD)。

**ステップ 5** 次のコマンドを入力して、IDS センサーへのこのコントローラの登録を有効または無効にします。

**config wps cids-sensor {enable | disable} index**

**ステップ 6** 次のコマンドを入力して、DoS 攻撃からの保護を有効または無効にします。

デフォルト値はディセーブルです。

(注) 潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するように IDS を誘導する場合があります。それによって、コントローラはこの正規のクライアントの接続を誤って解除し、DoS 攻撃が開始されます。自己免疫機能は、有効な場合にこのような攻撃を防ぐように設計されています。ただし、自己免疫機能を有効にすると、Cisco 792x フォンを使用した会話が断続的に中断されることがあります。792x フォンを使用しているときに頻繁に中断されるようであれば、この機能を無効にしてください。

**ステップ 7** 次のコマンドを入力して、設定を保存します。

**save config**

**ステップ 8** 次のコマンドのいずれかを入力して、IDS センサーの設定を表示します。

- **show wps cids-sensor summary**
- **show wps cids-sensor detail index**

**ステップ 9** 2 つ目のコマンドは、1 つ目のコマンドよりも詳細な情報を提供します。

**ステップ 10** 次のコマンドを入力して、自動免疫設定の情報を表示します。

**show wps summary**

以下に類似した情報が表示されます。

```
Auto-Immune
 Auto-Immune..... Disabled

Client Exclusion Policy
```

```

Excessive 802.11-association failures..... Enabled
Excessive 802.11-authentication failures..... Enabled
Excessive 802.1x-authentication..... Enabled
IP-theft..... Enabled
Excessive Web authentication failure..... Enabled
Signature Policy
Signature Processing..... Enabled

```

**ステップ 11** 次のコマンドを入力して、IDS センサー設定に関連するデバッグ情報を取得します。

**debug wps cids enable**

(注) センサーの設定を削除または変更するには、まず `config wps cids-sensor disable index` コマンドを入力して設定を無効にする必要があります。その後、センサーを削除するには、`config wps cids-sensor delete index` コマンドを入力します。

## 回避クライアントの表示 (CLI)

**ステップ 1** 次のコマンドを入力して、回避すべきクライアントのリストを表示します。

**show wps shun-list**

**ステップ 2** 次のコマンドを入力して、コントローラを、この回避リストに対応するモビリティグループ内の他のコントローラに同期させます。

**config wps shun-list re-sync**

(注) コントローラは、対応するタイマーが期限切れになっても、回避エントリに何も処理を行いません。回避エントリタイマーは、表示用としてのみ保持されます。回避エントリはコントローラが IPS サーバをポーリングするたびにクリーンアップされます。CIDS IPS サーバに接続できない場合、回避エントリはコントローラでタイムアウトが生じても削除されません。回避エントリは、CIDS IPS サーバが再び動作し、コントローラが CIDS IPS サーバをポーリングするときのみクリーンアップされます。





# 第 67 章

## IDS シグニチャの設定

- [IDS シグニチャについて](#), 609 ページ
- [IDS シグニチャの設定 \(GUI\)](#), 612 ページ
- [IDS シグニチャ イベントの表示 \(GUI\)](#), 615 ページ
- [IDS シグニチャの設定 \(CLI\)](#), 616 ページ
- [IDS シグニチャ イベントの表示 \(CLI\)](#), 617 ページ

### IDS シグニチャについて

コントローラ上で、IDS シグニチャ、または受信する 802.11 パケットにおけるさまざまなタイプの攻撃を識別するのに使用されるビットパターンのマッチングルールを設定することができます。シグニチャが有効化されると、コントローラに join されたアクセスポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。攻撃が検出されると、適切な緩和措置が開始されます。

シスコでは 17 の標準シグニチャをサポートしています。これらのシグニチャは 6 つの主要なグループに分かれます。初めの 4 つのグループには管理シグニチャが含まれており、後の 2 つのグループにはデータ シグニチャが含まれます。

- **ブロードキャスト認証解除フレームシグニチャ**：ブロードキャスト認証解除フレーム攻撃において、ハッカーは別のクライアントのブロードキャスト MAC 宛先アドレスに対して 802.11 認証解除フレームを送信します。この攻撃により、宛先クライアントは接続アクセスポイントから強制的にアソシエーション解除させられ、ネットワークの接続断が発生します。この処理が繰り返されると、クライアントでサービス利用ができない状態が発生します。ブロードキャスト認証解除フレームシグニチャ（優先順位 1）を使用してそのような攻撃を検出する場合、アクセスポイントでは、シグニチャの特性と一致するクライアント送信ブロードキャスト認証解除フレームがリッスンされます。アクセスポイントは、そのような攻撃を検出すると、コントローラに警告を送ります。システムの設定に応じて、危険性のあるデバイスが封じ込められて、そのデバイスの信号が許可されたクライアントに干渉しないようにされるか、コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されるか、または、その両方が実行されます。

- **NULL プロブ応答シグニチャ** : NULL プロブ応答攻撃において、ハッカーは無線クライアントアダプタに NULL プロブ応答を送信します。結果として、クライアントアダプタがロックされます。NULL プロブ応答シグニチャを使用してそのような攻撃が検出されると、アクセスポイントはワイヤレスクライアントを特定し、コントローラに警告を送ります。NULL プロブ応答シグニチャを次に示します。

- NULL probe resp 1 (優先順位 2)
- NULL probe resp 2 (優先順位 3)



(注) コントローラは、Signature Events Summary 出力内に履歴 NULL プロブ IDS イベントを記録しません。

- **管理フレームフラッドシグニチャ** : 管理フレームフラッド攻撃において、ハッカーはアクセスポイントに大量の 802.11 管理フレームを送り付けます。その結果、アクセスポイントにアソシエートしている、もしくはアソシエートを試みているすべての端末に対して、サービス利用ができない状態が発生します。この攻撃は、アソシエーション要求、認証要求、再アソシエーション要求、プローブ要求、アソシエーション解除要求、認証解除要求、予約管理サブタイプなど、さまざまなタイプの管理フレームを使用して実行されます。

管理フレームフラッドシグニチャを使用してそのような攻撃が検出されると、アクセスポイントによって、シグニチャのすべての特性と一致する管理フレームが特定されます。これらのフレームの検出頻度が、シグニチャで設定された閾値より大きくなると、これらのフレームを受信するアクセスポイントによって警告が送信されます。コントローラはトラップを生成し、それを Cisco Prime Infrastructure に転送します。

管理フレームフラッドシグニチャを次に示します。

- Assoc flood (優先順位 4)
- Auth flood (優先順位 5)
- Reassoc flood (優先順位 6)
- Broadcast probe flood (優先順位 7)
- Disassoc flood (優先順位 8)
- Deauth flood (優先順位 9)
- Reserved mgmt 7 (優先順位 10)
- Reserved mgmt F (優先順位 11)

予約管理フレームシグニチャ (Reserved mgmt) 7 および F は、将来使用するために予約されています。

- **Wellenreiter シグニチャ** : Wellenreiter は、無線 LAN スキャンおよびディスカバリユーティリティです。これを使用すると、アクセスポイントおよびクライアントに関する情報が漏洩してしまう可能性があります。Wellenreiter シグニチャ (優先順位 17) を使用してそのよう



な攻撃が検出されると、アクセスポイントは危険性のあるデバイスを特定し、コントローラに警告を送ります。

- **EAPOL フラッドシグニチャ**：EAPOL フラッド攻撃において、ハッカーは 802.1X 認証要求を含む EAPOL フレームを大量に発生させます。結果として、802.1X 認証サーバはすべての要求に応答できなくなり、有効なクライアントに正常な認証応答を送信できなくなります。そして、その影響を受けるすべてのクライアントにおいてサービス利用ができない状況が発生します。EAPOL フラッドシグニチャ（優先順位 12）を使用してそのような攻撃が検出されると、アクセスポイントは EAPOL パケットの最大許容数を超えるまで待機します。次に、コントローラに警告を送り、適切な緩和措置を実行します。
- **NetStumbler シグニチャ**：NetStumbler は、無線 LAN スキャンユーティリティです。これによって、アクセスポイントのブロードキャスト関連情報（動作チャネル、RSSI 情報、アダプタ製造業者名、SSID、WEP ステータス、GPS が接続された NetStumbler を実行するデバイスの経度と緯度など）が報告されます。NetStumbler は、アクセスポイントに対する認証とアソシエーションを正常に完了すると、次の文字列のデータ フレーム（NetStumbler のバージョンによって異なる）を送信します。

バージョン	文字列
3.2.0	「Flurble gronk bloopit、bnip Frundletrune」
3.2.3	「All your 802.11b are belong to us」
3.3.0	ホワイトスペースを送信

NetStumbler シグニチャを使用してそのような攻撃が検出されると、アクセスポイントは危険性のあるデバイスを特定してコントローラに警告を送ります。NetStumbler シグニチャは次のとおりです。

- NetStumbler 3.2.0（優先順位 13）
- NetStumbler 3.2.3（優先順位 14）
- NetStumbler 3.3.0（優先順位 15）
- NetStumbler generic（優先順位 16）

コントローラ上にはデフォルトで標準シグニチャ ファイルが存在します。このシグニチャ ファイルをコントローラからアップロードすることも、カスタムシグニチャファイルを作成してコントローラにダウンロードすることも、または標準シグニチャファイルを修正してカスタムシグニチャファイルを作成することもできます。

## IDS シグニチャの設定 (GUI)

### IDS シグニチャのアップロードまたはダウンロード

**ステップ 1** 必要に応じて、独自のカスタム シグニチャ ファイルを作成します。

**ステップ 2** Trivial File Transfer Protocol (TFTP) サーバが使用可能であることを確認します。TFTP サーバをセットアップするときには、次のガイドラインに従ってください。

- サービスポート経由でダウンロードする場合、サービスポートはルーティングできないため、TFTP サーバはサービスポートと同じサブネット上になければなりません。そうでない場合は、コントローラ上に静的ルートを作成する必要があります。
- ディストリビューションシステム ネットワーク ポートを経由してダウンロードする場合、ディストリビューションシステムポートはルーティング可能なので、TFTP サーバは同じサブネット上にあっても、別のサブネット上にあってもかまいません。
- サードパーティの TFTP サーバを Cisco Prime Infrastructure と同じ PC 上で実行することはできません。Prime Infrastructure 内蔵 TFTP サーバとサードパーティの TFTP サーバのどちらも、同じ通信ポートを使用するからです。

**ステップ 3** カスタムシグニチャファイル (\*.sig) をダウンロードする場合は、ファイルを TFTP サーバ上のデフォルトディレクトリに移動します。

**ステップ 4** [Commands] を選択して、[Download File to Controller] ページを開きます。

**ステップ 5** 次のいずれかの操作を行います。

- カスタムシグニチャファイルをコントローラにダウンロードする場合は、[Download File to Controller] ページの [File Type] ドロップダウンリストから [Signature File] を選択します。
- 標準シグニチャファイルをコントローラからアップロードする場合は、[Upload File] を選択してから、[Upload File from Controller] ページの [File Type] ドロップダウンリストから [Signature File] を選択します。

**ステップ 6** [Transfer Mode] ドロップダウンリストから、[TFTP] または [FTP] を選択します。

**ステップ 7** [IP Address] テキストボックスに、TFTP または FTP サーバの IP アドレスを入力します。

**ステップ 8** TFTP サーバを使用してシグニチャファイルをダウンロードする場合は、[Maximum Retries] テキストボックスに、コントローラがシグニチャファイルのダウンロードを試行する最大回数を入力します。指定できる範囲は 1 ~ 254 で、デフォルトは 10 です。

**ステップ 9** TFTP サーバを使用してシグニチャファイルをダウンロードする場合は、シグニチャファイルのダウンロードの試行時にコントローラがタイムアウトするまでの時間 (秒単位) を [Timeout] テキストボックスに入力します。範囲は 1 ~ 254 秒で、デフォルトは 6 秒です。

**ステップ 10** [File Path] テキスト ボックスに、ダウンロードまたはアップロードするシグニチャ ファイルのパスを入力します。デフォルト値は「/」です。

**ステップ 11** [File Name] テキスト ボックスに、ダウンロードまたはアップロードするシグニチャ ファイルの名前を入力します。

(注) シグニチャをアップロードする際、コントローラはユーザが指定した基本名に「\_std.sig」および「\_custom.sig」を追加したファイル名を使用して、標準シグニチャ ファイルとカスタム シグニチャ ファイルの両方を TFTP サーバにアップロードします。たとえば、「ids1」という名前のシグニチャ ファイルをアップロードする場合、コントローラは自動的に ids1\_std.sig と ids1\_custom.sig を生成して TFTP サーバにアップロードします。その後、必要に応じて TFTP サーバ上で ids1\_custom.sig を変更し（必ず「Revision = custom」を設定してください）、シグニチャ ファイルを自動的にダウンロードすることもできます。

**ステップ 12** FTP サーバを使用している場合は、次の手順に従います。

- 1 [Server Login Username] テキスト ボックスに、FTP サーバにログインするためのユーザ名を入力します。
- 2 [Server Login Password] テキスト ボックスに、FTP サーバにログインするためのパスワードを入力します。
- 3 [Server Port Number] テキスト ボックスに、ダウンロードが発生する FTP サーバのポート番号を入力します。デフォルト値は 21 です。

**ステップ 13** [Download] を選択してシグニチャファイルをコントローラにダウンロードするか、[Upload] を選択してコントローラからシグニチャ ファイルをアップロードします。

## IDS シグニチャの有効化または無効化

**ステップ 1** [Security] > [Wireless Protection Policies] > [Standard Signatures] または [Custom Signatures] の順に選択して、[Standard Signatures] ページまたは [Custom Signatures] ページを開きます。  
[Standard Signatures] ページには、現在コントローラ上に存在するシスコ提供のシグニチャのリストが表示されます。[Custom Signatures] ページには、現在コントローラ上に存在する、カスタマー提供のシグニチャのリストが表示されます。このページには、各シグニチャについて次の情報が表示されます。

- コントローラがシグニチャ チェックを行う順序、または優先順位。
- シグニチャ名。シグニチャが検出しようとする攻撃タイプを明示するもの。
- シグニチャがセキュリティ攻撃を検出するフレームタイプ。フレームタイプとしては、データおよび管理があります。
- シグニチャが攻撃を検出したとき、コントローラが行うべき処理。実行可能な処理は、None と Report です。

- シグニチャの状態。セキュリティ攻撃を検出するために、シグニチャが有効化されているかどうかを示すもの。
- シグニチャが検出しようとする攻撃のタイプの説明。

**ステップ 2** 次のいずれかの操作を行います。

- 個々の状態が [Enabled] に設定されたすべてのシグニチャ（標準およびカスタムの両方）を有効なままにしておくには、[Standard Signatures] ページまたは [Custom Signatures] ページの上部の [Enable Check for All Standard and Custom Signatures] チェックボックスをオンにします。デフォルト値が有効（オン）になっています。シグニチャが有効化されると、コントローラに join したアクセス ポイントでは、受信した 802.11 データまたは管理フレームに対してシグニチャ分析が行われ、整合性がない場合はコントローラに報告されます。
- コントローラ上のすべてのシグニチャ（標準およびカスタムの両方）を無効にしておく場合には、[Enable Check for All Standard and Custom Signatures] チェックボックスをオフにします。このチェックボックスをオフにすると、たとえシグニチャの個々の状態が [Enabled] に設定されている場合でも、すべてのシグニチャが無効になります。

**ステップ 3** [Apply] をクリックして、変更を確定します。

**ステップ 4** 目的とするシグニチャの優先順位番号をクリックして、個々のシグニチャを有効または無効にします。[Standard Signature（または Custom Signature）> Detail] ページが表示されます。このページには、[Standard Signatures] ページおよび [Custom Signatures] ページとほぼ同じ情報が表示されますが、次のような詳細も表示されます。

- アクセス ポイントによるシグニチャ分析およびコントローラへの結果報告に使用される追跡方法。表示される値は次のとおりです。
  - [Per Signature] : シグニチャ分析とパターン マッチングにおける追跡および報告は、シグニチャ別およびチャネル別に実行されます。
  - [Per MAC] : シグニチャ分析とパターン マッチングにおける追跡と報告は、チャネルごとに個々のクライアント MAC アドレス別に実行されます。
  - [Per Signature and MAC] : シグニチャ分析とパターン マッチングにおける追跡と報告は、シグニチャ別/チャネル別、および MAC アドレス別/チャネル別の両方で実行されます。
- セキュリティ攻撃の検出に使用されるパターン。

- ステップ 5** [Measurement Interval] テキストボックスに、設定された間隔内でシグニチャ頻度がしきい値に達するまでの経過時間 (秒数) を入力します。有効な値の範囲は 1 ~ 3600 秒で、デフォルト値はシグニチャによって異なります。
- ステップ 6** [Signature Frequency] テキストボックスに、個々のアクセスポイントレベルで特定されるべき、1 間隔あたりの一致パケット数を入力します。この値に達すると攻撃が検出されたと判断されます。有効な値の範囲は 1 間隔あたり 1 ~ 32,000 パケットで、デフォルト値はシグニチャによって異なります。
- ステップ 7** [Signature MAC Frequency] テキストボックスに、個々のアクセスポイントでクライアント別に特定されるべき、1 間隔あたりの一致パケット数を入力します。この値に達すると攻撃が検出されたと判断されます。有効な値の範囲は 1 間隔あたり 1 ~ 32,000 パケットで、デフォルト値はシグニチャによって異なります。
- ステップ 8** [Quiet Time] テキストボックスに、個々のアクセスポイントレベルで攻撃が検出されない状態が続き、アラームを停止できるようになるまでの時間 (秒単位) を入力します。有効な値の範囲は 60 ~ 32,000 秒で、デフォルト値はシグニチャによって異なります。
- ステップ 9** [State] チェックボックスをオンにしてこのシグニチャを有効にし、セキュリティ攻撃を検出するか、オフにしてこのシグニチャを無効にします。デフォルト値が有効 (オン) になっています。
- ステップ 10** [Apply] をクリックして、変更を確定します。[Standard Signatures] ページまたは [Custom Signatures] ページに、シグニチャの更新された状態が反映されます。
- ステップ 11** [Save Configuration] をクリックして、変更を保存します。

## IDS シグニチャ イベントの表示 (GUI)

- ステップ 1** [Security] > [Wireless Protection Policies] > [Signature Events Summary] の順に選択して、[Signature Events Summary] ページを開きます。
- ステップ 2** 特定のシグニチャによって検出された攻撃の詳細を表示するには、そのシグニチャのシグニチャタイプをクリックします。[Signature Events Detail] ページが表示されます。このページには、次の情報が表示されます。
- 攻撃者として特定されたクライアントの MAC アドレス
  - アクセスポイントが攻撃の追跡に使用する方法
  - 攻撃が検出されるまでに特定された 1 秒あたりの一致パケットの数
  - 攻撃が検出されたチャンネル上のアクセスポイント数
  - アクセスポイントが攻撃を検出した日時
- ステップ 3** 特定の攻撃に関する詳細を表示するには、その攻撃の [Detail link] をクリックします。[Signature Events Track Detail] ページが表示されます。
- 攻撃を検出したアクセスポイントの MAC アドレス

- 攻撃を検出したアクセス ポイントの名前
- アクセス ポイントが攻撃の検出に使用した無線のタイプ (802.11a または 802.11b/g)
- 攻撃が検出された無線チャネル
- アクセス ポイントから攻撃が報告された日時

## IDS シグニチャの設定 (CLI)

- ステップ 1 必要に応じて、独自のカスタム シグニチャ ファイルを作成します。
- ステップ 2 TFTP サーバが使用可能であることを確認します。
- ステップ 3 カスタム シグニチャ ファイル (\*.sig) を TFTP サーバ上のデフォルト ディレクトリに移動します。
- ステップ 4 **transfer {download | upload} mode tftp** コマンドを入力して、ダウンロードモードまたはアップロードモードを指定します。
- ステップ 5 **transfer {download | upload} datatype signature** コマンドを入力して、ダウンロードまたはアップロードするファイルのタイプを指定します。
- ステップ 6 **transfer {download | upload} serverip tftp-server-ip-address** コマンドを入力して、TFTP サーバの IP アドレスを指定します。  
 (注) TFTP サーバによっては、TFTP サーバ IP アドレスにスラッシュ (/) を入力するだけで、自動的に適切なディレクトリへのパスが判別されるものもあります。
- ステップ 7 **transfer {download | upload} path absolute-tftp-server-path-to-file** コマンドを入力して、ダウンロードまたはアップロードのパスを指定します。
- ステップ 8 **transfer {download | upload} filename filename.sig** コマンドを入力して、ダウンロードまたはアップロードするファイルを指定します。  
 (注) シグニチャをアップロードする際、コントローラはユーザが指定した基本名に「\_std.sig」および「\_custom.sig」を追加したファイル名を使用して、標準シグニチャ ファイルとカスタム シグニチャ ファイルの両方を TFTP サーバにアップロードします。たとえば、「ids1」という名前のシグニチャ ファイルをアップロードする場合、コントローラは自動的に **ids1\_std.sig** と **ids1\_custom.sig** を生成して TFTP サーバにアップロードします。その後、必要に応じて TFTP サーバ上で **ids1\_custom.sig** を変更し (必ず「Revision=custom」を設定してください)、シグニチャ ファイルを自動的にダウンロードすることもできます。
- ステップ 9 **transfer {download | upload} start** コマンドを入力し、プロンプトに y と応答して現在の設定を確認し、ダウンロードまたはアップロードを開始します。
- ステップ 10 次のコマンドを入力して、設定された間隔内でシグニチャ頻度がしきい値に達するまでの経過時間 (秒数) を指定します。  
**config wps signature interval signature\_id interval**

ここで、`signature_id` は、シグニチャを一意に識別するために使用する数字です。有効な値の範囲は 1 ～ 3600 秒で、デフォルト値はシグニチャによって異なります。

**ステップ 11** 次のコマンドを入力して、個々のアクセスポイントレベルで特定されるべき、1 間隔あたりの一致パケット数を指定します。この値に達すると攻撃が検出されたと判断されます。

```
config wps signature frequency signature_id frequency
```

有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

**ステップ 12** 次のコマンドを入力して、個々のアクセスポイントでクライアント別に特定されるべき、1 間隔あたりの一致パケット数を指定します。この値に達すると攻撃が検出されたと判断されます。

```
config wps signature mac-frequency signature_id mac_frequency
```

有効な値の範囲は 1 間隔あたり 1 ～ 32,000 パケットで、デフォルト値はシグニチャによって異なります。

**ステップ 13** 次のコマンドを入力して、個々のアクセスポイントレベルで攻撃が検出されない状態が続き、アラームを停止できるようになるまでの時間 (秒単位) を指定します。

```
config wps signature quiet-time signature_id quiet_time
```

有効な値の範囲は 60 ～ 32,000 秒で、デフォルト値はシグニチャによって異なります。

**ステップ 14** 次のいずれかの操作を行います。

- 個々の IDS シグニチャを有効または無効にするには、次のコマンドを入力します。

```
config wps signature {standard | custom} state signature_id {enable | disable}
```

- IDS シグニチャ処理を有効または無効 (すべての IDS シグニチャの処理を有効または無効) には、次のコマンドを入力します。

```
config wps signature {enable | disable}
```

(注) IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

**ステップ 15** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 16** 必要に応じて、特定のシグニチャまたはすべてのシグニチャをデフォルト値にリセットできます。そのためには、次のコマンドを入力します。

```
config wps signature reset {signature_id | all}
```

(注) シグニチャをデフォルト値にリセットするには、コントローラの CLI しか使用できません。

## IDS シグニチャ イベントの表示 (CLI)

- 次のコマンドを入力して、コントローラで IDS シグニチャ処理が有効か無効かを確認します。

```
show wps summary
```



(注) IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

- 次のコマンドを入力して、コントローラにインストールされているすべての標準シグニチャとカスタム シグニチャの個々の要約を表示します。

**show wps signature summary**

- 次のコマンドを入力して、有効なシグニチャによって検出された攻撃の数を表示します。

**show wps signature events summary**

- 次のコマンドを入力して、特定の標準シグニチャまたはカスタムシグニチャによって検出された攻撃の詳細を表示します。

**show wps signature events {standard | custom} precedence# summary**

- 次のコマンドを入力して、アクセス ポイントによってシグニチャ別/チャンネル別に追跡される攻撃の詳細を表示します。

**show wps signature events {standard | custom} precedence# detailed per-signature source\_mac**

- 次のコマンドを入力して、アクセス ポイントによって個別クライアントベース (MAC アドレス別) で追跡される攻撃の詳細を表示します。

**show wps signature events {standard | custom} precedence# detailed per-mac source\_mac**





# 第 68 章

## wIPS の設定

---

- [wIPS について](#), 619 ページ
- [wIPS の制約事項](#), 627 ページ
- [アクセス ポイントでの wIPS の設定 \(GUI\)](#), 627 ページ
- [アクセス ポイントでの wIPS の設定 \(CLI\)](#), 627 ページ
- [wIPS 情報の表示 \(CLI\)](#), 629 ページ

### wIPS について

Cisco 適応型ワイヤレス侵入防御システム (wIPS) は、無線の脅威の検出およびパフォーマンス管理のための高度な手法です。この手法では、ネットワークトラフィック分析、ネットワークデバイス/トポロジに関する情報、シグニチャベースの技法、および異常検出を組み合わせることにより、非常に正確で全面的な無線の脅威防御を実現できます。インフラストラクチャに完全に統合されたソリューションを採用すると、有線ネットワークと無線ネットワークの両方で無線トラフィックを継続的に監視し、ネットワークインテリジェンスを使用してさまざまなソースからの攻撃を分析することにより、損害または漏洩が発生する前に、攻撃をより正確に特定し事前に防止することができます。

シスコの適合型 wIPS には、Cisco 3300 シリーズ Mobility Services Engine (MSE) が必要です。MSE は、Cisco Aironet アクセスポイントの継続的な監視によって収集された情報の処理を一元化します。シスコの適合型 wIPS の機能と、MSE への Cisco Prime Infrastructure の統合により、wIPS サービスで wIPS ポリシーとアラームの設定、監視、およびレポートを行うことができます。



(注) お使いの wIPS がコントローラ、アクセスポイント、および MSE で構成されている場合、これら 3 つのエンティティをすべて UTC タイムゾーンに設定する必要があります。

シスコの適合型 wIPS はコントローラに設定されていません。代わりに、プロファイル設定が Cisco Prime Infrastructure から wIPS サービスに転送され、wIPS サービスによってそのプロファイルがコントローラに転送されます。プロファイルはコントローラのフラッシュメモリに格納さ

れ、アクセスポイントがコントローラに join するとアクセスポイントへ送信されます。アクセスポイントのアソシエイトが解除され、別のコントローラへ join すると、アクセスポイントは新しいコントローラから wIPS プロファイルを受信します。

wIPS 機能のサブセットを備えたローカルモードまたは FlexConnect モードのアクセスポイントは、拡張ローカルモードアクセスポイント、または ELM AP と呼ばれます。アクセスポイントが次のいずれかのモードであれば、そのアクセスポイントを wIPS モードで動作するように設定できます。

- Monitor
- Local
- FlexConnect

通常のローカルモードまたは FlexConnect モードのアクセスポイントは、ワイヤレス侵入防御システム (wIPS) 機能のサブセットによって拡張されています。この機能を使用すると、分離されたオーバーレイネットワークがなくても、アクセスポイントを展開して保護機能を提供できます。

wIPS ELM では、オフチャネルのアラームを検出する機能が制限されます。アクセスポイントは定期的にオフチャネルになり、短い期間内に動作していないチャンネルを監視し、そのチャンネルで攻撃を検出した場合はアラームをトリガーします。ただし、オフチャネルのアラーム検出はベストエフォートであり、攻撃を検出してアラームをトリガーするには時間がかかることがあります。これが原因となって ELM AP が断続的にアラームを検出し、確認できないためそれをクリアする場合があります。上記のいずれかのモードのアクセスポイントは、ポリシープロファイルに基づくアラームをコントローラ経由で定期的に wIPS サービスに送信できます。wIPS サービスはアラームを格納および処理して、SNMP トラップを生成します。Cisco Prime Infrastructure は自身の IP アドレスをトラップの宛先として設定し、SNMP トラップを MSE から受信します。

次の表に SNMP トラップ制御とそれに対応するトラップを示します。トラップ制御が有効な場合、そのトラップ制御のトラップもすべて有効です。



---

(注) コントローラは SNMP トラップの送信に SNMPv2 のみを使用します。

---

表 18 : SNMP トラップ制御と対応トラップ

タブ名	トラップコントロール	トラップ
General	Link (Port) Up/Down	linkUp、 linkDown
	Spanning Tree	newRoot、 topologyChange、 stpInstanceNewRootTrap、 stpInstanceTopologyChangeTrap
	Config Save	bsnDot11EssCreated、 bsnDot11EssDeleted、 bsnConfigSaved、 ciscoLwappScheduledResetNotif、 ciscoLwappClearResetNotif、 ciscoLwappResetFailedNotif、 ciscoLwappSysInvalidXmlConfig
AP	AP Register	bsnAPDisassociated、 bsnAPAssociated
	Ap Interface Up/Down	bsnAPIfUp、 bsnAPIfDown
Client Traps	802.11 Association	bsnDot11StationAssociate
	802.11 Disassociation	bsnDot11StationDisassociate
	802.11 Deauthentication	bsnDot11StationDeauthenticate
	802.11 Failed Authentication	bsnDot11StationAuthenticateFail
	802.11 Failed Association	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted
	NAC Alert	cldcClientWlanProfileName、 cldcClientIPAddress、 cldcApMacAddress、 cldcClientQuarantineVLAN、 cldcClientAccessVLAN

タブ名	トラップコントロール	トラップ
Security Traps	User Authentication	bsnTooManyUnsuccessLoginAttempts、 cLWAGuestUserLoggedIn、 cLWAGuestUserLoggedOut
	RADIUS Servers Not Responding	bsnRADIUSServerNotResponding、 ciscoLwappAAARadiusReqTimedOut
	WEP Decrypt Error	bsnWepKeyDecryptError
	Rogue AP	bsnAdhocRogueAutoContained、 bsnRogueApAutoContained、 bsnTrustedApHasInvalidEncryption、 bsnMaxRogueCountExceeded、 bsnMaxRogueCountClear、 bsnApMaxRogueCountExceeded、 bsnApMaxRogueCountClear、 bsnTrustedApHasInvalidRadioPolicy、 bsnTrustedApHasInvalidSsid、 bsnTrustedApIsMissing
	SNMP Authentication	agentSnmpAuthenticationTrapFlag
	Multiple Users	multipleUsersTrap
Auto RF Profile Traps	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
Auto RF Update Traps	channel update	bsnAPCurrentChannelChanged
	Tx Power Update	bsnAPCurrentTxPowerChanged

タブ名	トラップ コントロール	トラップ
Mesh Traps	Child Excluded Parent	ciscoLwappMeshChildExcludedParent
	Parent Change	ciscoLwappMeshParentChange
	Authfailure Mesh	ciscoLwappMeshAuthorizationFailure
	Child Moved	ciscoLwappMeshChildMoved
	Excessive Parent Change	ciscoLwappMeshExcessiveParentChange
	Excessive Children	ciscoLwappMeshExcessiveChildren
	Poor SNR	ciscoLwappMeshAbateSNR、 ciscoLwappMeshOnsetSNR
	Console Login	ciscoLwappMeshConsoleLogin
	Excessive Association	ciscoLwappMeshExcessiveAssociation
	Default Bridge Group Name	ciscoLwappMeshDefaultBridgeGroupName

次に、「SNMP トラップ制御とそれぞれのトラップ」の表に記載されているトラップについて説明します。

- 一般トラップ

- [SNMP Authentication] : SNMPv2 エンティティが、適切に認証されていないプロトコルメッセージを受信しました。



(注) SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラーメッセージが表示されます。ただし、認証エラーの場合、トラップ ログは生成されません。

- [Link (Port) Up/Down] : リンクのステータスは、アップまたはダウンから変更されます。
- [Link (Port) Up/Down] : リンクのステータスは、アップまたはダウンから変更されます。
- [Multiple Users] : 2 人のユーザが同じ ID でログインします。
- [Rogue AP] : 不正アクセス ポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセスポイントが存在しなくなっている場合にこのトラップが送信されます。
- [Config Save] : コントローラ設定が変更されると送信される通知。

- Cisco AP トラップ

- [AP Register] : アクセス ポイントがコントローラとアソシエートまたはアソシエート解除すると送信される通知です。
- [AP Interface Up/Down] : アクセス ポイント インターフェイス (802.11X) の状態がアップまたはダウンになると送信される通知です。

• クライアント関連トラップ

- [802.11 Association] : クライアントがアソシエーション フレームを送信すると送信されるアソシエーション通知。
- [802.11 Disassociation] : クライアントがディスアソシエーション フレームを送信すると送信されるディスアソシエーション通知。
- [802.11 Deauthentication] : クライアントが認証解除フレームを送信すると送信される認証解除通知。
- [802.11 Failed Authentication] : クライアントが成功以外のステータス コードの認証フレームを送信すると送信される認証エラー通知。
- [802.11 Failed Authentication] : クライアントが成功以外のステータス コードのアソシエーション フレームを送信すると送信されるアソシエーション エラー通知。
- [Exclusion] : クライアントが Exclusion Listed (blacklisted) である場合に送信されるアソシエーション失敗通知。
- [Authentication] : クライアントが正常に認証されると送信される認証通知。
- [Max Clients Limit Reached] : [Threshold] フィールドに定義されているクライアントの最大数がコントローラとアソシエートした場合に送信される通知。
- [NAC Alert] : クライアントが SNMP NAC 対応 WLAN に join する場合に送信されるアラート。

この通知は、NAC 対応 SSID のクライアントがレイヤ 2 認証を完了し、NAC アプライアンスにクライアントのプレゼンスについて通知する場合に生成されます。

cldcClientWlanProfileName は、802.11 無線クライアントが接続されている WLAN のプロファイル名を表します。cldcClientIPAddress は、クライアントの一意の IP アドレスを表します。cldcApMacAddress は、クライアントがアソシエートされている AP の MAC アドレスを表します。cldcClientQuarantineVLAN は、クライアントの隔離 VLAN を表します。cldcClientAccessVLAN は、クライアントのアクセス VLAN を表します。

- [Association with Stats] : クライアントがコントローラとアソシエートする、またはローミングする場合に、データ統計とともに送信されるアソシエーション通知。データの統計情報には、送受信されたパケットおよびバイトが含まれます。
- クライアントがコントローラからアソシエート解除するときに、データ統計とともに送信される Stats—Disassociate 通知を持つディスアソシエーション。データの統計情報には、送受信されたパケットおよびバイト、SSID、およびセッション ID が含まれます。



(注) 以降のリリースからリリース 7.4 にダウングレードする場合、リリース 7.4 でサポートされないトラップ（たとえば、NAC Alert トラップ）がダウングレード前に有効になっていると、すべてのトラップは無効になります。ダウングレードが終了したら、ダウングレード前に有効であったすべてのトラップを有効にする必要があります。他のすべてのトラップが無効にならないように、ダウングレードする前に新しいトラップを無効にすることをお勧めします。

#### • Security Traps

- [User Auth Failure] : このトラップは、クライアントの RADIUS 認証の失敗が発生したことを通知します。
- [RADIUS Server No Response] : このトラップは、RADIUS クライアントが送信した認証要求に応答する RADIUS サーバがないことを示します。
- [WEP Decrypt Error] : コントローラが WEP 復号化エラーを検出すると送信される通知です。
- [Rogue AP] : 不正アクセスポイントが検出されるたびに、このトラップが MAC アドレスとともに送信されます。また、以前に検出された不正アクセスポイントが存在しなくなっている場合にこのトラップが送信されます。
- [SNMP Authentication] : SNMPv2 エンティティが、適切に認証されていないプロトコルメッセージを受信しました。



(注) SNMP V3 モードで設定されているユーザが正しくないパスワードでコントローラにアクセスを試みると、認証は失敗し、エラーメッセージが表示されます。ただし、認証エラーの場合、トラップログは生成されません。

- [Multiple Users] : 2 人のユーザが同じ ID でログインします。

#### • SNMP Authentication

- [Load Profile] : [Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Noise Profile] : [Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Interference Profile] : [Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- [Coverage Profile] : [Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

#### • 自動 RF プロファイル トラップ

- [Load Profile] : [Load Profile] 状態が PASS と FAIL の間で変更されると送信される通知。

- [Noise Profile] : [Noise Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Interference Profile] : [Interference Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
  - [Coverage Profile] : [Coverage Profile] 状態が PASS と FAIL の間で変更されると送信される通知。
- 自動 RF 更新トラップ
    - [Channel Update] : アクセスポイントの動的チャンネルアルゴリズムが更新されると送信される通知。
    - [Tx Power Update] : アクセスポイントの動的送信電力アルゴリズムが更新されると送信される通知。
- Mesh Traps
    - Child Excluded Parent : 親メッシュノードを介して、コントローラに対するアソシエーションの失敗数が定義された回数に達すると送信される通知。
    - 子メッシュノード数が検出応答タイムアウトのしきい値制限を超えると送信される通知。子メッシュノードが、定義された間隔で除外された親メッシュノードのアソシエーションを試行することはありません。子メッシュノードは、ネットワークに join するときに、除外された親 MAC アドレスをコントローラに通知します。
    - Parent Change : 子メッシュノードがその親を変更すると、通知がエージェントによって送信されます。子メッシュノードは以前の親を記憶し、ネットワークに再 join する際に、親の変更についてコントローラに通知します。
    - Child Moved : 親メッシュノードが子メッシュノードとの接続を失うと送信される通知。
    - Excessive Parent Change : 子メッシュノードが親を頻繁に変更すると送信される通知です。各メッシュノードは一定期間の親の変更回数のカウントを保持します。これが、定義されたしきい値を超えると、子メッシュノードはコントローラに通知します。
    - Excessive Children : 子の数が RAP および MAP に関して超過すると送信される通知。
    - Poor SNR : 子メッシュノードが、バックホールリンクでより低い SNR を検出すると送信される通知です。他のトラップの場合、子メッシュノードが、「clMeshSNRThresholdAbate」によって定義されるオブジェクトより高い SNR をバックホールリンクで検出すると、通知をクリアするための通知が送信されます。
    - Console Login : MAP コンソールでのログインが成功するか、3回の試行の後に失敗するとエージェントによって通知が送信されます。
    - Default Bridge Group Name : 「デフォルト」のブリッジグループ名を使用して MAP メッシュノードが親に参加すると送信される通知。





(注) 上記以外のトラップにトラップ制御機能はありません。これらのトラップは、頻繁に生成されないため、トラップ制御は必要ありません。コントローラによって生成されるその他のトラップをオフにすることはできません。



(注) 上記のすべてのケースで、コントローラは単なる転送デバイスとして機能します。



(注) MIB をダウンロードするには、[ここ](#)をクリックしてください。

## wIPS の制約事項

- wIPS ELM は 1130 および 1240 アクセス ポイントではサポートされません。

## アクセス ポイントでの wIPS の設定 (GUI)

**ステップ 1** [Wireless] > [Access Points] > [All APs] > アクセス ポイント名の順に選択します。

**ステップ 2** [AP Mode] パラメータを設定します。wIPS 用のアクセス ポイントを設定するには、[AP Mode] ドロップダウンリストから次のモードのいずれかを選択します。

- Local
- FlexConnect
- Monitor

**ステップ 3** [AP Sub Mode] ドロップダウンリストから [wIPS] を選択して、[AP Sub Mode] を wIPS に設定します。

**ステップ 4** [Apply] をクリックします。

**ステップ 5** [Save Configuration] をクリックします。

## アクセス ポイントでの wIPS の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、監視モード用のアクセス ポイントを設定します。

```
config ap mode {monitor | local | flexconnect} Cisco_AP
```

(注) wIPS 用のアクセスポイントを設定するには、そのアクセスポイントが **monitor**、**local**、または **Flexconnect** モードでなければなりません。

**ステップ 2** アクセスポイントがリブートされることを知らせるメッセージが表示された場合、処理を続行するには **Y** と入力します。

**ステップ 3** 次のコマンドを入力して、変更を保存します。  
**save config**

**ステップ 4** 次のコマンドを入力して、アクセスポイント無線を無効にします。  
**config {802.11a | 802.11b} disable Cisco\_AP**

**ステップ 5** 次のコマンドを入力して、アクセスポイントで wIPS サブモードを設定します。  
**config ap mode ap\_mode submode wips Cisco\_AP**

(注) アクセスポイントで wIPS を無効にするには、**config ap mode ap\_mode submode none Cisco\_AP** コマンドを入力します。

**ステップ 6** 次のコマンドを入力して、wIPS に最適化されたチャンネルスキャンをアクセスポイントで有効にします。  
**config ap monitor-mode wips-optimized Cisco\_AP**

アクセスポイントは、250 ミリ秒の間、各チャンネルをスキャンします。監視設定に基づいてスキャンされるチャンネルの一覧が取得されます。次のオプションのいずれかを選択できます。

- All : アクセスポイントの無線でサポートされているすべてのチャンネル
- Country : アクセスポイントの使用国でサポートされているチャンネルのみ
- DCA : 動的チャンネル割り当て (DCA) アルゴリズムによって使用されるチャンネルセットのみ (デフォルトでは、アクセスポイントの使用国で許可された、オーバーラップしないすべてのチャンネルを含む)

**show advanced {802.11a | 802.11b} monitor** コマンドの出力の 802.11a または 802.11b Monitor Channels テキストボックスに、監視設定チャンネルセットが表示されます。

```
Default 802.11b AP monitoring
802.11b Monitor Mode..... enable
802.11b Monitor Channels..... Country channels
802.11b AP Coverage Interval..... 180 seconds
802.11b AP Load Interval..... 60 seconds
802.11b AP Noise Interval..... 180 seconds
802.11b AP Signal Strength Interval..... 60 seconds
```

**ステップ 7** 次のコマンドを入力して、アクセスポイント無線を再度有効にします。  
**config { 802.11a | 802.11b} enable Cisco\_AP**

**ステップ 8** 次のコマンドを入力して、変更を保存します。  
**save config**

## wIPS 情報の表示 (CLI)



(注) コントローラ GUI からアクセス ポイントサブモードを表示することもできます。そのためには、[Wireless] > [Access Points] > [All APs] > アクセスポイント名 > [Advanced] タブを選択します。アクセス ポイントが監視モードで、そのアクセス ポイントに wIPS サブモードが設定されている場合、[AP Sub Mode] テキスト ボックスに [wIPS] と表示されます。アクセス ポイントが監視モードではない場合、または、アクセス ポイントは監視モードであるが wIPS サブモードが設定されていない場合、[AP Sub Mode] テキスト ボックスには [None] と表示されます。

- 次のコマンドを入力して、アクセス ポイントの wIPS サブモードを表示します。  
**show ap config general Cisco\_AP**
- 次のコマンドを入力して、アクセス ポイントに設定された、wIPS に最適化されたチャンネル スキャンを表示します。  
**show ap monitor-mode summary**
- 次のコマンドを入力して、Cisco Prime Infrastructure によってコントローラに転送される wIPS 設定を表示します。  
**show wps wips summary**
- 次のコマンドを入力して、コントローラで現在動作している wIPS の状態を表示します。  
**show wps wips statistics**
- 次のコマンドを入力して、コントローラ上の wIPS 統計情報をクリアします。  
**clear stats wps wips**





# 第 69 章

## Wi-Fi Direct クライアント ポリシーの設定

---

- [Wi-Fi Direct クライアント ポリシーについて](#), 631 ページ
- [Wi-Fi Direct クライアント ポリシーの制限](#), 631 ページ
- [Wi-Fi Direct クライアント ポリシーの設定 \(GUI\)](#), 632 ページ
- [Wi-Fi Direct クライアント ポリシーの設定 \(CLI\)](#), 632 ページ
- [Wi-Fi Direct クライアント ポリシーの監視とトラブルシューティング \(CLI\)](#), 633 ページ

### Wi-Fi Direct クライアント ポリシーについて

Wi-Fi Direct 対応のデバイスは迅速な相互接続が可能で、印刷、同期、データ共有などのタスクを効率的に実行できます。Wi-Fi Direct デバイスは、複数のピアツーピア (P2P) デバイスおよびインフラストラクチャ無線 LAN (WLAN) に同時にアソシエートしている場合があります。コントローラを使用して、Wi-Fi Direct クライアント ポリシーを WLAN 単位で設定できます。その際、Wi-Fi デバイスとインフラストラクチャ WLAN のアソシエーションを許可または禁止するか、WLAN に対して Wi-Fi Direct クライアント ポリシーをすべて無効にすることができます。

### Wi-Fi Direct クライアント ポリシーの制限

Wi-Fi Direct クライアント ポリシーは、ローカル モードの AP が含まれる WLAN のみに適用できます。

## Wi-Fi Direct クライアント ポリシーの設定 (GUI)

---

- ステップ1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ2 Wi-Fi Direct クライアント ポリシーを設定する WLAN の WLAN ID をクリックします。 [WLANs > Edit] ページが表示されます。
- ステップ3 [Advanced] タブをクリックします。
- ステップ4 [Wi-Fi Direct Clients Policy] ドロップダウン リストから、次のいずれかのオプションを選択します。
- [Disabled] : クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します
  - [Allow] : Wi-Fi Direct クライアントと WLAN のアソシエーションを許可します
  - [Not-Allow] : Wi-Fi Direct クライアントと WLAN のアソシエーションを禁止します
- ステップ5 [Apply] をクリックします。
- 

## Wi-Fi Direct クライアント ポリシーの設定 (CLI)

---

- ステップ1 次のコマンドを入力して、WLAN に Wi-Fi Direct クライアント ポリシーを設定します。
- ```
config wlan wifidirect {allow | disable | not-allow} wlan-id
```
- このコマンドの構文は次のとおりです。
- **allow** : Wi-Fi Direct クライアントと WLAN のアソシエーションを許可します
 - **disable** : WLAN の Wi-Fi Direct クライアント ポリシーを無効にし、すべての Wi-Fi Direct クライアントの認証を解除します
 - **not-allow** : Wi-Fi Direct クライアントと WLAN のアソシエーションを禁止します
 - *wlan-id* : WLAN ID
- ステップ2 次のコマンドを入力して、設定を保存します。
- ```
save config
```
-

## Wi-Fi Direct クライアント ポリシーの監視とトラブルシューティング (CLI)

- 次のコマンドを入力して、Wi-Fi Direct クライアント ポリシーの監視およびトラブルシューティングを行います。
  - **show wlan wifidirect *wlan-id*** : WLAN の Wi-Fi Direct クライアント ポリシーのステータスを表示します
  - **show client wifiDirect-stats** : アソシエートされているクライアントの合計数と、Wi-Fi Direct クライアント ポリシーが有効な場合に拒否されるクライアントの数が表示されます。







# 第 70 章

## Web 認証プロキシの設定

---

- [Web 認証プロキシについて](#), 635 ページ
- [Web 認証プロキシの設定 \(GUI\)](#), 636 ページ
- [Web 認証プロキシの設定 \(CLI\)](#), 637 ページ

### Web 認証プロキシについて

この機能を使用すると、ブラウザで手動 Web プロキシが有効になっているクライアントに対し、コントローラによる認証を強化することができます。ユーザのブラウザで、ポート番号 8080 または 3128 を使用して手動プロキシが設定されている場合、クライアントが URL を要求すると、コントローラは応答の Web ページで、プロキシ設定が自動的に検出されるようにインターネットのプロキシ設定を変更するようユーザに要求します。これにより、ブラウザの手動プロキシ設定情報が失われることはなくなります。ユーザはこの設定を有効にしたあと、Web 認証ポリシーを通じてネットワークにアクセスできます。この機能がポート 8080 および 3128 に提供されるのは、それらのポートが Web プロキシサーバで最も一般的に使用されているからです。



(注) Web 認証プロキシのリダイレクトポートは CPU ACL でブロックされません。Web 認証プロキシ設定の中で、ポート 8080、3128、および 1 つのランダムなポートをブロックするように CPU ACL が設定されていても、これらのポートはブロックされません。これは、クライアントが `webauth_req` 状態でない限り、Web 認証ルールは CPU ACL ルールよりも優先されるからです。

Web ブラウザに設定できる 3 種類のインターネット設定を次に示します。

- 自動検出
- システム プロキシ
- 手動

手動プロキシサーバ設定では、ブラウザはプロキシサーバの IP アドレスとポートを使用します。この設定がブラウザで有効になっている場合、ワイヤレスクライアントは、設定されたポート上の宛先プロキシサーバの IP アドレスと通信します。Web 認証シナリオでは、コントローラはこのようなプロキシポートをリッスンしないので、クライアントはコントローラとの TCP 接続を確立できません。ユーザは、認証用のログインページを表示できず、ネットワークにアクセスすることはできません。

ワイヤレスクライアントは、Web 認証された WLAN に入ると、URL にアクセスしようとします。クライアントのブラウザに手動プロキシが設定されている場合、クライアントから発信されるすべての Web トラフィックは、ブラウザに設定されたプロキシ IP およびポートに送信されます。

- TCP 接続は、クライアントと、コントローラがプロキシとして動作しているプロキシサーバの IP アドレスの間で確立されます。
- クライアントは DHCP 応答を処理し、コントローラから JavaScript ファイルを取得します。このスクリプトによって、そのセッションに関するクライアントのプロキシ設定はすべて無効になります。



(注) 外部クライアントに対しては、コントローラはログインページを現状のまま (JavaScript なしで) 送信します。

- プロキシ設定をバイパスする要求。そのあと、コントローラは Web リダイレクション、ログイン、認証を実行できます。
- クライアントがネットワークから出て独自のネットワークに戻った場合は、DHCP が更新され、クライアントはブラウザに設定された以前のプロキシ設定を引き続き使用します。
- 外部 DHCP サーバで Web 認証プロキシを使用する場合、該当するスコープの DHCP サーバで DHCP オプション 252 を設定する必要があります。オプション 252 の値の形式は `http://<virtual ip>/proxy.js` です。内部の DHCP サーバでは、追加設定は必要ありません。



(注) FIPS モードでセキュアな Web 認証を設定する場合は、ブラウザに Mozilla Firefox を使用することをお勧めします。

## Web 認証プロキシの設定 (GUI)

ステップ 1 [Controller] > [General] の順に選択します。

ステップ 2 [WebAuth Proxy Redirection Mode] ドロップダウンリストから、[Enabled] または [Disabled] を選択します。

ステップ 3 [WebAuth Proxy Redirection Port] テキストボックスに、Web 認証プロキシのポート番号を入力します。このテキストボックスでは、コントローラが Web 認証プロキシリダイレクションを実行するためにリッスンするポート番号を指定します。デフォルトでは、80、8080、および 3128 の 3 つのポートが想定され

ています。これら以外の値に Web 認証リダイレクション ポートを設定した場合は、その値を指定してください。

**ステップ 4** [Apply] をクリックします。

## Web 認証プロキシの設定 (CLI)

- 次のコマンドを入力して、Web 認証プロキシリダイレクションを有効にします。  
**config network web-auth proxy-redirect {enable | disable}**
- 次のコマンドを入力して、クライアントに対してセキュア Web (https) 認証を設定します。  
**config network web-auth secureweb {enable | disable}**  
デフォルトでは、クライアントのセキュア Web (https) 認証は有効になっています。



(注) **config network web-auth secureweb disable** コマンドを使用してクライアントのセキュア Web (https) 認証を禁止するように設定する場合、Cisco WLC をリブートして変更を適用する必要があります。

- 次のコマンドを入力して、Web 認証ポート番号を設定します。  
**config network web-auth port port-number**  
このパラメータでは、コントローラが Web 認証プロキシリダイレクションを実行するためにリッスンするポート番号を指定します。デフォルトでは、80、8080、および 3128 の 3 つのポートが想定されています。これら以外の値に Web 認証リダイレクション ポートを設定した場合は、その値を指定してください。
- 次のいずれかのコマンドを入力して、Web 認証プロキシ設定の現在のステータスを表示します。
  - **show network summary**
  - **show running-config**





# 第 71 章

## 意図的な悪用の検出

---

- [意図的な悪用の検出, 639 ページ](#)

### 意図的な悪用の検出

コントローラでは、潜在的な脅威を知らせる役割を果たす3つの意図的な悪用に関するアラームをサポートしています。これらはデフォルトで有効になっているため、コントローラ上での設定は不要です。

- **ASLEAP 検出**：コントローラは、攻撃者が LEAP クラック ツールを起動した場合にトラップを生成します。トラップメッセージは、コントローラのトラップ ログで確認できます。
- **疑似アクセス ポイント検出**：高密度アクセス ポイント環境でのアクセス ポイントアラームの誤作動を回避するために、コントローラは疑似アクセスポイント検出ロジックを調整します。
- **ハニーポット アクセス ポイント検出**：コントローラは、不正なアクセスポイントが管理対象 SSID を使用している場合にトラップ イベントを生成します（コントローラで設定された WLAN）。トラップメッセージは、コントローラのトラップ ログで確認できます。





## 第 **V** 部

### WLAN の使用

- [WLAN の設定, 643 ページ](#)
- [WLAN ごとのクライアント カウントの設定, 651 ページ](#)
- [DHCP の設定, 655 ページ](#)
- [DHCP スコープの設定, 661 ページ](#)
- [WLAN の MAC フィルタリングの設定, 665 ページ](#)
- [ローカル MAC フィルタの設定, 667 ページ](#)
- [タイムアウトの設定, 669 ページ](#)
- [DTIM period の設定, 673 ページ](#)
- [ピアツーピア ブロッキングの設定, 677 ページ](#)
- [レイヤ 2 セキュリティの設定, 681 ページ](#)
- [Static WEP と Dynamic WEP の両方をサポートする WLAN の設定, 695 ページ](#)
- [Sticky Key Caching の設定, 701 ページ](#)
- [CKIP の設定, 705 ページ](#)
- [レイヤ 3 セキュリティの設定, 709 ページ](#)
- [キャプティブ バイパスの設定, 713 ページ](#)
- [MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定, 715 ページ](#)

- QoS プロファイルの割り当て, 719 ページ
- QoS Enhanced BSS の設定, 725 ページ
- メディア セッション スヌーピングおよびレポートの設定, 729 ページ
- Key Telephone System-Based CAC の設定, 735 ページ
- ローミングしている音声クライアントのリアンカーの設定, 739 ページ
- シームレスな IPv6 モビリティの設定, 743 ページ
- Cisco Client Extensions の設定, 751 ページ
- リモート LAN の設定, 755 ページ
- AP グループの設定, 759 ページ
- RF プロファイルの設定, 767 ページ
- 802.1X 認証を使用した Web リダイレクトの設定, 777 ページ
- NAC アウトオブバンド統合の設定, 785 ページ
- パッシブクライアントの設定, 791 ページ
- クライアント プロファイルの設定, 797 ページ
- WLAN ごとの RADIUS 送信元サポートの設定, 801 ページ
- モバイル コンシェルジュの設定, 805 ページ
- 経路ローミングの設定, 821 ページ
- VLAN タギング 802.1Q-in-Q の設定, 825 ページ





# 第 72 章

## WLAN の設定

---

- [WLAN の前提条件](#), 643 ページ
- [WLAN の制約事項](#), 644 ページ
- [WLAN について](#), 645 ページ
- [WLAN の作成および削除 \(GUI\)](#), 645 ページ
- [WLAN の有効化および無効化 \(GUI\)](#), 647 ページ
- [WLAN の作成および削除 \(CLI\)](#), 647 ページ
- [WLAN の有効化および無効化 \(CLI\)](#), 648 ページ
- [WLAN の表示 \(CLI\)](#), 648 ページ
- [WLAN の検索 \(GUI\)](#), 648 ページ
- [インターフェイスへの WLAN の割り当て](#), 649 ページ
- [Network Access Identifier の設定 \(CLI\)](#), 649 ページ

### WLAN の前提条件

- 最大 16 個の WLAN を各アクセス ポイントグループにアソシエートし、各グループに個々のアクセス ポイントを割り当てることができます。各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイントグループに属する WLAN だけをアドバタイズします。アクセス ポイントグループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。
- コントローラが VLAN トラフィックを正常にルーティングできるように、WLAN と管理インターフェイスにはそれぞれ別の VLAN を割り当てておくことをお勧めします。
- コントローラでは、同じ Service Set Identifier (SSID) の WLAN を区別するために、異なる属性が使用されます。

- 同じ SSID、同じレイヤ 2 ポリシーの WLAN は、WLAN ID が 17 より小さい場合は作成できません。
- WLAN が異なる AP グループに追加される場合、17 より大きい ID で、同じ SSID と同じレイヤ 2 ポリシーを持つ 2 つの WLAN を使用できます。



(注) この要件によって、クライアントが同じアクセスポイント無線の SSID を検出することがないようにします。

## WLAN の制約事項

- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- WLAN 名と SSID は 32 文字以内にする必要があります。スペースは WLAN プロファイル名と SSID では許可されません。
- WLAN から VLAN0 へのマッピング、VLAN 1002~1006 のマッピングはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- OfficeExtend アクセス ポイントはすべて同じアクセス ポイント グループ内にあり、このグループに含まれる WLAN は最大 15 個にする必要があります。アクセス ポイント グループ内の OfficeExtend アクセス ポイントを持つコントローラは、パーソナルな SSID に対して割り当てられる WLAN が 1 つであるため、接続されている各 OfficeExtend アクセス ポイントに最大 15 個の WLAN しか公開しません。
- Cisco FLEX 7500 シリーズ コントローラは、中央でスイッチされる WLAN の 802.1x セキュリティ バリエーションをサポートしません。たとえば、次のような設定は中央でスイッチされる WLAN で使用できません。
  - 802.1x AKM を使用した WPA1/WPA2
  - CCKM を使用した WPA1/WPA2
  - Dynamic WEP
  - 条件付き webauth
  - スプラッシュ Web ページリダイレクト
- 上記の任意の組み合わせで WLAN を設定する場合、ローカル スイッチングを使用するように WLAN を設定する必要があります。
- EAP パススルーを使用する WLAN を設定する場合、および以前のコントローラ バージョンにダウングレードする場合は、ダウンロード プロセス中に XML 検証エラーが発生すること

があります。この問題は、EAP パススルーが旧リリースでサポートされていないために発生します。設定は、デフォルトのセキュリティ設定 (WPA2/802.1X) になります。



(注) OEAP 600 シリーズ アクセス ポイントでは、最大で 2 つの WLAN と 1 つのリモート LAN がサポートされます。3 つ以上の WLAN と 1 つのリモート LAN を設定した場合は、AP グループに 600 シリーズ アクセス ポイントを割り当てることができます。2 つの WLAN と 1 つのリモート LAN のサポートも AP グループに適用されますが、600 シリーズ OEAP がデフォルト グループにある場合、WLAN またはリモート LAN ID を 7 以下にする必要があります。

- WLAN のプロファイル名は、ローカルでスイッチされる WLAN で最大 31 文字です。中央でスイッチされる WLAN では、32 文字のプロファイル名を使用できます。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用している必要があります。



注意

一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この機能を使用する際は、十分注意してください。

## WLAN について

この機能を使用して、Lightweight アクセス ポイントに対して最大の WLAN を制御できます。各 WLAN には、別個の WLAN ID、別個のプロファイル名、および WLAN SSID があります。すべてのコントローラは接続された各アクセス ポイントに対して最大 16 の WLAN を公開しますが、サポートされる WLAN の最大数まで作成した後、それらの WLAN を選択的に公開し (アクセス ポイントグループを使用)、無線ネットワークをより効率的に管理するために、別のアクセス ポイントにそれらの WLAN をパブリッシュできます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、コントローラがアクセスする必要がある特定の無線ネットワークを識別します。

## WLAN の作成および削除 (GUI)

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

このページでは、コントローラ上で現在設定されているすべての WLAN が表示されます。各 WLAN について、WLAN ID、プロファイル名、タイプ、SSID、ステータス、およびセキュリティ ポリシーを表示できます。

WLAN の合計数がページの右上隅に表示されます。WLAN のリストが複数ページに渡る場合は、ページ番号のリンクをクリックすることで、目的のページにアクセスできます。

(注) WLAN を削除する場合は、削除する WLAN の青いドロップダウン矢印の上にカーソルを置いて、[Remove] を選択します。もしくは、削除する WLAN の左側のチェックボックスをオンにして、ドロップダウンリストから [Remove Selected] を選択して、[Go] をクリックします。決定を確認するメッセージが表示されます。確認して先に進むと、割り当てられているアクセスポイントグループおよびアクセスポイント無線からその WLAN が削除されます。

**ステップ 2** ドロップダウンリストから [Create New] を選択し、[Go] をクリックして新規の WLAN を作成します。[WLANs > New] ページが表示されます。

(注) コントローラのソフトウェアリリース 5.2 以降にアップグレードすると、コントローラによって default-group アクセスポイントグループが作成され、その中に、最初の 16 個の WLAN (1 ~ 16 の ID を持つ WLAN。ただし、設定された WLAN の数が 16 に満たない場合は 16 より少なくなります) が自動的に割り当てられます。このデフォルトのグループは変更できません (このグループに WLAN を追加したり、このグループから WLAN を削除することはできません)。先頭の 16 の WLAN が追加または削除されるたびに、グループの内容は動的に更新されます。アクセスポイントは、アクセスポイントグループに属していない場合には、デフォルトグループに割り当てられ、そのデフォルトグループ内の WLAN を使用します。アクセスポイントは、未定義のアクセスポイントグループ名を有するコントローラと join した場合、そのグループ名を保持しますが、default-group アクセスポイントグループ内の WLAN を使用します。

**ステップ 3** [Type] ドロップダウンリストから、[WLAN] を選択して WLAN を作成します。

(注) 有線ゲスト ユーザー用にゲスト LAN を作成する場合は、[Guest LAN] を選択します。

**ステップ 4** [Profile Name] テキストボックスに、この WLAN に割り当てるプロファイル名を 32 文字以内で入力します。プロファイル名は固有である必要があります。

**ステップ 5** [WLAN SSID] テキストボックスに、この WLAN に割り当てる SSID を 32 文字以内で入力します。

**ステップ 6** [WLAN ID] ドロップダウンリストから、この WLAN の ID 番号を選択します。

(注) Cisco OEAP 600 がデフォルトグループにある場合は、WLAN/リモート LAN ID を ID 7 以下に設定する必要があります。

**ステップ 7** [Apply] をクリックして、変更を確定します。[WLANs > Edit] ページが表示されます。

(注) 編集する WLAN の ID 番号をクリックすることにより、[WLANs] ページから [WLANs > Edit] ページを開くこともできます。

**ステップ 8** [General] タブ、[Security] タブ、[QoS] タブおよび [Advanced] タブ上でパラメータを使用してこの WLAN を設定します。WLAN の特定の機能を設定する手順については、この章の後の項を参照してください。

**ステップ 9** [General] タブの [Status] チェックボックスをオンにして、この WLAN を有効にします。WLAN に対する設定変更が終了するまで、チェックボックスをオフにしておいてください。

**ステップ 10** [Apply] をクリックして、変更を確定します。

**ステップ 11** [Save Configuration] をクリックして、変更を保存します。

## WLAN の有効化および無効化 (GUI)

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。  
このページでは、コントローラ上で現在設定されているすべての WLAN が表示されます。
- ステップ 2** また、[WLANs] ページから、有効化または無効化する WLAN の左側のチェックボックスをオンにして、ドロップダウンリストから [Enable Selected] または [Disable Selected] を選択し、[Go] をクリックすることで、WLAN を有効化または無効化します。
- ステップ 3** [Apply] をクリックします。
- 

## WLAN の作成および削除 (CLI)

- 次のコマンドを入力して、新しい WLAN を作成します。

```
config wlan create wlan_id {profile_name | foreign_ap} ssid
```



(注) ssid を指定しない場合、**profile\_name** パラメータがプロファイル名と SSID の両方に対して使用されます。



(注) 設定ウィザードで WLAN 1 を作成した場合、これは有効にされた状態で作成されています。設定が完了するまでは、無効にしてください。**config wlan create** コマンドを使用して WLAN を新しく作成する場合は、無効モードで作成されます。設定が終了するまでは、無効のままにしてください。

- 次のコマンドを入力して、WLAN を削除します。

```
config wlan delete {wlan_id | foreign_ap}
```



(注) アクセスポイントグループに割り当てられている WLAN を削除しようとすると、エラーメッセージが表示されます。そのまま続行すると、アクセスポイントグループとアクセスポイントの無線から WLAN が削除されます。

## WLAN の有効化および無効化 (CLI)

- 次のコマンドを入力して、WLAN を有効にします (たとえば、WLAN に対する変更が終了した後)。

```
config wlan enable {wlan_id | foreign_ap | all}
```



(注) コマンドが失敗した場合は、エラーメッセージ (「Request failed for wlan 10 - Static WEP key size does not match 802.1X WEP key size」など) が表示されます。

- 次のコマンドを入力して、WLAN を無効にします (たとえば、WLAN を変更する前)。 **config wlan disable** {wlan\_id | foreign\_ap | all}  
値は次のとおりです。

*wlan\_id* は、WLAN ID (1 ~ 512) です。

**foreign\_ap** は、サードパーティ アクセス ポイントです。

**all** は、すべての WLAN です。



(注) 管理インターフェイスおよび AP マネージャインターフェイスが同じポートにマップされており、いずれも同じ VLAN のメンバである場合は、WLAN を無効にしてから、ポートマッピングをいずれかのインターフェイスに変更する必要があります。管理インターフェイスと AP マネージャインターフェイスが別々の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

## WLAN の表示 (CLI)

- 次のコマンドを入力して、既存の WLAN のリストを表示し、有効か無効かを確認します。

```
show wlan summary
```

## WLAN の検索 (GUI)

**ステップ 1** [WLANs] ページで、[Change Filter] をクリックします。[Add WLANs] ダイアログボックスが表示されます。

**ステップ 2** 次のいずれかの操作を行います。

- プロファイル名に基づいて WLAN を検索するには、[Profile Name] チェックボックスをオンにして、目的のプロファイル名を編集ボックスに入力します。

- SSID に基づいて WLAN を検索するには、[SSID] チェックボックスをオンにして、目的の SSID を編集ボックスに入力します。
- ステータスに基づいて WLAN を検索するには、[Status] チェックボックスをオンにして、ドロップダウン リストから [Enabled] または [Disabled] を選択します。

**ステップ 3** [Find] をクリックします。検索条件に一致した WLAN だけが [WLANs] ページに表示され、ページの上部の [Current Filter] フィールドに、リストを生成するために使用された検索条件（たとえば、None、Profile Name:user1、SSID:test1、Status:disabled）が指定されます。

（注） 設定されている検索条件をクリアして、WLAN の全リストを表示するには、[Clear Filter] をクリックします。

## インターフェイスへの WLAN の割り当て

WLAN をインターフェイスに割り当てるには、次のコマンドを使用します。

- 次のコマンドを入力して、インターフェイスに WLAN を割り当てます。

```
config wlan interface {wlan_id|foreignAp} interface_id
```

- WLAN を特定のインターフェイスに割り当てるには、*interface\_id* オプションを使用します。
- サードパーティアクセスポイントを使用するには、*foreignAp* オプションを使用します。

- インターフェイス割り当てステータスを確認するには、**show wlan summary** コマンドを入力します。

## Network Access Identifier の設定 (CLI)

各 WLAN プロファイル、VLAN インターフェイス、または AP グループのネットワーク アクセスサーバ ID (NAS-ID) を設定できます。RADIUS サーバがカスタマイズされた認証応答を送信できるように、異なるグループにユーザを分類する認証要求を介して、コントローラによって RADIUS サーバに NAS-ID が送信されます。

AP グループに対して NAS-ID を設定すると、その NAS-ID は、WLAN プロファイルまたは VLAN インターフェイスに対して設定されている NAS-ID をオーバーライドします。WLAN プロファイルに対して NAS-ID を設定すると、その NAS-ID は、VLAN インターフェイスに対して設定されている NAS-ID をオーバーライドします。

- 次のコマンドを入力して、WLAN プロファイルの NAS-ID を設定します。

```
config wlan nasid {nas-id-string|none} wlan-id
```

- 次のコマンドを入力して、VLAN インターフェイスの NAS-ID を設定します。

**config interface nasid** {*nas-id-string* | **none**} *interface-name*

- 次のコマンドを入力して、AP グループの NAS-ID を設定します。

**config wlan apgroup nasid** {*nas-id-string* | **none**} *apgroup-name*

コントローラが RADIUS サーバと通信するときに、NAS-ID 属性は AP グループ、WLAN、または VLAN インターフェイスで設定された NAS-ID に置き換えられます。

AP グループ、WLAN、または VLAN インターフェイスのコントローラ上で設定されている NAS-ID が認証に使用されます。NAS-ID の設定はコントローラ全体には伝播されません。





# 第 73 章

## WLAN ごとのクライアント カウントの設定

- [WLAN ごとのクライアント カウントの設定に関する制約事項](#), 651 ページ
- [WLAN ごとのクライアント カウントの設定について](#), 652 ページ
- [WLAN ごとのクライアント カウントの設定 \(GUI\)](#), 652 ページ
- [WLAN ごとの最大クライアント数の設定 \(CLI\)](#), 652 ページ
- [WLAN ごとの各 AP 無線に対する最大クライアント数の設定 \(GUI\)](#), 653 ページ
- [WLAN ごとの各 AP 無線に対する最大クライアント数の設定 \(CLI\)](#), 653 ページ
- [クライアントの認証解除 \(CLI\)](#), 653 ページ

### WLAN ごとのクライアント カウントの設定に関する制約事項

- WLAN ごとのクライアントの最大数機能は、FlexConnect ローカル認証を使用する場合、サポートされません。
- WLAN ごとのクライアントの最大数機能は、接続モードのアクセス ポイントでのみサポートされます。
- WLAN が接続クライアントの最大数の制限に達しているか、AP 無線および新しいクライアントが WLAN に参加しようとしている場合、クライアントは既存のクライアントが切断されるまで WLAN に接続できません。
- ローミングクライアントは新しいクライアントと見なされます。クライアントの接続数の最大制限に到達している WLAN に対して新しいクライアントは、既存のクライアントが切断されたときにのみ接続できます。



(注) サポートされているクライアント数の詳細については、コントローラの製品データシートを参照してください。

## WLAN ごとのクライアントカウントの設定について

WLANに接続できるクライアントの数の制限を設定できます。これは、コントローラに接続できるクライアントの数の制限があるシナリオで役立ちます。たとえば、コントローラが WLAN 上の最大 256 個のクライアントに対応でき、これらのクライアントが企業ユーザ（従業員）およびゲストユーザ間で共有される場合について考えます。特定の WLAN にアクセス可能なゲストクライアントの数の制限を設定できます。WLANごとに設定できるクライアントの数は、使用しているプラットフォームによって異なります。

## WLAN ごとのクライアントカウントの設定（GUI）

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
  - ステップ 2 クライアント数を制限する WLAN の ID 番号をクリックします。[WLANs>Edit] ページが表示されます。
  - ステップ 3 [Advanced] タブをクリックします。
  - ステップ 4 [Maximum Allowed Clients] テキストボックスに許可されるクライアントの最大数を入力します。
  - ステップ 5 [Apply] をクリックします。
  - ステップ 6 [Save Configuration] をクリックします。
- 

## WLAN ごとの最大クライアント数の設定（CLI）

- 
- ステップ 1 次のコマンドを入力して、最大クライアント数を設定する WLAN ID を確認します。  
**show wlan summary**  
リストから WLAN ID を取得します。
  - ステップ 2 次のコマンドを入力して、WLAN ごとの最大クライアント数を設定します。  
**config wlan max-associated-clients max-clients wlan-id**
-

## WLAN ごとの各 AP 無線に対する最大クライアント数の設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 クライアント数を制限する WLAN の ID 番号をクリックします。[WLANs>Edit] ページが表示されます。
- ステップ 3 [Advanced] タブで、アクセス ポイント無線あたり使用できるクライアントの最大数を [Maximum Allowed Clients Per AP Radio] テキスト ボックスに入力します。最大 200 のクライアントを設定できます。
- ステップ 4 [Apply] をクリックします。
- 

## WLAN ごとの各 AP 無線に対する最大クライアント数の設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、無線ごとの最大クライアント数を設定する WLAN ID を確認します。
- ```
show wlan summary
```
- リストから WLAN ID を取得します。
- ステップ 2 次のコマンドを入力して、WLAN ごとの最大クライアント数を設定します。
- ```
config wlan max-radio-clients client_count
```
- 最大 200 のクライアントを設定できます。
- ステップ 3 **show 802.11a** コマンドを入力して、設定済みの最大関連クライアントを表示します。
- 

## クライアントの認証解除 (CLI)

コントローラを使用して、ユーザ名、IP アドレス、または MAC アドレスに基づいてクライアントを認証解除できます。同じユーザ名を持つ複数のクライアントセッションがある場合、ユーザ名に基づいてすべてのクライアントセッションを認証解除できます。異なるインターフェイスにわたって重複した IP アドレスがある場合、MAC アドレスを使用してクライアントを認証解除できます。



(注) コントローラ GUI を使用してクライアントを認証解除することはできません。

- **config client deauthenticate** {*mac-addr* | *ipv4-addr* | *ipv6-addr* | *user-name*}





# 第 74 章

## DHCP の設定

---

- [DHCP for WLANs の設定に関する制限](#), 655 ページ
- [Dynamic Host Configuration Protocol について](#), 655 ページ
- [DHCP の設定 \(GUI\)](#), 657 ページ
- [DHCP の設定 \(CLI\)](#), 659 ページ
- [DHCP のデバッグ \(CLI\)](#), 659 ページ

### DHCP for WLANs の設定に関する制限

- 内部 DHCP サーバのコントローラでは、Cisco Aironet 600 シリーズ OfficeExtend アクセス ポイントはサポートされません。
- 内部 DHCP サーバは Cisco Flex 7500 シリーズ コントローラではサポートされません。回避策として、外部 DHCP サーバを使用できます。
- ローカルスイッチングと集中管理 DHCP 機能が有効な WLAN では、静的 IP アドレスを持つクライアントは許可されません。集中管理 DHCP を有効にすると、DHCP の必要なオプションが内部的に有効になります。

### Dynamic Host Configuration Protocol について

WLAN では、同じ Dynamic Host Configuration Protocol (DHCP) サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないように設定できます。DHCP サーバには、内部 DHCP サーバと外部 DHCP サーバの 2 つのタイプがあります。

#### 内部 DHCP サーバ

コントローラは、内部 DHCP サーバを持っています。このサーバは、一般的に、DHCP サーバを持たないブランチ オフィスで使用されます。無線ネットワークには、通常、コントローラと同

じ IP サブネット上にある最大 10 台のアクセス ポイントが含まれます。内部サーバは、ワイヤレス クライアント、ダイレクトコネク トアクセス ポイント、およびアクセス ポイントからリレーされた DHCP 要求に対して DHCP アドレスを提供します。Lightweight アクセス ポイントのみサポートされています。内部 DHCP サーバを使用する場合は、コントローラの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

内部サーバでは、DHCP オプション 43 はサポートされていません。したがって、アクセス ポイントは、ローカル サブネット ブロードキャスト、ドメイン ネーム システム (DNS)、またはブライミングなどの別の方法を使用してコントローラの管理インターフェイスの IP アドレスを見つける必要があります。

内部 DHCP サーバプールは、そのコントローラの無線クライアントだけをサポートし、他のコントローラのクライアントはサポートしません。また、内部 DHCP サーバは、無線クライアントだけをサポートし、有線クライアントをサポートしません。

クライアントがコントローラの内部 DHCP サーバを使用する場合、IP アドレスは、再起動後には保持されません。その結果、複数のクライアントに同じ IP アドレスが割り当てられることがあります。IP アドレスの競合を解決するには、クライアントは既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。有線ゲスト クライアントは常に、ローカルまたは外部 コントローラに接続されたレイヤ 2 にあります。




---

(注) DHCPv6 は内部 DHCP サーバではサポートされません。

---

## 外部 DHCP サーバ

オペレーティング システムは、DHCP リレーをサポートする業界標準の外部 DHCP サーバを使用することにより、ネットワークに対しては DHCP リレーとして機能し、クライアントに対しては DHCP サーバとして機能するように設計されています。これは、各 コントローラは、DHCP サーバに対しては DHCP リレー エージェントとして機能し、無線クライアントに対しては仮想 IP アドレスでの DHCP サーバとして機能することを意味します。

コントローラは DHCP サーバから取得したクライアント IP アドレスをキャプチャするため、コントローラ内、コントローラ間、およびサブネット間でのクライアントローミング時に、各クライアントに対して同じ IP アドレスが保持されます。




---

(注) 外部 DHCP サーバは DHCPv6 をサポートします。

---

## DHCP 割り当て

DHCP はインターフェイスごとに、または WLAN ごとに設定できます。特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することをお勧めします。

個々のインターフェイスに DHCP サーバを割り当てることができます。プライマリおよびセカンダリ DHCP サーバの管理インターフェイス、AP マネージャインターフェイス、動的インターフェ

イスの設定、DHCP サーバをイネーブルまたはディセーブルするためのサービスポートインターフェイスの設定を行うことができます。WLAN で DHCP サーバを定義することもできます。この場合、サーバは、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きします。

### セキュリティに関する注意事項

高度なセキュリティが必要な場合は、すべてのクライアントが DHCP サーバから IP アドレスを取得するように設定してください。この要件を適用するために、DHCP アドレスですべての WLAN を設定できます。Assignment Required 設定で設定して、クライアントの固定 IP アドレスが禁止されるようにします。DHCP Addr. Assignment Required が選択されている場合、クライアントは DHCP を使って IP アドレスを取得する必要があります。固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。クライアントの DHCP プロキシとして動作するコントローラが、DHCP トラフィックを監視します。



(注) 無線による管理をサポートする WLAN では、管理（デバイスサービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。

セキュリティが多少劣ってもかまわない場合は、DHCP Addr. Assignment Required を無効に設定して WLAN を作成できます。その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。



(注) DHCP アドレス 有線ゲスト LAN に対する Assignment Required は、サポートされていません。

個別の WLAN は、[DHCP アドレス割り当て必須 (DHCP Address Assignment Required)] を無効にして作成できます。これは、コントローラの DHCP プロキシがイネーブルの場合だけです。DHCP プロキシをディセーブルにする必要があるプライマリ/セカンダリ コンフィギュレーションの DHCP サーバを定義しないでください。このような WLAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。これらの WLAN は、無線接続による管理をサポートしていません。

## DHCP の設定 (GUI)

管理インターフェイス、AP マネージャ インターフェイス、または動的インターフェイスにプライマリ DHCP サーバを設定するには、「ポートとインターフェイスの設定」の章を参照してください。

内部DHCPサーバを使用する場合は、コントローラの管理インターフェイスのIPアドレスをDHCPサーバのIPアドレスとして設定する必要があります。

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** インターフェイスを割り当てる WLAN の ID 番号をクリックします。[WLANs > Edit] ([General]) ページが表示されます。
- ステップ 3** [General] タブの [Status] チェックボックスをオフにし、[Apply] をクリックして WLAN を無効にします。
- ステップ 4** WLAN の ID 番号を再度クリックします。
- ステップ 5** [General] タブの [Interface] ドロップダウンリストから、この WLAN で使用するプライマリ DHCP サーバを設定したインターフェイスを選択します。
- ステップ 6** [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。
- ステップ 7** WLAN 上で、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きする DHCP サーバを定義する場合、[DHCP Server Override] チェックボックスをオンにして、[DHCP Server IP Addr] テキストボックスに目的の DHCP サーバの IP アドレスを入力します。チェックボックスはデフォルトでは、無効になっています。
- (注) DHCP の設定には、DHCP サーバのオーバーライドではなく、特定のインターフェイスに割り当てられたプライマリの DHCP アドレスを使用する方式が優先されます。
  - (注) DHCP サーバのオーバーライドはデフォルト グループにのみ適用できます。
  - (注) WLAN で DHCP サーバのオーバーライドが有効になっており、コントローラの DHCP プロキシが有効になっている場合、WLAN にマッピングされるインターフェイスが DHCP サーバの IP アドレスを持っているか、または WLAN に DHCP サーバの IP アドレスを設定する必要があります。
- ステップ 8** すべてのクライアントが DHCP サーバから IP アドレスを取得するよう設定するには、[DHCP Addr. Assignment Required] チェックボックスをオンにします。この機能が有効になっている場合、固定 IP アドレスを持つクライアントはネットワーク上で許可されません。デフォルト値はディセーブルです。
- (注) DHCP Addr. Assignment Required は、有線ゲスト LAN ではサポートされていません。
- ステップ 9** [Apply] をクリックします。
- ステップ 10** [General] タブの [Status] チェックボックスをオンにし、[Apply] をクリックして WLAN をもう一度有効にします。
- ステップ 11** [Save Configuration] をクリックします。
-



## DHCP の設定 (CLI)

ステップ 1 次のコマンドを入力して、WLAN を無効にします。

```
config wlan disable wlan-id
```

ステップ 2 この WLAN で使用するプライマリ DHCP サーバを設定したインターフェイスを指定するには、次のコマンドを入力します。

```
config wlan interface wlan-id interface_name
```

ステップ 3 WLAN 上で、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きする DHCP サーバを定義するには、次のコマンドを入力します。

```
config wlan dhcp_server wlan-id dhcp_server_ip_address
```

(注) DHCP の設定には、DHCP サーバのオーバーライドではなく、特定のインターフェイスに割り当てられたプライマリの DHCP アドレスを使用する方式が優先されます。オーバーライド機能を有効にした場合、**show wlan** コマンドを使用して DHCP サーバが WLAN に割り当てられていることを確認できます。

(注) WLAN で DHCP サーバのオーバーライドが有効になっており、コントローラの DHCP プロキシが有効になっている場合、WLAN にマッピングされるインターフェイスが DHCP サーバの IP アドレスを持っているか、または WLAN に DHCP サーバの IP アドレスを設定する必要があります。

ステップ 4 次のコマンドを入力して、WLAN を再び有効にします。

```
config wlan enable wlan-id
```

## DHCP のデバッグ (CLI)

DHCP をデバッグするには、次のコマンドを使用します。

- **debug dhcp packet {enable | disable}** : DHCP パケットのデバッグを有効または無効にします。
- **debug dhcp message {enable | disable}** : DHCP エラー メッセージのデバッグを有効または無効にします。
- **debug dhcp service-port {enable | disable}** : サービス ポート上の DHCP パケットのデバッグを有効または無効にします。





# 第 75 章

## DHCP スコープの設定

---

- [DHCP スコープの設定に関する制限](#), 661 ページ
- [DHCP スコープについて](#), 661 ページ
- [DHCP スコープの設定 \(GUI\)](#), 661 ページ
- [DHCP スコープの設定 \(CLI\)](#), 663 ページ

### DHCP スコープの設定に関する制限

最大 16 の DHCP スコープを設定できます。

### DHCP スコープについて

コントローラには組み込みの DHCP リレーエージェントがあります。ただし、別個の DHCP サーバを持たないネットワーク セグメントが必要な場合、コントローラに IP アドレスとサブネットマスクを無線クライアントに割り当てる組み込みの DHCP スコープを設定できます。一般に、1 つのコントローラには、それぞれが各種 IP アドレスを指定する 1 つまたは複数の DHCP スコープを設定できます。

DHCP スコープは内部 DHCP が機能するために必要となります。コントローラで DHCP が定義されると、管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスのプライマリ DHCP サーバの IP アドレスをコントローラの管理インターフェイスにポイントすることができます。

### DHCP スコープの設定 (GUI)

- 
- ステップ 1** [Controller] > [Internal DHCP Server] > [DHCP Scope] を選択して、[DHCP Scopes] ページを開きます。このページには、これまでに設定されたすべての DHCP スコープが表示されます。

(注) 既存の DHCP スコープを削除するには、そのスコープの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

- ステップ 2** 新しい DHCP スコープを追加するには、[New] をクリックします。[DHCP Scope > New] ページが表示されます。
- ステップ 3** [Scope Name] テキスト ボックスに、新しい DHCP スコープの名前を入力します。
- ステップ 4** [Apply] をクリックします。DHCP Scopes ページが再度表示されたら、新しいスコープの名前をクリックします。[DHCP Scope > Edit] ページが表示されます。
- ステップ 5** [Pool Start Address] テキスト ボックスに、クライアントに割り当てられた範囲の開始 IP アドレスを入力します。
- (注) このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。
- ステップ 6** [Pool End Address] テキスト ボックスに、クライアントに割り当てられた範囲の終了 IP アドレスを入力します。
- (注) このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。
- ステップ 7** [Network] テキスト ボックスに、この DHCP スコープの対象となるネットワークの名前を入力します。この IP アドレスは、[Interfaces] ページで設定されている、ネットマスクが適用された管理インターフェイスによって使用されます。
- ステップ 8** [Netmask] テキスト ボックスに、すべての無線クライアントに割り当てられたサブネット マスクを入力します。
- ステップ 9** [Lease Time] テキスト ボックスに、IP アドレスをクライアントに対して許可する時間 (0 ~ 65536 秒) を入力します。
- ステップ 10** [Default Routers] テキスト ボックスに、コントローラに接続しているオプションルータの IP アドレスを入力します。各ルータには、DHCP フォワーディングエージェントを含める必要があります。これにより、単一コントローラで複数のコントローラのクライアントを処理できます。
- ステップ 11** [DNS Domain Name] テキスト ボックスに、1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションのドメイン ネーム システム (DNS) ドメイン名を入力します。
- ステップ 12** [DNS Servers] テキスト ボックスに、オプションの DNS サーバの IP アドレスを入力します。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。
- ステップ 13** [Netbios Name Servers] テキスト ボックスに、Internet Naming Service (WINS) サーバなど、オプションの Microsoft Network Basic Input Output System (NetBIOS) ネーム サーバの IP アドレスを入力します。
- ステップ 14** [Status] ドロップダウン リストから、[Enabled] を選択してこの DHCP スコープを有効にするか、または [Disabled] を選択して無効にします。
- ステップ 15** [Apply] をクリックして、変更を確定します。
- ステップ 16** [Save Configuration] をクリックして、変更を保存します。
- ステップ 17** [DHCP Allocated Leases] を選択して、無線クライアントの残りのリース時間を表示します。[DHCP Allocated Lease] ページが表示され、無線クライアントの MAC アドレス、IP アドレス、および残りのリース時間が示されます。

## DHCP スコープの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、新しい DHCP スコープを作成します。  
**config dhcp create-scope scope**  
 (注) DHCP スコープを削除する場合は、次のコマンドを入力します。 **config dhcp delete-scope scope**
- ステップ 2** クライアントに割り当てられた範囲の開始および終了 IP アドレスを指定するには、次のコマンドを入力します。  
**config dhcp address-pool scope start end**  
 (注) このプールは、各 DHCP スコープで一意でなければならず、ルータまたは他のサーバの固定 IP アドレスを含めることはできません。
- ステップ 3** この DHCP スコープの対象となるネットワーク（ネットマスクが適用された管理インターフェイスによって使用される IP アドレス）およびすべての無線クライアントに割り当てられたサブネット マスクを指定するには、次のコマンドを入力します。  
**config dhcp network scope network netmask**
- ステップ 4** 次のコマンドを入力して、クライアントに IP アドレスを許容する時間（0 ～ 65536 秒）を指定します。  
**config dhcp lease scope lease\_duration**
- ステップ 5** コントローラに接続されているオプション ルータの IP アドレスを指定するには、次のコマンドを入力します。  
**config dhcp default-router scope router\_1 [router\_2] [router\_3]**  
 各ルータには、DHCP フォワーディング エージェントを含める必要があります。これにより、単一コントローラで複数のコントローラのクライアントを処理できます。
- ステップ 6** 次のコマンドを入力して、1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションのドメイン ネーム システム (DNS) ドメイン名を指定します。  
**config dhcp domain scope domain**
- ステップ 7** 次のコマンドを入力して、オプションの DNS サーバの IP アドレスを指定します。  
**config dhcp dns-servers scope dns1 [dns2] [dns3]**  
 各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。
- ステップ 8** 次のコマンドを入力して、Internet Naming Service (WINS) サーバなど、オプションの Microsoft Network Basic Input Output System (NetBIOS) ネーム サーバの IP アドレスを指定します。  
**config dhcp netbios-name-server scope wins1 [wins2] [wins3]**
- ステップ 9** 次のコマンドを入力して、この DHCP スコープを有効または無効にします。  
**config dhcp {enable | disable} scope**

**ステップ 10** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 11** 次のコマンドを入力して、設定されている DHCP スコープのリストを表示します。

**show dhcp summary**

以下に類似した情報が表示されます。

```
Scope Name Enabled Address Range
Scope 1 No 0.0.0.0 -> 0.0.0.0
Scope 2 No 0.0.0.0 -> 0.0.0.0
```

**ステップ 12** 次のコマンドを入力して、特定のスコープの DHCP 情報を表示します。

**show dhcp scope**

以下に類似した情報が表示されます。

```
Enabled..... No
Lease Time..... 0
Pool Start..... 0.0.0.0
Pool End..... 0.0.0.0
Network..... 0.0.0.0
Netmask..... 0.0.0.0
Default Routers..... 0.0.0.0 0.0.0.0 0.0.0.0
DNS Domain.....
DNS..... 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers..... 0.0.0.0 0.0.0.0 0.0.0.0
```

---



## 第 76 章

# WLAN の MAC フィルタリングの設定

- [MAC フィルタリングの制限, 665 ページ](#)
- [WLAN の MAC フィルタリングについて, 665 ページ](#)
- [MAC フィルタリングの有効化, 665 ページ](#)

## MAC フィルタリングの制限

- MAC フィルタはゲスト LAN 用に設定できません。

## WLAN の MAC フィルタリングについて

クライアント許可または管理者許可に MAC フィルタリングを使用する場合は、WLAN レベルで先に有効にしておく必要があります。任意の WLAN でローカル MAC アドレス フィルタリングを使用する予定がある場合は、この項のコマンドを使用して WLAN の MAC フィルタリングを設定します。

## MAC フィルタリングの有効化

WLAN 上で MAC フィルタリングを有効にするには、次のコマンドを使用します。

- MAC フィルタリングを有効にするには、**config wlan mac-filtering enable wlan\_id** コマンドを入力します。
- WLAN の MAC フィルタリングが有効になっていることを確認するには、**show wlan** コマンドを入力します。

MAC フィルタリングを有効にすると、WLAN に追加した MAC アドレスにのみ WLAN への join が許可されます。追加されていない MAC アドレスは、WLAN への join が許可されません。







# 第 77 章

## ローカル MAC フィルタの設定

- [ローカル MAC フィルタの設定に関する前提条件](#), 667 ページ
- [ローカル MAC フィルタについて](#), 667 ページ
- [ローカル MAC フィルタの設定 \(CLI\)](#), 667 ページ

### ローカル MAC フィルタの設定に関する前提条件

WLAN で AAA を有効にして、インターフェイス名を上書きする必要があります。

### ローカル MAC フィルタについて

コントローラには MAC フィルタリング機能が組み込まれています。これは、RADIUS authorization サーバで提供されるものとよく似ています。

### ローカル MAC フィルタの設定 (CLI)

- コントローラに MAC フィルタ エントリを作成するには、**config macfilter add *mac\_addr* *wlan\_id* [*interface\_name*] [*description*] [*IP\_addr*]** コマンドを入力します。  
次のパラメータはオプションです。
  - *mac\_addr* : クライアントの MAC アドレス。
  - *wlan\_id* : クライアントがアソシエートしている WLAN ID。
  - *interface\_name* : インターフェイスの名前。このインターフェイス名は WLAN に設定されたインターフェイスを上書きするために使用されます。
  - *description* : インターフェイスの簡単な説明。二重引用符で囲みます (たとえば、"Interface1") 。

° *IP\_addr* : 上記の *mac addr* 値で指定される MAC アドレスを持つパッシブクライアントに使用される IP アドレス。

- IP アドレスを既存の MAC フィルタ エントリに割り当てるには、**config macfilter ip-address *mac\_addr* *IP\_addr*** コマンドを入力します (**config macfilter add** コマンドで割り当てられていない場合)。
- MAC アドレスが WLAN に割り当てられていることを確認するには、**show macfilter** コマンドを入力します。



---

(注) MAC フィルタリングが設定されている場合、コントローラはまず RADIUS サーバを使用してワイヤレスクライアントを認証しようとします。ローカル MAC フィルタリングが試行されるのは、RADIUS サーバがタイムアウトしたか、RADIUS サーバが設定されていないために、RADIUS サーバが検出されない場合のみです。

---



# 第 78 章

## タイムアウトの設定

---

- [無効なクライアントのタイムアウトの設定, 669 ページ](#)
- [セッションタイムアウトの設定, 670 ページ](#)
- [ユーザアイドルタイムアウトの設定, 671 ページ](#)

### 無効なクライアントのタイムアウトの設定

#### 無効なクライアントのタイムアウトの設定について

無効なクライアントに対してタイムアウトを設定できます。アソシエートしようとした際に認証で3回失敗したクライアントは、それ以降のアソシエーションの試みでは自動的に無効にされます。タイムアウト期間が経過すると、クライアントは認証の再試行を許可され、アソシエートすることができます。このとき、認証に失敗すると再び排除されます。無効なクライアントに対してタイムアウトを設定するには、次のコマンドを使用します。

#### 無効なクライアントのタイムアウトの設定 (CLI)

- 無効なクライアントにタイムアウトを設定するには、**config wlan exclusionlist wlan\_id timeout** コマンドを入力します。有効なタイムアウトの範囲は、1 ~ 2147483647 秒です。値 0 を指定すると、クライアントが永久的に無効になります。
- 現在のタイムアウトを確認するには、**show wlan** コマンドを入力します。

## セッションタイムアウトの設定

### セッションタイムアウトについて

WLAN にセッション タイムアウトを設定できます。セッション タイムアウトとは、クライアントセッションが再認証を要求することなくアクティブである最大時間を指します。

### セッションタイムアウトの設定 (GUI)

設定可能なセッション タイムアウトの範囲は次のとおりです。

- 802.1x は 300 ～ 86400。
- 他のすべてのセキュリティ タイプは 0 ～ 65535。



(注) セッション タイムアウトを 0 に設定すると、オープンシステムの場合はセッション タイムアウトが無効になり、その他のシステム タイプでは 86400 秒になります。

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 セッション タイムアウトを割り当てる WLAN の ID 番号をクリックします。
- ステップ 3 [WLANs>Edit] ページが表示されたら、[Advanced] タブを選択します。[WLANs>Edit] ([Advanced]) ページが表示されます。
- ステップ 4 この WLAN のセッション タイムアウトを設定するには、[Enable Session Timeout] チェックボックスをオンにします。チェックボックスをオフにするということは、0 に設定することと同じであり、これは各セッション タイプのセッション タイムアウトの最大値です。
- ステップ 5 [Apply] をクリックして、変更を確定します。
- ステップ 6 [Save Configuration] をクリックして、変更を保存します。

### セッションタイムアウトの設定 (CLI)

- ステップ 1 WLAN の無線クライアントにセッション タイムアウトを設定するには、次のコマンドを入力します。  
**config wlan session-timeout wlan\_id timeout**  
デフォルト値は、レイヤ 2 セキュリティ タイプが [802.1X]、[Static WEP+802.1X]、[WPA+WPA2 with 802.1X]、[CCKM]、または [802.1X+CCKM] 認証キー管理の場合は 1800 秒、その他すべてのレイヤ 2 セ

セキュリティタイプ ([Open WLAN]/[CKIP]/[Static WEP]) については 0 秒です。値 0 はタイムアウトなしに相当します。

**ステップ 2** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 3** WLAN の現在のセッションタイムアウト値を表示するには、次のコマンドを入力します。

```
show wlan wlan_id
```

以下に類似した情報が表示されます。

```
WLAN Identifier..... 9
Profile Name..... test12
Network Name (SSID)..... test12
...
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... 1800 seconds
...
```

## ユーザアイドルタイムアウトの設定

### WLAN ごとのユーザアイドルタイムアウトについて

これは、コントローラのすべての WLAN プロファイルに適用可能なユーザアイドルタイムアウト機能の現在の実装に対する拡張です。この機能拡張により、個々の WLAN プロファイルに対してユーザアイドルタイムアウトを設定できます。このユーザアイドルタイムアウトは、この WLAN プロファイルに属するすべてのクライアントに適用できます。

クライアントが指定されたユーザアイドルタイムアウト中にデータのしきい値のクォータを送信せず、クライアントが非アクティブであると見なされ、認証解除された場合、しきい値によってトリガーされるタイムアウトを設定することもできます。クライアントが送信するデータがユーザアイドルタイムアウト内で指定されたしきい値のクォータを超える場合、クライアントはアクティブであると見なされ、コントローラは別のタイムアウト期間中に更新します。しきい値のクォータがタイムアウト期間内に達した場合、タイムアウト期間が更新されます。

ユーザのアイドルタイムアウトを 120 秒に指定し、ユーザのアイドルしきい値を 10 メガバイトに指定するとします。120 秒が経過した後、クライアントが 10 メガバイトのデータを送信しない場合、そのクライアントは非アクティブであると見なされ、認証解除されます。クライアントが 120 秒の間に 10 メガバイトに達した場合、タイムアウト期間が更新されます。

### WLAN ごとのユーザアイドルタイムアウトの設定 (CLI)

- 次のコマンドを入力して、WLAN に対してユーザアイドルタイムアウトを設定します。

**config wlan usertimeout** *timeout-in-seconds wlan-id*

- 次のコマンドを入力して、WLAN に対してユーザアイドルしきい値を設定します。

**config wlan user-idle-threshold** *value-in-bytes wlan-id*



## 第 79 章

# DTIM period の設定

- [DTIM Period](#) について, 673 ページ
- [DTIM period の設定 \(GUI\)](#) , 674 ページ
- [DTIM period の設定 \(CLI\)](#) , 674 ページ

## DTIM Period について

802.11 ネットワークでは、Lightweight アクセス ポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的に送信します。アクセスポイントでビーコンがブロードキャストされると、DTIM period で設定した値に基づいて、バッファされたブロードキャストフレームおよびマルチキャストフレームが送信されます。この機能により、ブロードキャストデータやマルチキャストデータが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1 (ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信) または 2 (ビーコン1回おきに送信) のいずれかに設定されます。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを毎秒 5 回送信します。これらの設定はいずれも、ブロードキャストフレームおよびマルチキャストフレームの頻度を想定する、Voice over IP (VoIP) を含むアプリケーションに適しています。

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます (255 回のビーコンごとにブロードキャストフレームおよびマルチキャストフレームを送信します)。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセスポイントは、バッファされたブロードキャストフレームおよびマルチキャストフレームを 10 秒ごとに 1 回送信します。このレートにより省電力クライアントで、ブロードキャストとマルチキャストをリッスンし、ウェイクアップするまでのスリープ状態が長くなり、バッテリー寿命を長くできます。



(注) ビーコン期間は、コントローラでミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位 (TU) (1 TU = 1.024 ミリ秒) に、内部的に変換されます。Cisco の 802.11n アクセスポイントでは、この値は直近の 17 TU の倍数に丸められます。たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャストメッセージとマルチキャストメッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

特定の WLAN で 802.11 無線ネットワークの DTIM 期間を設定できます。たとえば、音声 WLAN とデータ WLAN に異なる DTIM 値を設定できます。

## DTIM period の設定 (GUI)

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 DTIM period を設定する WLAN の ID 番号をクリックします。
- ステップ 3 [Status] チェックボックスをオフにしてこの WLAN を無効にします。
- ステップ 4 [Apply] をクリックします。
- ステップ 5 [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。
- ステップ 6 [DTIM Period] で [802.11a/n/ac] テキストボックスと [802.11b/g/n] テキストボックスに 1 ~ 255 までの値を入力します。デフォルト値は 1 (ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信) です。
- ステップ 7 [Apply] をクリックします。
- ステップ 8 [General] タブを選択して、[WLANs > Edit] ([General]) ページを開きます。
- ステップ 9 [Status] チェックボックスをオンにして、この WLAN を再び有効にします。
- ステップ 10 [Save Configuration] をクリックします。

## DTIM period の設定 (CLI)

- ステップ 1 次のコマンドを入力して、WLAN を無効にします。  
`config wlan disable wlan_id`
- ステップ 2 次のコマンドを入力して、特定の WLAN の 802.11 無線ネットワークの DTIM period を設定します。  
`config wlan dtim {802.11a | 802.11b} dtim wlan_id`



*dtim* の値は、1 ~ 255 (両端の値を含む) です。デフォルト値は 1 (ブロードキャストフレームおよびマルチキャストフレームはビーコンのたびに送信) です。

**ステップ 3** 次のコマンドを入力して、WLAN を再び有効にします。

```
config wlan enable wlan_id
```

**ステップ 4** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 5** 次のコマンドを入力して、DTIM period を確認します。

```
show wlan wlan_id
```

---





## 第 80 章

# ピアツーピア ブロッキングの設定

- [ピア ツー ピア ブロッキングの制約事項, 677 ページ](#)
- [ピアツーピア ブロッキングについて, 678 ページ](#)
- [ピアツーピア ブロッキングの設定 \(GUI\) , 678 ページ](#)
- [ピアツーピア ブロッキングの設定 \(CLI\) , 679 ページ](#)

## ピア ツー ピア ブロッキングの制約事項

- 4.2 以前のコントローラのソフトウェア リリースでは、コントローラはアドレス解決プロトコル (ARP) 要求ストリームを転送します (他のすべてのトラフィックと同様)。コントローラのソフトウェア リリース 4.2 以降では、ARP 要求は、ピアツーピア ブロッキングに設定された動作に従ってダイレクトされます。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- 以前のリリースから、グローバルピアツーピアブロッキングをサポートしているコントローラソフトウェアリリース 4.2 以降にアップグレードすると、各 WLAN はトラフィックをアップストリーム VLAN に転送するピアツーピア ブロッキング処理で設定されます。
- FlexConnect では、特定の FlexConnect AP または AP のサブセットのみにソリューションのピアツーピア ブロッキング設定を適用することはできません。これは、SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- 中央スイッチングのクライアントに対応する統合ソリューションではピアツーピアアップストリーム転送がサポートされます。しかし、これは FlexConnect ソリューションでサポートされません。これはピア ツー ピア ドロップとして処理され、クライアント パケットはドロップされます。
- 中央スイッチングのクライアントに対応する統合ソリューションでは、別々の AP にアソシエートされたクライアントに対するピアツーピア ブロッキングがサポートされます。ただし、このソリューションでは、同一の AP に接続するクライアントだけがターゲットとなります。FlexConnect ACL は、この制限の回避策として使用できます。

## ピアツーピア ブロッキングについて

ピアツーピア ブロッキングが個別の WLAN に対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピアブロッキング設定を継承します。ピアツーピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがコントローラ内でローカルにブリッジされたり、コントローラによってドロップされたり、またはアップストリーム VLAN へ転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートされたクライアントに対して、ピアツーピアブロッキングがサポートされます。

WLAN ごとに、ピアツーピア設定がコントローラによって FlexConnect AP にプッシュされます。4.2 以前のコントローラのソフトウェア リリースでは、ピアツーピアブロッキングはすべての WLAN 上のすべてのクライアントにグローバルに適用され、それによって同じ VLAN 上の 2 つのクライアント間のトラフィックが、コントローラでブリッジされるのではなく、アップストリーム VLAN に転送されていました。この動作の結果、スイッチはパケットを受け取ったのと同じポートからパケットを転送しないため、通常アップストリームスイッチでトラフィックがドロップされます。

## ピアツーピア ブロッキングの設定 (GUI)

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** ピアツーピアブロッキングを設定する WLAN の ID 番号をクリックします。

**ステップ 3** [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。

**ステップ 4** [P2P Blocking] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [Disabled] : ピアツーピアブロッキングを無効にして、可能な場合にはコントローラ内でトラフィックをローカルにブリッジします。これは、デフォルト値です。

(注) コントローラ内の VLAN でトラフィックがブリッジされることはありません。

- [Drop] : コントローラでパケットを破棄するようにします。

- [Forward-UpStream] : パケットがアップストリーム VLAN に転送されるようにします。これらのパケットに対して行われる動作は、コントローラよりも上流にあるデバイスにより決定されます。

(注) FlexConnect ローカルスイッチングに設定された WLAN でピアツーピアブロッキングを有効にするには、[P2P Blocking] ドロップダウン リストから [Drop] を選択し、[FlexConnect Local Switching] チェックボックスをオンにします。

**ステップ 5** [Apply] をクリックして、変更を確定します。

**ステップ 6** [Save Configuration] をクリックして、変更を保存します。

## ピアツーピア ブロッキングの設定 (CLI)

- ステップ 1** WLAN のピアツーピア ブロッキングを設定するには、次のコマンドを入力します。  
**config wlan peer-blocking {disable | drop | forward-upstream} wlan\_id**
- ステップ 2** 次のコマンドを入力して、変更を保存します。  
**save config**
- ステップ 3** 次のコマンドを入力して、WLAN のピアツーピア ブロッキングのステータスを参照します。  
**show wlan wlan\_id**

以下に類似した情報が表示されます。

```
WLAN Identifier..... 1
Profile Name..... test
Network Name (SSID)..... test
Status..... Enabled
...
...
...
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
Local EAP Authentication..... Disabled
```





# 第 81 章

## レイヤ 2 セキュリティの設定

---

- レイヤ 2 セキュリティの前提条件, 681 ページ
- Static WEP キーの設定 (CLI) , 682 ページ
- 802.1X 動的キーおよび許可の設定 (CLI) , 682 ページ
- 802.11r BSS の高速移行の設定, 683 ページ
- 802.1X 認証への MAC 認証フェールオーバーの設定, 689 ページ
- 802.11w の設定, 690 ページ

### レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN は、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーを使用してする必要があります。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし (オープン WLAN)
- Static WEP または 802.1X



---

(注) Static WEP と 802.1X は両方とも、ビーコン応答とプローブ応答で同じビットによってアドバタイズされるので、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、Static WEP と 802.1X の両方を使用できません。

---

- WPA/WPA2



- (注) 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ2つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access (WPA) /Temporal Key Integrity Protocol (WPA) で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。

## Static WEP キーの設定 (CLI)

コントローラでは、アクセスポイント上で Static WEP キーを制御できます。WLAN の Static WEP を設定するには、次のコマンドを使用します。

- 次のコマンドを入力して、802.1X 暗号化を無効にします。

```
config wlan security 802.1X disable wlan_id
```

- 次のコマンドを入力して、40/64 ビットまたは 104/128 ビット WEP キーを設定します。

```
config wlan security static-wep-key encryption wlan_id {40 | 104} {hex | ascii} key key_index
```

- 40/64 ビットまたは 104/128 ビット暗号化を指定するには、**40** または **104** オプションを使用します。デフォルトの設定は、104/128 です。
- WEP キーの文字形式を指定するには、**hex** または **ascii** オプションを使用します。
- 40 ビット/64 ビット WEP キーの場合は 10 桁の 16 進数 (0 ~ 9、a ~ f、または A ~ F の組み合わせ) または印刷可能な 5 つの ASCII 文字を入力します。または、104 ビット/128 ビット キーの場合は 26 桁の 16 進数または 13 の ASCII 文字を入力します。
- キー インデックス (キー スロットとも呼ばれます) を入力します。デフォルト値は 0 で、これはキー インデックス 1 に相当します。有効な値は 0 ~ 3 (キー インデックス 1 ~ 4) です。

## 802.1X 動的キーおよび許可の設定 (CLI)

コントローラでは、アクセスポイント上で Extensible Authentication Protocol (EAP; 拡張認証プロトコル) を使用する 802.1X Dynamic WEP キーを制御できます。また、WLAN の 802.1X ダイナミック キー設定をサポートしています。



- (注) Lightweight アクセスポイントとワイヤレスクライアントで LEAP を使用するには、CiscoSecure Access Control Server (ACS) を設定する際に RADIUS サーバタイプとして [Cisco-Aironet] を選択することを確認します。

- 各無線 LAN のセキュリティ設定を確認するには、次のコマンドを入力します。



**show wlan wlan\_id**

新しい WLAN のデフォルトのセキュリティ設定は、ダイナミック キーが有効な 802.1X です。レイヤ 2 の堅牢なポリシーを維持するには、802.1X を WLAN 上で設定したままにします。

- 次のコマンドを入力して、802.1X 暗号化を無効または有効にします。

**config wlan security 802.1X {enable | disable} wlan\_id**

802.1X 認証を有効にした後、コントローラから、ワイヤレスクライアントと認証サーバとの間で EAP 認証パケットが送信されます。このコマンドにより、すべての EAP タイプのパケットは、コントローラとの送受信が可能になります。



(注) コントローラは、同じ WLAN で Web 認証と 802.1X 認証の両方を実行します。クライアントは、最初に 802.1x で認証されます。認証が成功すると、クライアントは、Web 認証クレデンシャルを提供する必要があります。Web 認証が成功すると、クライアントは RUN 状態に移行します。

- 次のコマンドを入力して、WLAN の 802.1X 暗号化レベルを変更します。

**config wlan security 802.1X encryption wlan\_id [0 | 40 | 104]**

- 802.1X 暗号化なしを指定するには、**0** オプションを使用します。
- 40/64 ビット暗号化を指定するには、**40** オプションを使用します。
- 104/128 ビット暗号化を指定するには、**104** オプションを使用します（これは、デフォルトの暗号化設定です）。

## 802.11r BSS の高速移行の設定

### 802.11r 高速移行の制約事項

- この機能はメッシュ アクセス ポイントでサポートされません。
- この機能は FlexConnect モードのアクセス ポイントでサポートされません。
- FlexConnect モードのアクセス ポイントの場合、
  - 802.11r 高速移行は、中央でスイッチされる WLAN とローカルにスイッチされる WLAN でのみサポートされます。
  - この機能は、ローカル認証が有効になっている WLAN ではサポートされません。
- この機能は、Cisco 600 シリーズ OfficeExtend アクセス ポイントなどの Linux ベースの AP ではサポートされません。

- 802.11r クライアント アソシエーションは、スタンドアロン モードのアクセス ポイントではサポートされません。
- 802.11r 高速ローミングは、スタンドアロン モードのアクセス ポイントではサポートされません。
- ローカル認証 WLAN と中央認証 WLAN 間の 802.11r 高速ローミングはサポートされていません。
- クライアントがスタンドアロン モードの Over-the-DS 事前認証を使用する場合、802.11r 高速ローミングはサポートされません。
- EAP LEAP 方式はサポートされません。 WAN リンク遅延は、最大 2 秒間にアソシエーション時間を抑制します。
- スタンドアロン AP からクライアントへのサービスは、セッション タイマーが切れるまでサポートされます。
- TSpec は 802.11r 高速ローミングではサポートされません。 したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。 音声またはデータの最大遅延を確認する必要があります。 コントローラは、Over-the-Air および Over-the-DS の両方の方式をローミングする間、802.11r 高速移行の認証要求を処理します。
- この機能は、オープンで WPA2 設定の WLAN でのみサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange (RSN IE) の解析を担当するサブリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。 この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。 ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。 802.11r 対応クライアントは、802.11r と 802.11i の両方の認証キー管理スイートが有効にされている WLAN の 802.11i クライアントとしてアソシエートできます。

回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作するようにするか、またはアップグレードすることです。 そうすることで、レガシークライアントは、802.11r 対応 WLAN と正常にアソシエートできます。

もう 1 つの回避策は、同じ名前異なるセキュリティ設定 (FT および非 FT) の 2 つの SSID を持つことです。
- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。 また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能 (DoS) 攻撃を回避するため、各 コントローラでは、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。

## 802.11r の高速移行について

高速ローミングの IEEE 標準である 802.11r は、クライアントがターゲット AP にローミングする前でも、新しい AP との最初のハンドシェイクが実行される、高速移行 (FT) と呼ばれるローミングの新しい概念が導入されています。初期ハンドシェイクによって、クライアントと AP が事前に Pairwise Transient Key (PTK) 計算をできるようになります。これらの PTK キーは、クライアントが新しいターゲット AP の再アソシエーション要求または応答の交換をした後で、クライアントと AP に適用されます。

802.11r は、次の 2 通りのローミングを提供します。

- 無線
- Over-the-DS (分散システム)

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN 設定には、FT (高速移行) と呼ばれる、新しい認証キー管理 (AKM) タイプが含まれています。

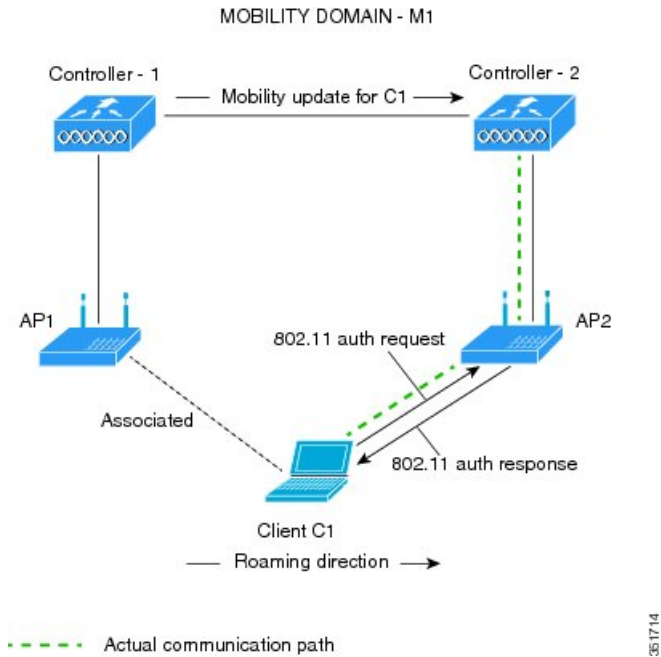
### クライアントのローミング方法

FT プロトコルを使用して現在の AP からターゲット AP に移動するクライアントでは、メッセージ交換は次の 2 つの方法のいずれかを使用して行われます。

- 無線：クライアントは、FT 認証アルゴリズムを使用する IEEE 802.11 認証を使用して、ターゲット AP と直接通信を行います。
- Over-the-DS：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との間の通信は、クライアントと現在の AP 間の FT アクションフレームで実行されてから、コントローラによって送信されます。

この図は、Over the Air クライアントのローミングを設定するときに行われるメッセージ交換のシーケンスを示します。

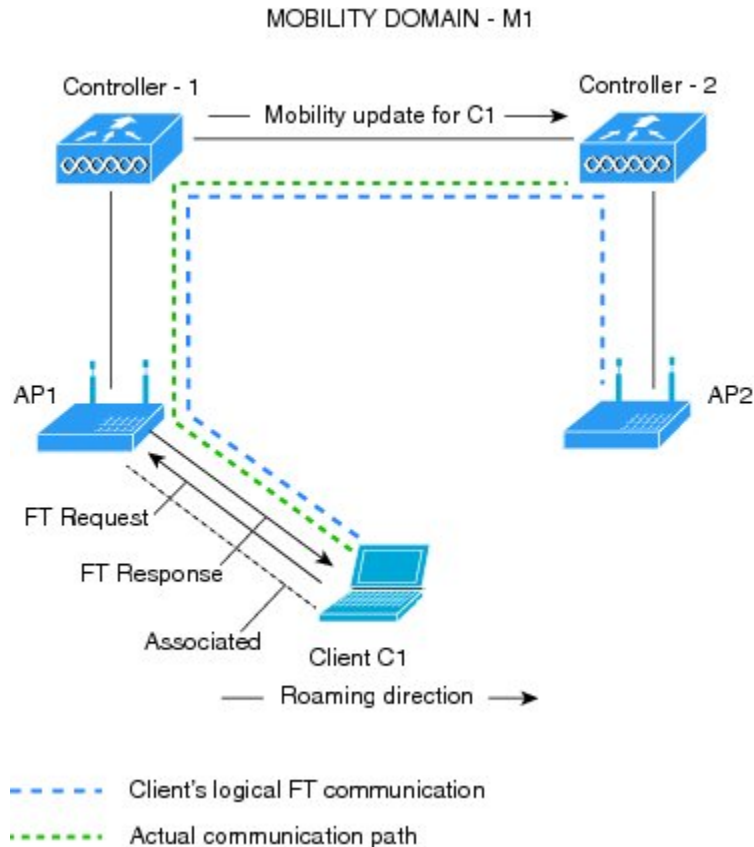
図 46 : Over the Air クライアント ローミング設定時のメッセージ交換



351714

この図は、Over the DS クライアントのローミングを設定するときに実行されるメッセージ交換のシーケンスを示します。

図 47: *Over the DS* クライアント ローミング設定時のメッセージ交換



051715

## 802.11r の高速移行の設定 (GUI)

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 WLAN ID をクリックして、[WLANs > Edit] ページを開きます。
- ステップ 3 [Security] > [Layer 2] タブを選択します。
- ステップ 4 [Layer 2 Security] ドロップダウンリストから、[WPA+WPA2] を選択します。  
高速移行の認証キーの管理パラメータが表示されます。
- ステップ 5 [Fast Transition] チェックボックスを選択または選択解除して、WLAN の高速移行を有効または無効にします。
- ステップ 6 [Over the DS] チェックボックスを選択または選択解除して、分散システム経由の高速移行を有効または無効にします。  
このオプションは、高速移行を有効にした場合だけ使用できます。

- ステップ 7** [Reassociation Timeout] ボックスに、AP へのクライアントの再アソシエーション試行がタイムアウトになる秒数を入力します。  
有効範囲は 1 ~ 100 秒です。  
このオプションは、高速移行を有効にした場合だけ使用できます。
- ステップ 8** 認証キー管理の場合は、[FT 802.1X]、または [FT PSK] を選択します。対応するチェックボックスを選択するかまたは選択解除して、キーを有効または無効にします。[FT PSK] チェックボックスを選択する場合、[PSK Format] ドロップダウンリストから [ASCII] または [Hex] を選択して、キー値を入力します。
- ステップ 9** [WPA gtk-randomize State] ドロップダウンリストで [Enable] または [Disable] を選択して、WPA グループの一時的なキー (GTK) randomize state を設定します。
- ステップ 10** [Apply] をクリックして設定値を保存します。
- 

## 802.11r の高速移行の設定 (CLI)

---

- ステップ 1** 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft {enable | disable} wlan-id** コマンドを使用します。  
デフォルトで、高速移行は無効です。
- ステップ 2** 分散システム上の 802.11r 高速移行パラメータを有効または無効にするには、**config wlan security ft over-the-ds {enable | disable} wlan-id** コマンドを使用します。  
デフォルトで、分散システム上の高速移行は無効です。
- ステップ 3** 事前共有キー (PSK) を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-psk {enable | disable} wlan-id** コマンドを使用します。  
デフォルトで、PSK を使用した認証キー管理は無効です。
- ステップ 4** 802.1X を使用した高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft-802.1X {enable | disable} wlan-id** コマンドを使用します。  
デフォルトで、802.1X を使用した認証キー管理は無効です。
- ステップ 5** 802.11r 高速移行の再アソシエーションタイムアウトを有効または無効にするには、**config wlan security ft reassociation-timeout timeout-in-seconds wlan-id** コマンドを使用します。  
有効範囲は 1 ~ 100 秒です。再アソシエーションタイムアウトのデフォルト値は 20 秒です。
- ステップ 6** 分散システム上の高速移行の認証キー管理を有効または無効にするには、**config wlan security wpa akm ft over-the-ds {enable | disable} wlan-id** コマンドを使用します。  
デフォルトで、分散システム上の高速移行の認証キー管理は無効です。

- ステップ 7** クライアントの高速移行の設定を表示するには、**show client detailed *client-mac*** コマンドを使用します。
- ステップ 8** WLAN の高速移行の設定を表示するには、**show wlan *wlan-id*** コマンドを使用します。
- ステップ 9** 高速移行イベントのデバッグを有効または無効にするには、**debug ft events {enable | disable}** コマンドを使用します。
- ステップ 10** 高速移行のキー生成のデバッグを有効または無効にするには、**debug ft keys {enable | disable}** コマンドを使用します。

## 802.11r BSS の高速移行のトラブルシューティング

症状	解決策
非 802.11r レガシー クライアントはすでに接続していません。	WLAN で FT が有効であるかどうかを確認します。その場合、非 FT WLAN が作成される必要があります。
WLAN を設定する場合、FT 設定オプションは表示されません。	WPA2 を使用されているかどうかを確認します (802.1x/PSK)。FT は WPA2 SSID およびオープン SSID だけでサポートされます。
802.11r クライアントは、新しいコントローラにレイヤ 2 のローミングを実行するときに、再認証するとおもわれます。	コントローラの GUI で、[WLANs] > [WLAN Name] > [Security] > [Layer 2] と移動して、再認証タイムアウトがデフォルトの 20 よりも小さくなっているかどうか確認します。

## 802.1X 認証への MAC 認証フェールオーバーの設定

クライアントに対する Static WEP による MAC 認証が失敗したときに、802.1X 認証を開始するようにコントローラを設定できます。RADIUS サーバが、クライアントを認証解除する代わりにクライアントからのアクセス要求を拒否した場合、コントローラは 802.1X 認証を受けることをクライアントに強制できます。クライアントが 802.1X 認証にも失敗した場合、クライアントは認証解除されます。

MAC 認証が成功し、クライアントが 802.1X 認証を要求する場合、クライアントがデータトラフィックの送信を許可されるには、802.1X 認証をパスする必要があります。クライアントが 802.1X 認証を選択しない場合、クライアントが MAC 認証にパスすれば、クライアントは認証を宣言されます。

## 802.1X 認証への MAC 認証フェールオーバーの設定 (GUI)

- 
- ステップ 1 [WLANs] > [WLAN ID] を選択して、[WLANs > Edit] ページを開きます。
- ステップ 2 [Security] タブで、[Layer 2] タブをクリックします。
- ステップ 3 [MAC Filtering] チェックボックスを選択します。
- ステップ 4 [Mac Auth or Dot1x] チェックボックスをオンにします。
- 

## 802.1X 認証への MAC 認証フェールオーバーの設定 (CLI)

---

802.1X 認証への MAC 認証フェールオーバーを設定するには、次のコマンドを入力します。

```
config wlan security 802.1X on-macfilter-failure {enable | disable} wlan-id
```

---

## 802.11w の設定

### 802.11w の制約事項

- Cisco の従来の管理フレーム保護は 7.4 リリースで実装されている 802.11w 標準には関連しません。
- 802.11w 標準は FlexConnect の動作が設定されたものを除くすべての 802.11n 対応 AP でサポートされます。
- 802.11w 標準は、Cisco ワイヤレス LAN コントローラのモデルシリーズ、2500、5500、8500、および WiSM2 でサポートされています。  
802.11w 標準は、Cisco ワイヤレス LAN コントローラのモデル、Flex 7500 と仮想 Wireless LAN Controller でサポートされていません。
- 802.11w はオープン WLAN、WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用されていません。
- 802.11w が設定された WLAN では、WPA2-PSK または WPA2-802.1x セキュリティを設定する必要があります。



## 802.11w に関する情報

Wi-Fiは、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャストメディアです。認証/認証解除、アソシエーション/ディスアソシエーション、ビーコンおよびプローブなどの制御/管理フレームは、無線クライアントによって、APを選択し、ネットワークサービスのセッションを開始するために使用されます。

機密保持レベルを提供する暗号化可能なデータトラフィックとは異なり、これらのフレームは、すべてのクライアントによって解釈されることが必要であり、したがってオープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。たとえば、攻撃者はクライアントとAPの間のセッションを切断するために、APから管理フレームをスプーフィングする可能性があります。

管理フレーム保護のための802.11w標準が7.4リリースに実装されています。

802.11wプロトコルは、管理フレーム保護（PMF）サービスによって保護された一連の強力な管理フレームにのみ適用されます。これらには、ディスアソシエーション、認証解除、ロバスタクションフレームが含まれます。

したがって、ロバスタクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトラム管理
- QoS
- DLS
- ブロック ACK
- 無線測定
- 高速 BSS 移行
- SA クエリー
- 保護されたデュアルパブリックアクション
- ベンダー固有保護

802.11wが無線メディアで実行されると、次のことが行われます。

- ディスアソシエーションフレームと認証解除フレームに対して、（MIC情報要素を含めることにより）APの暗号保護によるクライアント保護が追加されます。これによって、DoS攻撃でのスプーフが防止されます。
- アソシエーションの復帰期間とSAクエリーの手順から構成されるセキュリティアソシエーション（SA）ティアダウン保護メカニズムを追加することによって、インフラストラクチャの保護が追加され、スプーフィングされた要求によるすでに接続済みのクライアントの切断が防止されます。

## 802.11w の設定 (GUI)

- 
- ステップ 1** [WLANs] > [WLAN ID] の順に選択して、[WLANs > Edit] ページを開きます。
- ステップ 2** [Security] タブで、[Layer 2] セキュリティ タブを選択します。
- ステップ 3** [Layer 2 Security] ドロップダウン リストから、[WPA+WPA2] を選択します。  
802.11w IGTK キーはフォーウェイ ハンドシェイクを使用して生成されます。つまり、レイヤ 2 で WPA2 セキュリティ用に設定された WLAN でのみ使用できます。
- (注) WPA2 は必須であり、暗号化タイプは AES である必要があります。TKIP は無効です。
- ステップ 4** ドロップダウン リストから PMF 状態を選択します。  
次のオプションを使用できます。
- [Disabled] : WLAN での 802.11w MFP 保護を無効にします。
  - [Optional] : クライアントが 802.11w をサポートしている場合に使用します。
  - [Required] : 802.11w をサポートしていないクライアントが WLAN とアソシエートできないようにします。
- ステップ 5** PMF 状態を [Optional] または [Required] のいずれかとして選択する場合、次を行います。
- a) [Comeback Timer] ボックスに、Association Comeback の間隔をミリ秒単位で入力します。これは、有効なセキュリティ アソシエーションの後に、アクセス ポイントがクライアントと再度アソシエーションする期間です。
  - b) [SA Query Timeout] ボックスに、Security Association (SA) クエリーがタイムアウトするまでの最大時間を入力します。
- ステップ 6** [Authentication Key Management] セクションで、次の手順を実行します。
- a) [PMF 802.1X] チェックボックスをオンまたはオフにして、管理フレームを保護するために 802.1X 認証を設定します。
  - b) [PMF PSK] チェックボックスをオンまたはオフにして、PMF 用に事前共有されているキーを設定します。PSK フォーマットには ASCII または 16 進数のいずれかを選択し、PSK を入力します。
- ステップ 7** [Apply] をクリックします。
- ステップ 8** [Save Configuration] をクリックします。
- 

## 802.11w の設定 (CLI)

- 次のコマンドを入力して、PMF の 802.1X 認証を設定します。  
**config wlan security wpa akm pmf 802.1x {enable | disable} wlan-id**
- 次のコマンドを入力して、PMF の事前共有キーのサポートを設定します。

**config wlan security wpa akm pmf psk {enable | disable} wlan-id**

- 完了しない場合、次のコマンドを入力して、WLAN の事前共有キーを設定します。  
**config wlan security wpa akm psk set-key {ascii | hex} psk wlan-id**
- 次のコマンドを入力して、保護された管理フレームを設定します。  
**config wlan security pmf {disable | optional | required} wlan-id**
- 次のコマンドを入力して、Association Comeback の時間設定を構成します。  
**config wlan security pmf association-comeback timeout-in-seconds wlan-id**
- 次のコマンドを入力して、SA クエリー リトライ タイムアウト設定を構成します。  
**config wlan security pmf saquery-retrytimeout timeout-in-milliseconds wlan-id**
- 次のコマンドを入力して、WLAN の 802.11w 設定ステータスを表示します。  
**show wlan wlan-id**
- 次のコマンドを入力して、PMF のデバッグを設定します。  
**debug pmf events {enable | disable}**





## 第 82 章

# Static WEP と Dynamic WEP の両方をサポートする WLAN の設定

- [Static および Dynamic WEP の設定に関する制約事項, 695 ページ](#)
- [Static WEP と Dynamic WEP の両方をサポートする WLAN について, 696 ページ](#)
- [WPA1+WPA2 の設定, 698 ページ](#)

## Static および Dynamic WEP の設定に関する制約事項

- OEAP 600 シリーズはクライアントの高速ローミングをサポートしません。デュアルモードの音声クライアントは、OEAP602 アクセス ポイントの 2 つのスペクトラム間をローミングするときに、コール品質が低下します。1 帯域だけで接続するために、音声デバイスを 2.4 GHz または 5.0 GHz 設定することを推奨します。
- コントローラ ソフトウェアは、CCX バージョン 1 ~ 5 をサポートします。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。コントローラは、クライアントデータベースにクライアントの CCX バージョンを格納し、これを使用してクライアントの機能を制限します。CCKMを使用するには、クライアントでCCXv4 またはv5をサポートする必要があります。CCXの詳細については、「Cisco Client Extensions の設定」の項を参照してください。
- 複数の VLAN クライアントが WGB でサポートされる統合アーキテクチャでは、WEP 暗号化が WGB で有効である場合、暗号化の暗号スイートおよび WEP キーをグローバルに設定する必要があります。設定しない場合、有線 VLAN クライアントのマルチキャストトラフィックが失敗します。

## Static WEP と Dynamic WEP の両方をサポートする WLAN について

Static WEP キーをサポートする WLAN は 4 つまで設定できます。また、これらすべての Static WEP WLAN に Dynamic WEP も設定できます。Static WEP と Dynamic WEP を両方サポートする WLAN を設定する際の留意事項は次のとおりです。

- Static WEP キーおよび Dynamic WEP キーは、同じ長さである必要があります。
- Static WEP と Dynamic WEP の両方をレイヤ 2 セキュリティ ポリシーとして設定する場合は、他のセキュリティ ポリシーを指定できません。つまり、Web 認証を設定できません。ただし、Static WEP と Dynamic WEP のいずれかをレイヤ 2 セキュリティ ポリシーとして設定する場合は、Web 認証を設定できます。

## WPA1 と WPA2

Wi-Fi 保護アクセス (WPA または WPA1) および WPA2 は、無線 LAN システム用のデータ保護とアクセス コントロールを提供する Wi-Fi Alliance の規格ベースのセキュリティ ソリューションです。WPA1 は、IEEE 802.11i 規格に準拠していますが、規格の承認前に実装されたものです。これに対して、WPA2 は、承認された IEEE 802.11i 規格が Wi-Fi Alliance によって実装されています。

WPA1 のデフォルトでは、データの保護に Temporal Key Integrity Protocol (TKIP) および Message Integrity Check (MIC) が使用されますが、WPA2 では Counter Mode with Cipher Block Chaining Message Authentication Code Protocol を使用したより強力な Advanced Encryption Standard 暗号化アルゴリズム (AES-CCMP) が使用されます。WPA1 および WPA2 のデフォルトでは、両方とも 802.1X を使用して認証キー管理を行います。ただし、次のオプションも使用できます。

- **802.1X** : IEEE によって定義された無線 LAN セキュリティの規格。802.1X for 802.11、または単に 802.1X と呼ばれます。802.1X をサポートするアクセス ポイントは、無線ネットワークを介して通信を行う相手となるワイヤレスクライアントおよび認証サーバ (RADIUS サーバなど) との間のインターフェイスとして機能します。[802.1X] が選択されている場合は、802.1X クライアントのみがサポートされます。
- **PSK** : PSK (WPA 事前共有キーまたは WPA パスフレーズとも呼ばれます) を選択した場合は、事前共有キー (またはパスフレーズ) を設定する必要があります。このキーは、クライアントと認証サーバの間で Pairwise Master Key (PMK; ペアワイズマスターキー) として使用されます。
- **CCKM** : Cisco Centralized Key Management (CCKM) では、迅速なキーの再生成技術を使用しています。この技術を使用すると、クライアントは、通常 150 ミリ秒 (ms) 以下で、コントローラを経由せずにあるアクセス ポイントから別のアクセス ポイントにローミングできます。CCKM により、クライアントが新しいアクセス ポイントと相互に認証を行い、再アソシエーション時に新しいセッションキーを取得するために必要な時間が短縮されます。CCKM の迅速かつ安全なローミングでは、無線 VoIP、Enterprise Resource Planning (ERP)、Citrix ベースのソリューションなどの時間依存型のアプリケーションにおいて、認識できるほどの

遅延は発生しません。CCKM は、CCXv4 に準拠する機能です。CCKM が選択されている場合は、CCKM クライアントのみがサポートされます。

CCKM を有効にすると、アクセスポイントの動作は、高速ローミングのコントローラと次の点で異なります。

- クライアントから送信されるアソシエーション要求の Robust Secure Network Information Element (RSN IE) で CCKM が有効になっているものの、CCKM IE がエンコードされておらず、PMKID だけが RSN IE でエンコードされている場合、コントローラは完全な認証を行いません。代わりに、コントローラは PMKID を検証し、フォーウェイハンドシェイクをします。
  - クライアントから送信されるアソシエーション要求の RSN IE で CCKM が有効になっているものの、CCKM IE がエンコードされておらず、PMKID だけが RSN IE でエンコードされている場合でも、AP は完全な認証を行います。CCKM が RSN IE で有効になっている場合、このアクセスポイントではアソシエーション要求と一緒に送信される PMKID は使用されません。
- 802.1X+CCKM—通常の動作状態の間、802.1X が有効になっているクライアントは、主要な RADIUS サーバとの通信を含む完全な 802.1X 認証を実行することにより、新しいアクセスポイントとの相互認証を行います。ただし、802.1X および CCKM の迅速で安全なローミング用に WLAN を設定した場合、CCKM が有効になっているクライアントは、RADIUS サーバに対して再認証せずに、あるアクセスポイントから別のアクセスポイントに安全にローミングを行います。このオプションが選択されている場合、CCKM クライアントと非 CCKM クライアントの両方がサポートされるため、802.1X+CCKM はオプションの CCKM と見なされます。

単一の WLAN では、WPA1、WPA2、および 802.1X/PSK/CCKM/802.1X+CCKM のクライアントに join を許可できます。このような WLAN 上のすべてのアクセスポイントは、WPA1、WPA2、および 802.1X/PSK/CCKM/802.1X+CCKM 情報要素をビーコンおよびプローブ応答でアドバタイズします。WPA1 または WPA2、あるいは両方を有効にした場合は、データトラフィックを保護するために設計された 1 つまたは 2 つの暗号方式（暗号化アルゴリズム）を有効にすることもできます。具体的には、WPA1 または WPA2、あるいはその両方に対して、AES または TKIP、またはその両方を有効にすることができます。TKIP は WPA1 のデフォルト値で、AES は WPA2 のデフォルト値です。

## WPA1+WPA2 の設定

### WPA1+WPA2 の設定 (GUI)

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
- ステップ 3** [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit] ([Security] > [Layer 2]) ページを開きます。
- ステップ 4** [Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択します。
- ステップ 5** [WPA+WPA2 Parameters] で、[WPA Policy] チェックボックスをオンにして WPA1 を有効にするか、[WPA2 Policy] チェックボックスをオンにして WPA2 を有効にするか、または両方のチェックボックスをオンにして WPA1 と WPA2 を両方有効にします。
- (注) WPA1 および WPA2 のデフォルト値は、両方とも無効になっています。WPA1 と WPA2 を両方とも無効のままにすると、アクセス ポイントは、[ステップ 7](#) で選択する認証キー管理方式に対してのみ情報要素をビーコンおよびプローブ応答でアドバタイズします。
- ステップ 6** WPA1、WPA2、またはその両方に対して、AES データ暗号化を有効にする場合は [AES] チェックボックスをオンにし、TKIP データ暗号化を有効にする場合は [TKIP] チェックボックスをオンにします。WPA1 および WPA2 のデフォルト値は、それぞれ TKIP および AES です。
- ステップ 7** [Auth Key Mgmt] ドロップダウン リストから、[802.1X]、[CCKM]、[PSK]、または [802.1X+CCKM] のいずれかのキー管理方式を選択します。
- (注) Cisco の OEAP 600 では、CCKM はサポートされていません。802.1X または PSK を選択する必要があります。
- (注) Cisco OEAP 600 の場合、TKIP および AES セキュリティ暗号化の設定は、WPA と WPA2 で同一であることが必要です。
- ステップ 8** [ステップ 7](#) で [PSK] を選択した場合は、[PSK Format] ドロップダウン リストから [ASCII] または [HEX] を選択し、空のテキスト ボックスに事前共有キーを入力します。WPA の事前共有キーには、8 ～ 63 個の ASCII テキスト文字、または 64 桁の 16 進数文字が含まれている必要があります。
- (注) PSK パラメータは、設定専用パラメータです。PSK キーに設定された値は、セキュリティ上の理由からユーザには表示されません。たとえば、PSK キーを設定するときに、キー形式として [HEX] を選択した場合に、あとでこの WLAN のパラメータを表示すると、表示される値はデフォルト値になります。デフォルトは ASCII です。
- ステップ 9** [Apply] をクリックして、変更を確定します。
- ステップ 10** [Save Configuration] をクリックして、変更を保存します。
-



## WPA1+WPA2 の設定 (CLI)

- ステップ 1** 次のコマンドを入力して、WLAN を無効にします。  
**config wlan disable wlan\_id**
- ステップ 2** 次のコマンドを入力して、WLAN の WPA を有効または無効にします。  
**config wlan security wpa {enable | disable} wlan\_id**
- ステップ 3** 次のコマンドを入力して、WLAN の WPA1 を有効または無効にします。  
**config wlan security wpa wpa1 {enable | disable} wlan\_id**
- ステップ 4** WLAN の WPA2 を有効または無効にするには、次のコマンドを入力します。  
**config wlan security wpa wpa2 {enable | disable} wlan\_id**
- ステップ 5** WPA1 または WPA2 に対して AES または TKIP データ暗号化を有効または無効にするには、次のコマンドを入力します。
- **config wlan security wpa wpa1 ciphers {aes | tkip} {enable | disable} wlan\_id**
  - **config wlan security wpa wpa2 ciphers {aes | tkip} {enable | disable} wlan\_id**
- WPA1 および WPA2 のデフォルト値は、それぞれ TKIP および AES です。
- WGB に VLAN 設定がある場合、**encryption vlan 80 mode ciphers tkip** など、特定の VLAN に対して暗号化モードとキーを設定する必要があります。次に、コマンド **encryption mode ciphers tkip** を入力して、マルチキャスト インターフェイスに暗号化モードをグローバルに設定する必要があります。
- ステップ 6** 802.1X、PSK、または CCKM 認証キー管理を有効または無効にするには、次のコマンドを入力します。  
**config wlan security wpa akm {802.1X | psk | cckm} {enable | disable} wlan\_id**
- デフォルト値は 802.1X です。
- ステップ 7** ステップ 6 で PSK を有効にした場合は、次のコマンドを入力して事前共有キーを指定します。  
**config wlan security wpa akm psk set-key {ascii | hex} psk-key wlan\_id**
- WPA の事前共有キーには、8 ～ 63 個の ASCII テキスト文字、または 64 桁の 16 進数文字が含まれている必要があります。
- ステップ 8** 高速移行に対して認証キー管理スイートを有効または無効にするには、次のコマンドを入力します。  
**config wlan security wpa akm ft {802.1X | psk} {enable | disable} wlan\_id**
- (注) AKM スイートとして PSK または高速移行 PSK を選択できません。
- ステップ 9** AP とクライアント間のグループの一時的キー (GTK) のランダム化を有効または無効にするには、次のコマンドを入力します。  
**config wlan security wpa gtk-random {enable | disable} wlan\_id**
- ステップ 10** 802.1X 認証キー管理で WPA2、または CCKM 認証キー管理で WPA1 または WPA2 を有効にした場合、必要に応じて、PMK キャッシュ ライフタイム タイマーを使用して、クライアントでの再認証をトリガーします。タイマーは、AAA サーバから受信したタイムアウト値または WLAN のセッション タイムアウト

設定に基づきます。タイマーが切れるまでに残されている時間を確認するには、次のコマンドを入力します。

**show pmk-cache all**

802.1X 認証キー管理で WPA2 を有効にした場合、コントローラは opportunistic PMKID キャッシュと sticky (non-opportunistic) PMKID キャッシュの両方をサポートします。sticky PMKID キャッシュ (SKC) で、クライアントは、アソシエートする AP ごとに異なる、複数の PMKID を保存します。opportunistic PMKID キャッシュ (OKC) は、クライアントあたり 1 つの PMKID だけを保存します。デフォルトで、コントローラは OKC をサポートします。

**ステップ 11** WLAN を有効にするには、次のコマンドを入力します。

**config wlan enable wlan\_id**

**ステップ 12** 次のコマンドを入力して、設定を保存します。

**save config**

---



# 第 83 章

## Sticky Key Caching の設定

- [Sticky Key Caching](#) について, 701 ページ
- [Sticky Key Caching](#) の制約事項, 701 ページ
- [Sticky Key Caching](#) の設定 (CLI) , 702 ページ

### Sticky Key Caching について

コントローラは Sticky Key Caching (SKC) をサポートします。Sticky Key Caching により、クライアントは、アソシエートする AP ごとに異なる PMKID を受信し、保存します。AP も、クライアントに発行される PMKID のデータベースを維持します。

SKC では、クライアントは Pairwise Master Key Security Association (PMKSA) に対してそれぞれの Pairwise Master Key ID (PMKID) を保存します。クライアントがそれに対する PMKSA を保持する AP を見つけた場合、アソシエーション要求内で PMKID を AP に送信します。PMKSA が AP で稼働している場合は、AP は、高速ローミングをサポートします。SKC では、クライアントがアソシエートする新しい AP に関して完全な認証が実行され、すべての AP とアソシエートされる PMKSA をクライアントが維持しなければなりません。SKC の場合、PMKSA はクライアントが保存する AP のキャッシュごとであり、新しい AP の BSSID に基づいて事前に計算されます。

### Sticky Key Caching の制約事項

- コントローラは、クライアントあたり最大 8 つの AP の SKC をサポートします。クライアントがセッションあたり 8 以上の AP にローミングする場合、クライアントのローミング時に、古い AP は削除され、新しくキャッシュされたエントリが保存されます。大規模な展開に SKC を使用しないことを推奨します。
- SKC は、WPA2 が有効になっている WLAN でのみ動作します。
- SKC は、モビリティグループのアクセスコントローラでは機能しません。
- SKC はローカルモードの AP でのみ動作します。

## Sticky Key Caching の設定 (CLI)

ステップ 1 次のコマンドを入力して、WLAN を無効にします。

```
config wlan disable wlan_id
```

ステップ 2 次のコマンドを入力して、sticky key caching を有効にします。

```
config wlan security wpa wpa2 cache sticky enable wlan_id
```

デフォルトでは、SKC は無効で opportunistic key caching (OKC) が有効になっています。

(注) SKC は、WPA2 が有効になっている WLAN でのみ動作します。

SKC が有効かどうかを確認するには、次のコマンドを入力します。

```
show wlan wlan_id
```

以下に類似した情報が表示されます。

```
WLAN Identifier..... 2
Profile Name..... new
Network Name (SSID)..... new
Status..... Disabled
MAC Filtering..... Disabled
Security
 802.11 Authentication:..... Open System
 Static WEP Keys..... Disabled
 802.1X..... Disabled
 Wi-Fi Protected Access (WPA/WPA2)..... Enabled
 WPA (SSN IE)..... Disabled
 WPA2 (RSN IE)..... Enabled
 TKIP Cipher..... Disabled
 AES Cipher..... Enabled
 Auth Key Management
 802.1x..... Disabled
 PSK..... Enabled
 CCKM..... Disabled
 FT(802.11r)..... Disabled
 FT-PSK(802.11r)..... Disabled
 SKC Cache Support..... Enabled
 FT Reassociation Timeout..... 20
 FT Over-The-Air mode..... Enabled
 FT Over-The-Ds mode..... Enabled
 CCKM tsf Tolerance..... 1000
 Wi-Fi Direct policy configured..... Disabled
 EAP-Passthrough..... Disabled
```

ステップ 3 WLAN を有効にするには、次のコマンドを入力します。

```
config wlan enable wlan_id
```

**ステップ 4** 次のコマンドを入力して、設定を保存します。  
**save config**

---





## 第 84 章

# CKIP の設定

- [CKIP について](#) , 705 ページ
- [CKIP の設定 \(GUI\)](#) , 706 ページ
- [CKIP の設定 \(CLI\)](#) , 707 ページ

## CKIP について

Cisco Key Integrity Protocol (CKIP) は、IEEE 802.11 メディアを暗号化するためのシスコ独自のセキュリティプロトコルです。CKIP では、インフラストラクチャモードでの 802.11 セキュリティを強化するために、キーの置換、メッセージの整合性チェック (MIC)、およびメッセージシーケンス番号が使用されています。ソフトウェアリリース 4.0 以降では、静的キーを使用した CKIP をサポートしています。この機能を正常に動作させるには、WLAN に対して Aironet 情報要素 (IE) を有効にする必要があります。

Lightweight アクセス ポイントは、ビーコンおよびプローブ応答パケットに Aironet IE を追加し、CKIP ネゴシエーションビット (キー置換およびマルチモジュラハッシュメッセージ整合性チェック [MMH MIC]) の一方または両方を設定することにより、CKIP のサポートをアドバタイズします。キー置換は、基本の暗号キーおよび現在の初期ベクトル (IV) を使用して新しいキーを作成するデータ暗号化技術です。MMH MIC では、ハッシュ関数を使用してメッセージ整合性コードを計算することにより、暗号化されたパケットでのパケット改ざん攻撃を回避します。

WLAN で指定された CKIP の設定は、アソシエートを試みるすべてのクライアントに必須です。WLAN で CKIP のキー置換および MMH MIC の両方が設定されている場合、クライアントは両方をサポートする必要があります。WLAN がこれらの機能の 1 つだけに設定されている場合は、クライアントではその CKIP 機能だけをサポートする必要があります。

CKIP では、5 バイトおよび 13 バイトの暗号キーは 16 バイトのキーに拡張される必要があります。キーを拡張するためのアルゴリズムは、アクセス ポイントで発生します。キーは、長さが 16 バイトに達するまで、そのキー自体に繰り返し追加されます。Lightweight アクセス ポイントはすべて CKIP をサポートしています。



- (注) CKIP は Static WEP での使用についてのみサポートされています。Dynamic WEP での使用はサポートされていません。したがって、Dynamic WEP で CKIP を使用するように設定された無線クライアントは、CKIP 用に設定されている WLAN にアソシエートできません。CKIP なしで Dynamic WEP を使用する (安全性がより低い) か、または TKIP または AES で WPA/WPA2 を使用する (安全性がより高い) ことを推奨します。

## CKIP の設定 (GUI)

- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
- ステップ 3** [Advanced] タブを選択します。
- ステップ 4** [Aironet IE] チェックボックスをオンにして、この WLAN に対する Aironet IE を有効にし、[Apply] をクリックします。
- ステップ 5** [General] タブを選択します。
- ステップ 6** [Status] チェックボックスがオンになっている場合は、これをオフにしてこの WLAN を無効にし、[Apply] をクリックします。
- ステップ 7** [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit] ([Security] > [Layer 2]) ページを開きます。
- ステップ 8** [Layer 2 Security] ドロップダウンリストから [CKIP] を選択します。
- ステップ 9** [CKIP Parameters] で、[Key Size] ドロップダウンリストから CKIP 暗号キーの長さを選択します。その範囲は、[Not Set]、[40 bits]、または [104 bits] です。デフォルトは、[Not Set] です。
- ステップ 10** [Key Index] ドロップダウンリストからこのキーに割り当てる番号を選択します。キーは、最高 4 つまで設定できます。
- ステップ 11** [Key Format] ドロップダウンリストから、[ASCII] または [HEX] を選択し、[Encryption Key] テキストボックスに暗号化キーを入力します。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。
- ステップ 12** この WLAN に対して MMH MIC データ保護を有効にする場合は、[MMH Mode] チェックボックスをオンにします。デフォルト値では無効 (またはオフ) になっています。
- ステップ 13** この形式の CKIP データ保護を有効にする場合は、[Key Permutation] チェックボックスをオンにします。デフォルト値では無効 (またはオフ) になっています。
- ステップ 14** [Apply] をクリックして、変更を確定します。
- ステップ 15** [General] タブを選択します。
- ステップ 16** [Status] チェックボックスをオンにして、この WLAN を有効にします。
- ステップ 17** [Apply] をクリックして、変更を確定します。
- ステップ 18** [Save Configuration] をクリックして、変更を保存します。



## CKIP の設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、WLAN を無効にします。  
**config wlan disable** *wlan\_id*
- ステップ 2 この WLAN の Aironet IE を有効にするには、次のコマンドを入力します。  
**config wlan ccx aironet-ie enable** *wlan\_id*
- ステップ 3 WLAN の CKIP を有効または無効にするには、次のコマンドを入力します。  
**config wlan security ckip** {enable | disable} *wlan\_id*
- ステップ 4 WLAN に対して CKIP 暗号化キーを指定するには、次のコマンドを入力します。  
**config wlan security ckip akm psk set-key** *wlan\_id* {40 | 104} {hex | ascii} *key key\_index*
- ステップ 5 WLAN に対して CKIP MMH MIC を有効または無効にするには、次のコマンドを入力します。  
**config wlan security ckip mmh-mic** {enable | disable} *wlan\_id*
- ステップ 6 WLAN に対して CKIP キー置換を有効または無効にするには、次のコマンドを入力します。  
**config wlan security ckip kp** {enable | disable} *wlan\_id*
- ステップ 7 WLAN を有効にするには、次のコマンドを入力します。  
**config wlan enable** *wlan\_id*
- ステップ 8 次のコマンドを入力して、設定を保存します。  
**save config**
-





# 第 85 章

## レイヤ 3 セキュリティの設定

---

- [VPN パススルーを使用したレイヤ 3 セキュリティの設定, 709 ページ](#)
- [Web 認証を使用したレイヤ 3 セキュリティの設定, 710 ページ](#)

### VPN パススルーを使用したレイヤ 3 セキュリティの設定

#### VPN パススルーを使用したレイヤ 3 セキュリティの制約事項

- レイヤ 2 トンネリングプロトコル (L2TP) と IPSec は、コントローラでサポートされていません。
- レイヤ 3 セキュリティ設定は、WLAN でクライアント IP アドレスを無効にしているときはサポートされません。
- VPN パススルー オプションは、Cisco 5500 シリーズのコントローラでは使用できません。しかし、ACL を使用してオープン WLAN を作成すると、その機能をこのコントローラで再現できます。

#### VPN パススルーについて

コントローラは、VPN パススルー、つまり VPN クライアントから送信されるパケットの「通過」をサポートします。VPN パススルーの例として、ラップトップから本社オフィスの VPN サーバへの接続が挙げられます。

## VPN パススルーの設定

### VPN パススルーの設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 VPN パススルーを設定する WLAN の ID 番号をクリックします。[WLANs>Edit] ページが表示されます。
- ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit] ([Security] > [Layer 3]) ページを開きます。
- ステップ 4 [Layer 3 Security] ドロップダウン リストから、[VPN Pass-Through] を選択します。
- ステップ 5 [VPN Gateway Address] テキストボックスに、クライアントにより開始され、コントローラを通過した VPN トンネルを終端しているゲートウェイ ルータの IP アドレスを入力します。
- ステップ 6 [Apply] をクリックして、変更を確定します。
- ステップ 7 [Save Configuration] をクリックして設定を保存します。
- 

### VPN パススルーの設定 (CLI)

VPN パススルーを設定するには、次のコマンドを使用します。

- `config wlan security passthru {enable | disable} wlan_id gateway`  
`gateway` には、VPN トンネルを終端している IP アドレスを入力します。
- パススルーが有効であることを確認するには、次のコマンドを入力します。  
`show wlan`

## Web 認証を使用したレイヤ 3 セキュリティの設定

### WLAN の Web 認証を設定するための前提条件

- HTTP/HTTPS Web 認証のリダイレクトを開始するには、常に HTTP URL のみを使用し、HTTPS URL を使用しないでください。
- CPU ACL が HTTP/HTTPS トラフィックをブロックするように設定されている場合、正常な Web ログイン認証の後に、リダイレクションページでエラーが発生する可能性があります。
- Web 認証を有効にする前に、すべてのプロキシサーバがポート 53 以外のポートに対して設定されていることを確認してください。
- WLAN の Web 認証を有効にする場合、コントローラがワイヤレス クライアントで送受信されるトラフィックを転送することを示すメッセージが認証前に表示されます。DNS トラ

フィックを規制し、DNS トンネリング攻撃を検出および予防するために、ゲスト VLAN の背後にファイアウォールまたは侵入検知システム (IDS) を設置することをお勧めします。

- Web 認証が WLAN で有効になっており、さらに、CPU ACL のルールもある場合、クライアントベースの Web 認証ルールは、クライアントが非認証である限り優先されます (webAuth\_Reqd ステート)。クライアントが RUN 状態になると、CPU ACL ルールが適用されます。したがって、コントローラで CPU ACL ルールが有効である場合、次の状態で、仮想インターフェイス IP に対する allow ルール (任意の方向) が必要になります。
  - CPU ACL で、両方向とも allow ACL ルールが設定されていない。
  - allow ALL ルールが設定されているが、優先順位が高いポート 443 または 80 に対する DENY ルールが割り当ても設定されている。
- 仮想 IP に対する allow ルールは、TCP プロトコルおよびポート 80 (secureweb が無効な場合) またはポート 443 (secureweb が有効な場合) に設定します。このプロセスは、仮想インターフェイス IP アドレスへのクライアントのアクセスを許可し、CPU ACL ルールが設定されている場合に正常認証をポストするために必要です。

## WLAN の Web 認証の設定に関する制約事項

- Web 認証はレイヤ 2 セキュリティポリシー (オープン認証、オープン認証+WEP、WPA-PSK) でのみサポートされています。7.4 リリースでは、Web 認証での 802.1X の使用がサポートされています。
- Web 認証のユーザ名フィールドでの特殊文字はサポートされていません。
- クライアントが WebAuth SSID に接続したときに、事前認証 ACL が VPN ユーザを許可するように設定されていると、クライアントは数分ごとに SSID との接続を解除されます。Webauth SSID の接続には、Web ページでの認証が必要です。

Web 認証ユーザ セクションの [WLANs] > [Security] > [AAA servers] > [Authentication priority] で次の ID ストアを選択して、Web 認証ユーザを認証できます。

- ローカル
- RADIUS
- LDAP

複数の ID ストアを選択すると、コントローラはユーザの認証が成功するまで、リストの各 ID ストアを指定された順序で上から下までチェックします。コントローラがリストの最後に達しても ID ストアのいずれかに未認証のユーザが残っている場合、認証は失敗します。

## Web 認証について

コントローラで VPN パススルーが有効になっていない場合に限り、WLAN では Web 認証を使用できます。Web 認証は、セットアップも使用方法も簡単で、SSL とともに使用することで WLAN 全体のセキュリティを向上させることができます。

## Web 認証の設定

### Web 認証の設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
  - ステップ 2 Web 認証を設定する WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。
  - ステップ 3 [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit] ([Security] > [Layer 3]) ページを開きます。
  - ステップ 4 [Web Policy] チェックボックスをオンにします。
  - ステップ 5 [Authentication] オプションが選択されていることを確認します。
  - ステップ 6 [Apply] をクリックして、変更を確定します。
  - ステップ 7 [Save Configuration] をクリックして設定を保存します。
- 

### Web 認証の設定 (CLI)

- 
- ステップ 1 特定の WLAN で Web 認証を有効または無効にするには、次のコマンドを入力します。  
**config wlan security web-auth {enable | disable} wlan\_id**
  - ステップ 2 Web 認証ポリシーのタイマーが切れたときにゲストユーザの IP アドレスを解放して、ゲストユーザが 3 分間 IP アドレスを取得しないようにするには、次のコマンドを入力します。  
**config wlan webauth-exclude wlan\_id {enable | disable}**  

デフォルト値はディセーブルです。コントローラに内部 DHCP スコープを設定するときに、このコマンドを適用できます。デフォルトでは、ゲストユーザは、Web 認証のタイマーが切れた場合、別のゲストユーザがその IP アドレスを取得する前に、ただちに同じ IP アドレスに再アソシエートできます。ゲストユーザの数が多く、または DHCP プールの IP アドレスが限られている場合、一部のゲストユーザが IP アドレスを取得できなくなる可能性があります。

ゲスト WLAN でこの機能を有効にした場合、Web 認証ポリシーのタイマーが切れると、ゲストユーザの IP アドレスが解放され、このゲストユーザは 3 分間 IP アドレスの取得から除外されます。その IP アドレスは、別のゲストユーザが使用できます。3 分経つと、除外されていたゲストユーザは、可能であれば、再アソシエートし、IP アドレスを取得できるようになります。
  - ステップ 3 次のコマンドを入力して、Web 認証のステータスを表示します。  
**show wlan wlan\_id**
-



## 第 86 章

# キャプティブバイパスの設定

- [キャプティブバイパスについて](#), 713 ページ
- [キャプティブバイパスの設定 \(CLI\)](#), 714 ページ

## キャプティブバイパスについて

WISPr は、ユーザが異なるワイヤレス サービスプロバイダー間をローミングできるようにするドラフトプロトコルです。一部のデバイス (Apple iOS デバイスなど) には、指定の URL に対する HTTP WISPr 要求に基づいて、デバイスがインターネットに接続するかどうかを決定するときに使用するメカニズムが搭載されています。このメカニズムは、インターネットへの直接接続が不可能なときにデバイスが自動的に Web ブラウザを開くために使用されます。これにより、ユーザがインターネットにアクセスするために、自身の認証情報を提供することが可能となります。実際の認証は、デバイスが新しい SSID に接続するたびにバックグラウンドで実行されます。

クライアントデバイス (Apple iOS デバイス) は、WISPr 要求をコントローラに送信します。コントローラはユーザエージェントの詳細をチェックし、コントローラでの Web 認証代行受信により HTTP 要求をトリガーします。ユーザエージェントによって提供される IOS バージョンおよびブラウザの詳細の確認後に、コントローラによってクライアントはキャプティブポータル設定のバイパスを許可され、インターネットにアクセスできます。



(注) IOS7 用キャプティブポータルバイパスは、Cisco ワイヤレス LAN コントローラ リリース 7.6 でのみサポートされています。

この HTTP 要求は、他のページ要求がワイヤレスクライアントによって実行されると、コントローラでの Web 認証代行受信をトリガーします。この代行受信によって Web 認証プロセスが発生し、プロセスは正常に完了します。Web 認証がいずれかのコントローラ スプラッシュ ページ機能で使用されていると (設定された RADIUS サーバが URL を指定)、WISPr 要求が非常に短い間隔で発信されるので、スプラッシュ ページが表示されることはなく、いずれかのクエリーが指定のサーバに到達できるとただちに、バックグラウンドで実行されている Web リダイレクションまたはスプラッシュ ページ表示プロセスが中断されます。そして、デバイスによってページ要求が処理され、スプラッシュ ページ機能は中断されます。

たとえば、Apple は iOS 機能を導入して、キャプティブ ポータルがある場合のネットワーク アクセスを容易にしました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することにより、キャプティブ ポータルの存在を検出します。この要求は、Apple iOS バージョン 6 以前の場合は<http://www.apple.com/library/test/success.html>、および Apple iOS バージョン 7 以降の場合は複数の該当するターゲット URL に送られます。応答が受信されると、インターネット アクセスが使用可能であると見なされ、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブポータルによってブロックされたと見なされ、Apple の Captive Network Assistant (CNA) が疑似ブラウザを自動起動して管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。コントローラは、この疑似ブラウザがポップアップ表示されないようにします。

現在、WISPr 検出プロセスをバイパスするようにコントローラを設定できるようになりました。それによって、ユーザが、ユーザ コンテキストでスプラッシュ ページロードを引き起こす Web ページを要求したときに、バックグラウンドで WISPr 検出を実行せずに、Web 認証代行受信だけが行われるようにすることができます。

## キャプティブバイパスの設定 (CLI)

キャプティブバイパスを設定するには、次のコマンドを使用します。

- **config network web-auth captive-bypass {enable | disable}** : ネットワーク レベルでのキャプティブポータルのバイパスに対するコントローラのサポートを有効または無効にします。
- **show network summary** : WISPr プロトコル検出機能のステータスを表示します。





# 第 87 章

## MAC フィルタリングおよび Web 認証を伴う フォールバック ポリシーの設定

---

- [MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーについて](#), 715 ページ
- [MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定 \(GUI\)](#), 716 ページ
- [MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定 \(CLI\)](#), 717 ページ

### MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシー について

レイヤ2およびレイヤ3セキュリティを組み合わせたフォールバック ポリシー メカニズムを設定できます。MAC フィルタリングおよび Web 認証の両方が設定されているシナリオで、MAC フィルタ (RADIUS サーバ) を使用して WLAN への接続を試行する場合、クライアントが認証に失敗すると、Web 認証にフォールバックできるように認証を設定できます。クライアントが MAC フィルタ認証をパスすると、Web 認証が省略され、クライアントは WLAN に接続されます。この機能を使用して、MAC フィルタ認証エラーのみに基づいたアソシエーション解除を回避できます。

## MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定 (GUI)



(注) フォールバック ポリシーを設定する前に、MAC フィルタリングを有効にする必要があります。

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** Web 認証に対してフォールバック ポリシーを設定する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。
- ステップ 3** [Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit] ([Security] > [Layer 3]) ページを開きます。
- ステップ 4** [Layer 3 Security] ドロップダウン リストから、[None] を選択します。
- ステップ 5** [Web Policy] チェックボックスをオンにします。
- (注) コントローラは、認証前にワイヤレスクライアントで送受信される DNS トラフィックを転送します。
- 次のオプションが表示されます。
- Authentication
  - Passthrough
  - Conditional Web Redirect
  - Splash Page Web Redirect
  - On MAC Filter Failure
- ステップ 6** [On MAC Filter Failure] をクリックします。
- ステップ 7** [Apply] をクリックして、変更を確定します。
- ステップ 8** [Save Configuration] をクリックして設定を保存します。
-

## MAC フィルタリングおよび Web 認証を伴うフォールバック ポリシーの設定 (CLI)



(注) フォールバック ポリシーを設定する前に、MAC フィルタリングを有効にする必要があります。MAC フィルタリングを有効にする方法については、「[WLAN の MAC フィルタリングについて](#)」の項を参照してください。

**ステップ 1** 特定の WLAN で Web 認証を有効または無効にするには、次のコマンドを入力します。  
**config wlan security web-auth on-macfilter-failure wlan-id**

**ステップ 2** Web 認証ステータスを表示するには、次のコマンドを入力します。  
**show wlan wlan\_id**

```
FT Over-The-Ds mode..... Enabled
CKIP Disabled
 IP Security..... Disabled
 IP Security Passthru..... Disabled
Web Based Authentication..... Enabled-On-MACFilter-Failure
 ACL..... Unconfigured
Web Authentication server precedence:
 1..... local
 2..... radius
 3..... ldap
```





# 第 88 章

## QoS プロファイルの割り当て

- [QoS プロファイルについて](#), 719 ページ
- [WLAN への QoS プロファイルの割り当て \(GUI\)](#), 720 ページ
- [WLAN への QoS プロファイルの割り当て \(CLI\)](#), 722 ページ

### QoS プロファイルについて

Cisco UWN ソリューション WLAN では、Platinum/音声、Gold/ビデオ、Silver/ベストエフォート（デフォルト）、Bronze/バックグラウンドの4つのレベルのQoSをサポートしています。音声転送 WLAN で Platinum QoS を使用するよう設定したり、低帯域幅 WLAN で Bronze QoS を使用するよう割り当てたり、その他すべてのトラフィックに残りの QoS レベルを割り当てたりすることができます。

WLAN QoS レベルは、無線トラフィックの特定の 802.11e User Priority (UP) を定義します。この UP は、WMM 以外の有線トラフィックの優先順位を導出すると同時に、さまざまな優先レベルの WMM トラフィックを管理する際の上限值としても機能します。

ワイヤレスレート制限は、アップストリームおよびダウンストリームトラフィックの両方に定義できます。レート制限は SSID ごとに定義するか、または最大レート制限としてすべてのクライアントに対して指定できます（あるいは両方を行えます）。これらのレート制限は個別に設定できます。

アクセスポイントは、次の表の値に従ってこの QoS プロファイル固有の UP を使用することで、無線 LAN 上で確認可能な IP DSCP 値を導出します。

表 19: アクセスポイントの QoS 変換値

AVVID トラフィック タイプ	AVVID IP DSCP	QoS プロファイル	AVVID 802.1p	IEEE 802.11e UP
ネットワーク制御	56 (CS7)	Platinum	7	7

AVVID トラフィック タイプ	AVVID IP DSCP	QoS プロファイル	AVVID 802.1p	IEEE 802.11e UP
ネットワーク間制御 (CAPWAP 制御、 802.11 管理)	48 (CS6)	Platinum	6	7
音声	46 (EF)	Platinum	5	6
対話型ビデオ	34 (AF41)	Gold	4	5
ミッションクリティカル	26 (AF31)	Gold	3	4
トランザクション	18 (AF21)	Silver	2	3
バルク データ	10 (AF11)	Bronze	1	2
ベスト エフォート	0 (BE)	Silver	0	0
スカベンジャー	2	Bronze	0	1



(注) 表に記載されていない DSCP 値に対する IEEE 802.11e UP 値は、DSCP の上位 (MSB) 3 ビットを考慮して算出されます。

たとえば、DSCP 32 (バイナリ 100 000) に対する IEEE 802.11e UP 値は、10 進数に相当する MSB (100) 値で、これは 4 になります。DSCP 32 の 802.11e UP 値は 4 です。

## WLAN への QoS プロファイルの割り当て (GUI)

### はじめる前に

まだ設定していない場合は、「QoS プロファイルの設定 (GUI)」セクションの指示に従って 1 つ以上の QoS プロファイルを設定してください。

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 QoS プロファイルを割り当てる WLAN の ID 番号をクリックします。
- ステップ 3 [WLANs > Edit] ページが表示されたら、[QoS] タブを選択します。
- ステップ 4 [Quality of Service (QoS)] ドロップダウンリストから、次のいずれかを選択します。

- Platinum (voice)
- Gold (video)
- Silver (best effort)
- Bronze (background)

(注) Silver (ベスト エフォート) がデフォルト値です。

**ステップ 5** データ レートをユーザ単位で定義するには、次の手順を実行します。

- a) [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
- b) [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックのピーク データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
 

(注) burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

バースト データ レートを設定する前に平均データ レートを設定してください。
- c) [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
 

(注) 平均リアルタイム レートが UDP トラフィック用に使用されているとき、平均データ レートは TCP トラフィックの測定に使用されます。すべてのエントリに対してキロビット/秒の単位で測定されます。平均データ レートと平均リアルタイム レートは、TCP や UDP などの上位層プロトコルに適用されているので、これらの値は異なる場合があります。これらの異なるレートの値は帯域幅に影響を与えません。
- d) [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックのピーク リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
 

(注) バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

**ステップ 6** データ レートを SSID 単位で定義するには、次の手順を実行します。

- a) [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
- b) [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックのピーク データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
 

(注) burst-data-rate は average-data-rate 以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。

- c) [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
- d) [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックのピークリアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。
- (注) バーストリアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされる場合があります。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Save Configuration] をクリックします。

## WLAN への QoS プロファイルの割り当て (CLI)

まだ設定していない場合は、「QoS プロファイルの設定 (CLI)」セクションの指示に従って1つ以上の QoS プロファイルを設定してください。

ステップ 1 QoS プロファイルを WLAN に割り当てるには、次のコマンドを入力します。

```
config wlan qos wlan_id {bronze | silver | gold | platinum}
```

Silver がデフォルト値です。

ステップ 2 QoS プロファイルのレート制限パラメータを無効にするには、次のコマンドを入力します。

```
config wlan override-rate-limit wlan-id {average-data-rate | average-realtime-rate | burst-data-rate | burst-realtime-rate} {per-ssid | per-client} {downstream | upstream} rate
```

ステップ 3 **save config** コマンドを入力します。

ステップ 4 QoS プロファイルを WLAN に適切に割り当てたことを確認するには、次のコマンドを入力します。

```
show wlan wlan_id
```

以下に類似した情報が表示されます。

```
WLAN Identifier..... 1
Profile Name..... test
Network Name (SSID)..... test
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist..... Disabled
Session Timeout..... 0
Interface..... management
WLAN ACL..... unconfigured
```



```
DHCP Server..... 1.100.163.24
DHCP Address Assignment Required..... Disabled
Quality of Service..... Silver (best effort)
WMM..... Disabled
...
```

---





# 第 89 章

## QoS Enhanced BSS の設定

- [Cisco 7921 および 7920 Wireless IP Phone で QoS Enhanced BSS を使用するための前提条件, 725 ページ](#)
- [QoS Enhanced BSS の制約事項, 726 ページ](#)
- [QoS Enhanced BSS について, 726 ページ](#)
- [QBSS の設定 \(GUI\) , 727 ページ](#)
- [QBSS の設定 \(CLI\) , 728 ページ](#)

### Cisco 7921 および 7920 Wireless IP Phone で QoS Enhanced BSS を使用するための前提条件

Cisco 7921 および 7920 Wireless IP Phone をコントローラで使用する場合は、次のガイドラインに従ってください。

- 各コントローラで、アグレッシブなロード バランシングが無効にされている必要があります。無効化されていない場合、電話による初期ローミングが失敗し、オーディオパスが中断されることがあります。
- Dynamic Transmit Power Control (DTPC) 情報要素 (IE) が、**config 802.11b dtpc enable** コマンドを使用して有効にされている必要があります。DTPC IE は、アクセス ポイントがその送信電力で情報をブロードキャストすることを可能にする、ビーコンおよびプローブの情報要素です。7921 または 7920 電話は、この情報を使用して、その送信電力を、アソシエート先のアクセス ポイントと同じレベルに自動的に調整します。このようにして、両方のデバイスが同じレベルで送信するようになります。
- 7921 と 7920 電話のおよびコントローラの両方で、Cisco Centralized Key Management (CCKM) 高速ローミングがサポートされます。
- WEP を設定する際、コントローラおよび 7921 または 7920 電話によって、用語上の違いがあります。7921 または 7920 で 128 ビット WEP を使用する場合は、コントローラを 104 ビットに設定してください。

- スタンドアロンの 7921 電話では、load-based の CAC が有効にされ、また WLAN 上で WMM Policy が Required に設定されている必要があります。
- コントローラでは、ファームウェアバージョン 1.1.1 を使用して 7921 電話から送られるトラフィック分類 (TCLAS) がサポートされます。この機能により、7921 電話への音声ストリームを正しく分類することができます。
- 1242 シリーズアクセスポイントの 802.11a 無線で 7921 電話を使用する場合は、24-Mbps データレートを Supported に設定して、それよりも小さい Mandatory データレート (12 Mbps など) を選択します。さもないと、電話の音声品質が低下するおそれがあります。

## QoS Enhanced BSS の制約事項

- OEAP 600 シリーズアクセスポイントでは、CAC はサポートされません。
- デフォルトで、QBSS は無効になっています。
- 7920 電話は、CAC 機能が制限された、非 WMM 電話です。電話は、アソシエート先のアクセスポイントのチャンネル使用率を確認し、それをアクセスポイントからビーコンにより通知されたしきい値と比較します。チャンネル使用率がしきい値より低い場合は、7920 は電話をかけます。対照的に、7921 電話は、完全な機能を備えた WMM 電話で、Traffic Specifications (TSPEC) を使用して、電話をかける前に音声キューにアクセスします。7921 電話は、load-based の CAC と適切に連動します。load-based の CAC では、音声に取り分けられたチャンネルの割合を使用して、それに応じて通話を制限しようとします。

7921 電話は WMM をサポートし、7920 電話はサポートしないため、これらの電話を混合環境で使用する場合に両方の電話を適切に設定していないと、キャパシティと音声品質の問題が生じる可能性があります。7921 および 7920 電話の両方を有効にして同じネットワーク上で共存させるには、load-based の CAC と 7920 AP CAC の両方がコントローラで有効にされ、WMM Policy が Allowed に設定されていることを確認してください。7921 ユーザより、7920 ユーザの方が多く場合、これらの設定は特に重要になります。

- 音声をサポートしているすべての無線ネットワークでは、ベンダーに関係なく、コントローラ GUI または CLI を使用して、アグレッシブロードバランシングを常にオフにすることを推奨します。アグレッシブロードバランシングがオンになっていると、ハンドセットが最初の再アソシエーション試行で拒否されたとき、音声クライアントはローミングすると可聴アーティファクトを聞くことができます。

## QoS Enhanced BSS について

QoS Enhanced Basis Service Set (QBSS) 情報要素 (IE) により、アクセスポイントはそのチャンネル使用率をワイヤレスデバイスに通知できます。チャンネル使用率が高いアクセスポイントではリアルタイムトラフィックを効率的に処理できないため、7921 または 7920 電話では、QBSS 値を使用して、他のアクセスポイントにアソシエートするべきかどうか判断されます。次の 2 つのモードで QBSS を有効にできます。

- 802.11E QBSS 規格を満たすデバイス (Cisco 7921 IP Phone など) をサポートしている、Wi-Fi Multimedia (WMM) モード
- 802.11b/g ネットワーク上で Cisco 7920 IP Phone をサポートしている 7920 サポート モード  
7920 サポート モードには、次の 2 つのオプションが含まれています。
  - コール アドミッション制御 (CAC) がクライアント デバイス上で設定され、クライアントデバイスによってアダプタイズされている必要がある 7920 電話のサポート (通常、旧式の 7920 電話)
  - CAC がアクセス ポイント上で設定され、アクセス ポイントによってアダプタイズされている必要がある 7920 電話のサポート (通常、新式の 7920 電話)  
アクセス ポイントで制御される CAC が有効になっている場合、アクセス ポイントは、シスコが所有する CAC Information Element (IE;情報要素) を送信し、標準の QBSS IE を送信しません。

## QBSS の設定 (GUI)

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** WMM モードを設定する WLAN の ID 番号をクリックします。
- ステップ 3** [WLANs] > [Edit] ページが表示されたら、[QoS] タブを選択して [WLANs > Edit (QoS)] ページを開きます。
- ステップ 4** 7921 電話および WMM 規格を満たすその他のデバイスに対して WMM モードを有効にするかどうかに応じて、[WMM Policy] ドロップダウン リストから次のオプションのいずれかを選択してください。
- [Disabled] : WLAN 上で WMM を無効にします。これは、デフォルト値です。
  - [Allowed] : WLAN 上でクライアント デバイスに WMM の使用を許可します。
  - [Required] : クライアント デバイスで WMM の使用を必須にします。WMM をサポートしていないデバイスは WLAN に join できません。
- ステップ 5** アクセス ポイントで制御される CAC を必要とする電話で 7920 サポート モードを有効にする場合は、[7920 AP CAC] チェックボックスをオンにします。デフォルト値はオフです。
- ステップ 6** クライアントで制御される CAC を必要とする電話で 7920 サポート モードを有効にする場合は、[7920 Client CAC] チェックボックスをオンにします。デフォルト値はオフです。  
(注) 1 つの WLAN で、WMM モードとクライアントにより制御された CAC モードの両方を有効にすることはできません。
- ステップ 7** [Apply] をクリックして、変更を確定します。
- ステップ 8** [Save Configuration] をクリックして、変更を保存します。
-

## QBSS の設定 (CLI)

---

**ステップ 1** QBSS サポートを追加する WLAN の ID 番号を決定するには、次のコマンドを入力します。

```
show wlan summary
```

**ステップ 2** 次のコマンドを入力して、WLAN を無効にします。

```
config wlan disable wlan_id
```

**ステップ 3** 7921 電話および WMM 規格を満たすその他のデバイスで WMM モードを設定するには、次のコマンドを入力します。

```
config wlan wmm {disabled | allowed | required} wlan_id
```

値は次のとおりです。

- **disabled** は、WLAN 上の WMM モードを無効にします。
- **allowed** は、WLAN 上のクライアント デバイスに WMM の使用を許可します。
- **required** は、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に join できません。

**ステップ 4** クライアントで制御される CAC を必要とする電話で 7920 サポート モードを有効または無効にするには、次のコマンドを入力します。

```
config wlan 7920-support client-cac-limit {enable | disable} wlan_id
```

(注) 1つの WLAN で、WMM モードとクライアントにより制御された CAC モードの両方を有効にすることはできません。

**ステップ 5** アクセス ポイントで制御される CAC を必要とする電話で 7920 サポート モードを有効または無効にするには、次のコマンドを入力します。

```
config wlan 7920-support ap-cac-limit {enable | disable} wlan_id
```

**ステップ 6** 次のコマンドを入力して、WLAN を再び有効にします。

```
config wlan enable wlan_id
```

**ステップ 7** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 8** WLAN が有効であり、[Dot11-Phone Mode (7920)] テキスト ボックスがコンパクト モードに設定されていることを確認するには、次のコマンドを入力します。

```
show wlan wlan_id
```

---



## 第 90 章

# メディアセッションスヌーピングおよびレポートの設定

- [メディアセッションスヌーピングおよびレポートの制約事項](#), 729 ページ
- [メディアセッションスヌーピングおよびレポートについて](#), 729 ページ
- [メディアセッションスヌーピングの設定 \(GUI\)](#), 730 ページ
- [メディアセッションスヌーピングの設定 \(CLI\)](#), 730 ページ

## メディアセッションスヌーピングおよびレポートの制約事項

コントローラ ソフトウェア リリース 6.0 以降では、Voice over IP (VoIP) Media Session Aware (MSA) スヌーピングおよびレポートをサポートしています。

## メディアセッションスヌーピングおよびレポートについて

この機能により、アクセス ポイントは Session Initiation Protocol (SIP) の音声コールの確立、終了、および失敗を検出し、それをコントローラおよび Cisco Prime Infrastructure にレポートできます。各 WLAN に対して、Voice over IP (VoIP) のスヌーピングおよびレポートを有効または無効にできます。

VoIP Media Session Aware (MSA) スヌーピングを有効にすると、この WLAN をアダプタイズするアクセス ポイント無線は、SIP RFC 3261 に準拠する SIP 音声パケットを検索します。非 RFC 3261 準拠の SIP 音声パケットや Skinny Call Control Protocol (SCCP) 音声パケットは検索しません。ポート番号 5060 に宛てた、またはポート番号 5060 からの SIP パケット (標準的な SIP シグナリングポート) はいずれも、詳細検査の対象として考慮されます。アクセス ポイントでは、Wi-Fi Multimedia (WMM) クライアントと非 WMM クライアントがコールを確立している段階、コールがアクティブになった段階、コールの終了処理の段階を追跡します。両方のクライアントタイプのアップストリームパケット分類は、アクセス ポイントで行われます。ダウンストリームパケット分類は、WMM クライアントはコントローラで、非 WMM クライアントはアクセスポ

イントで行われます。アクセスポイントは、コールの確立、終了、失敗など、主要なコールイベントをコントローラと Cisco Prime Infrastructure に通知します。

VoIP MSA コールに関する詳細な情報がコントローラによって提供されます。コールが失敗した場合、コントローラはトラブルシューティングで有用なタイムスタンプ、障害の原因 (GUIで)、およびエラーコード (CLIで) が含まれるトラップログを生成します。コールが成功した場合、追跡用にコール数とコール時間を表示します。Cisco Prime Infrastructure の [Event] ページに、失敗した VoIP コール情報が表示されます。

## メディアセッションスヌーピングの設定 (GUI)

- 
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** メディアセッションスヌーピングを設定する WLAN の ID 番号をクリックします。
- ステップ 3** [WLANs > Edit] ページで [Advanced] タブをクリックします。
- ステップ 4** [Voice] の下の [Media Session Snooping] チェックボックスをオンしてメディアセッションスヌーピングを有効にするか、オフにしてこの機能を無効にします。デフォルト値はオフです。
- ステップ 5** [Apply] をクリックします。
- ステップ 6** [Save Configuration] をクリックします。
- ステップ 7** 次の手順で、アクセスポイント無線の VoIP 統計情報を表示します。
- a) [Monitor] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] の順に選択して、[802.11a/n/ac] (または 802.11b/g/n) Radios] ページを開きます。
  - b) 右にスクロールし、VoIP 統計を表示したいアクセスポイントの [Detail] リンクをクリックします。[Radio > Statistics] ページが表示されます。  
[VoIP Stats] セクションには、このアクセスポイント無線について、音声コールの累積の数と長さが表示されます。音声コールが正常に発信されるとエントリが自動的に追加され、コントローラからアクセスポイントが解除されるとエントリが削除されます。
- ステップ 8** [Management] > [SNMP] > [Trap Logs] の順に選択して、コールが失敗した場合に生成されるトラップを表示します。[Trap Logs] ページが表示されます。  
たとえば、図のログ 0 はコールが失敗したことを示しています。ログでは、コールの日時、障害の内容、障害発生の原因が示されます。
- 

## メディアセッションスヌーピングの設定 (CLI)

- 
- ステップ 1** 特定の WLAN で VoIP スヌーピングを有効または無効にするには、次のコマンドを入力します。
- ```
config wlan call-snoop {enable | disable} wlan_id
```


ステップ 2 次のコマンドを入力して、変更を保存します。

```
save config
```

ステップ 3 特定の WLAN のメディアセッションスヌーピングのステータスを表示するには、次のコマンドを入力します。

```
show wlan wlan_id
```

以下に類似した情報が表示されます。

```
WLAN Identifier..... 1
Profile Name..... wpa2-psk
Network Name (SSID)..... wpa2-psk
Status..... Enabled
...
FlexConnect Local Switching..... Disabled
  FlexConnect Learn IP Address..... Enabled
  Infrastructure MFP protection..... Enabled (Global Infrastructure MFP
Disabled)
  Client MFP..... Optional
  Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Enabled
```

ステップ 4 メディアセッションスヌーピングが有効であり、コールがアクティブである場合の MSA クライアントのコール情報を表示するには、次のコマンドを入力します。

```
show call-control client callInfo client_MAC_address
```

以下に類似した情報が表示されます。

```
Uplink IP/port..... 192.11.1.71 / 23870
Downlonk IP/port..... 192.12.1.47 / 2070
UP..... 6
Calling Party..... sip:1054
Called Party..... sip:1000
Call ID..... 58635b00-850161b7-14853-1501a8
Number of calls for given client is..... 1
```

ステップ 5 コールが成功した場合のメトリックまたはコールが失敗した場合に生成されるトラップを表示するには、次のコマンドを入力します。

```
show call-control ap {802.11a | 802.11b} Cisco_AP {metrics | traps}
```

show call-control ap {802.11a | 802.11b} Cisco_AP metrics と入力すると、次のような情報が表示されます。

```
Total Call Duration in Seconds..... 120
Number of Calls..... 10
```

show call-control ap {802.11a | 802.11b} Cisco_AP traps と入力すると、次のような情報が表示されます。

```
Number of traps sent in one min..... 2
Last SIP error code..... 404
Last sent trap timestamp..... Jun 20 10:05:06
```

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラーコードが表示されます。次の表では、失敗したコールの考えられるエラーコードについて説明します。

表 20: 失敗した **Voice over IP (VoIP)** コールのエラーコード

| エラーコード | 整数型 | 説明 |
|--------|-----------------------------|--|
| 1 | unknown | 不明なエラー。 |
| 400 | badRequest | 構文が不正であるため要求を認識できませんでした。 |
| 401 | unauthorized | 要求にはユーザ認証が必要です。 |
| 402 | paymentRequired | 将来的な使用のために予約されています。 |
| 403 | forbidden | サーバは要求を認識しましたが、実行を拒否しています。 |
| 404 | notFound | サーバは、このユーザが Request-URI に指定されたドメインに存在しないという情報を持っています。 |
| 405 | methodNotAllowed | Request-Line で指定されたメソッドが認識されているものの、Request-URI で指定されたアドレスでは許可されていません。 |
| 406 | notAcceptabl | 要求によって指定されたリソースは、送信された要求内の [Accept] ヘッダーテキストボックスによって許容されないコンテンツ特性を持つ応答エンティティしか生成できません。 |
| 407 | proxyAuthenticationRequired | クライアントは、最初にプロキシで認証される必要があります。 |
| 408 | requestTimeout | サーバは、時間内にユーザのロケーションを確認できなかったため、適切な時間内に応答を作成できませんでした。 |
| 409 | conflict | リソースの現在の状態と競合したために、要求を完了できませんでした。 |
| 410 | gone | 要求されたリソースがサーバで使用できず、転送アドレスが不明です。 |

| エラーコード | 整数型 | 説明 |
|--------|-------------------------|---|
| 411 | lengthRequired | 要求のエンティティ自体が、サーバが処理を想定しているサイズ、または処理できるサイズより大きいため、サーバが要求の処理を拒否しています。 |
| 413 | requestEntityTooLarge | 要求のエンティティ自体が、サーバが処理を想定しているサイズ、または処理できるサイズより大きいため、サーバが要求の処理を拒否しています。 |
| 414 | requestURITooLarge | Request-URI がサーバが解釈を想定している長さよりも長いために、サーバが要求の処理を拒否しています。 |
| 415 | unsupportedMediaType | 要求されたメソッドについて、要求のメッセージ本文の形式がサーバでサポートされていないために、サーバが要求の処理を拒否しています。 |
| 420 | badExtension | Proxy-Require または Require ヘッダー テキスト ボックスで指定されたプロトコル拡張が、サーバで認識されませんでした。 |
| 480 | temporarilyNotAvailable | 着信側のエンドシステムが正常に通信できるものの、着信側が現在、利用不能です。 |
| 481 | callLegDoesNotExist | User-Agent Server (UAS; ユーザ エージェント サーバ) が既存のダイアログまたはトランザクションと一致していない要求を受け取りました。 |
| 482 | loopDetected | サーバはループを検出しました。 |
| 483 | tooManyHops | サーバは Max-Forwards ヘッダー テキスト ボックスの値が 0 である要求を受信しました。 |
| 484 | addressIncomplete | サーバは Request-URI が不完全である要求を受信しました。 |
| 485 | ambiguous | Request-URI があいまいです。 |
| 486 | busy | 着信側のエンドシステムは正常に接続されましたが、着信側は現在、このエンドシステムで追加のコールを受け入れようとしないうか、受け入れることができません。 |
| 500 | internalServerError | サーバで、要求の処理を妨げる予期しない状態が発生しました。 |

| エラーコード | 整数型 | 説明 |
|--------|----------------------|---|
| 501 | notImplemented | サーバは要求を処理するために必要な機能をサポートしていません。 |
| 502 | badGateway | ゲートウェイまたはプロキシとして機能しているサーバが、要求を処理するためにアクセスしたダウンストリームサーバから無効な応答を受信しました。 |
| 503 | serviceUnavailable | 一時的な過負荷またはメンテナンスのために、サーバが一時的に要求を処理できなくなっています。 |
| 504 | serverTimeout | サーバは、要求を処理するためにアクセスした外部サーバから時間内に応答を受信しませんでした。 |
| 505 | versionNotSupported | サーバは、要求で使用された SIP プロトコルのバージョンをサポートしていないか、サポートを拒否しています。 |
| 600 | busyEverywhere | 着信側のエンドシステムは正常に接続されましたが、着信側はこの時点でビジーであるか、コールに応答しようとしていません。 |
| 603 | decline | 着信側のマシンは正常に接続されましたが、ユーザが参加しようとしていないか、参加できません。 |
| 604 | doesNotExistAnywhere | サーバには、Request-URI で示されたユーザが存在しないという情報があります。 |
| 606 | notAcceptable | ユーザのエージェントは正常に接続されましたが、セッションの説明の一部（メディア、帯域幅、アドレス指定形式など）が受け入れられませんでした。 |

(注) メディアセッションスヌーピングに関する問題が発生した場合は、**debug call-control {all|event} {enable|disable}** コマンドを入力して、すべてのメディアセッションスヌーピングメッセージまたはイベントをデバッグしてください。



第 91 章

Key Telephone System-Based CAC の設定

- [Key Telephone System-Based CAC の制約事項](#), 735 ページ
- [Key Telephone System-Based CAC について](#), 735 ページ
- [KTS-based CAC の設定 \(GUI\)](#), 736 ページ
- [KTS-based CAC の設定 \(CLI\)](#), 736 ページ

Key Telephone System-Based CAC の制約事項

- コントローラは、クライアントからの SSID Capability Check Request メッセージを無視しません。
- KTS CAC クライアントには、優先コールはサポートされていません。
- コントローラ間ローミングには、理由コード 17 はサポートされていません。
- KTS-based CAC 機能を有効にするには、次の作業を行ってください。
 - WLAN 上で WMM を有効にします。
 - 無線レベルで ACM を有効にします。
 - 無線レベルでの TSPEC 非アクティブ タイムアウトの処理を有効にします。

Key Telephone System-Based CAC について

Key Telephone System-based CAC は、NEC MH240 ワイヤレス IP 電話で使用されるプロトコルです。KTS-based SIP クライアントで CAC をサポートし、そのようなクライアントからの帯域幅要求メッセージを処理し、AP 無線で要求された帯域幅を割り当て、プロトコルの一部であるその他のメッセージを処理するように、コントローラを設定できます。

コールが開始されると、KTS-based CAC クライアントが帯域幅要求メッセージを送信し、それに対してコントローラが、帯域幅が割り当てられるかどうかを示す帯域幅確認メッセージで応答し

ます。帯域幅が利用可能な場合のみ、コールが許可されます。クライアントは、APから別のAPにローミングする場合、別の帯域幅要求メッセージをコントローラに送信します。

帯域幅の割り当ては、帯域幅要求メッセージからのデータレートとパケット化間隔を使用して計算されるメディア時間によって異なります。KTS-based CAC クライアントの場合、パケット化間隔が 20 ミリ秒の G.711 コーデックが、メディア時間の計算に使用されます。

コントローラは、クライアントからの帯域幅リリースメッセージを受信したあと、帯域幅を解放します。コントローラ内ローミングとコントローラ間ローミングのいずれの場合も、クライアントが別の AP にローミングすると、コントローラは前の AP の帯域幅を解放し、新規の AP に帯域幅を割り当てます。クライアントのアソシエーションが解除された場合、または非アクティブの状態が 120 秒間続いた場合、コントローラは帯域幅を解放します。クライアントの非アクティブまたはディスアソシエーションによって、クライアント用の帯域幅が解放された場合、コントローラからクライアントへの通知はありません。

KTS-based CAC の設定 (GUI)

はじめる前に

WLAN に対して KTS-based CAC を有効にするには、次の作業を実行します。

- WLAN の QoS プロファイルを Platinum に設定します。
- WLAN を Disabled 状態に設定します。
- WLAN に対する FlexConnect ローカルスイッチングを Disabled 状態にします ([WLANs> Edit] ページの [Advanced] タブをクリックし、[FlexConnect Local Switching] チェックボックスをオフにします)。

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 KTS-based CAC ポリシーを設定する WLAN の ID 番号をクリックします。

ステップ 3 [WLANs> Edit] ページで [Advanced] タブをクリックします。

ステップ 4 [Voice] の下の [KTS based CAC Policy] チェックボックスをオンまたはオフにして、WLAN に対する KTS-based CAC を有効または無効にします。

ステップ 5 [Apply] をクリックして、変更を確定します。

KTS-based CAC の設定 (CLI)

はじめる前に

WLAN に対して KTS-based CAC を有効にするには、次の作業を実行します。

- WLAN の QoS プロファイルを Platinum に設定するには、次のコマンドを入力します。

config wlan qos wlan-id platinum

- WLAN を無効にするには、次のコマンドを入力します。

config wlan disable wlan-id

- WLAN に対する FlexConnect ローカル スイッチングを無効にするには、次のコマンドを入力します。

config wlan flexconnect local-switching wlan-id disable

ステップ 1 WLAN に対して KTS-based CAC を有効にするには、次のコマンドを入力します。

config wlan kts-cac enable wlan-id

ステップ 2 KTS-based CAC 機能を有効にするには、次の作業を行ってください。

- a) WLAN 上で WMM を有効にするには、次のコマンドを入力します。

config wlan wmm allow wlan-id

- b) 無線レベルで ACM を有効にするには、次のコマンドを入力します。

config 802.11a cac voice acm enable

- c) 無線レベルで TSPEC 非アクティブ タイムアウトの処理を有効にするには、次のコマンドを入力します。

config 802.11a cac voice tspec-inactivity-timeout enable

関連コマンド

- クライアントが KTS-based CAC をサポートするかどうかを確認するには、次のコマンドを入力します。

show client detail client-mac-address

以下に類似した情報が表示されます。

```
Client MAC Address..... 00:60:b9:0d:ef:26
Client Username ..... N/A
AP MAC Address..... 58:bc:27:93:79:90

QoS Level..... Platinum
802.1P Priority Tag..... disabled
KTS CAC Capability..... Yes
WMM Support..... Enabled
Power Save..... ON
```

- KTS-based CAC に関する問題をトラブルシューティングするには、次のコマンドを入力します。

debug cac kts enable

- CAC に関する他の問題をトラブルシューティングするには、次のコマンドを入力します。

- **debug cac event enable**

- **debug call-control all enable**



第 92 章

ローミングしている音声クライアントのリアンカーの設定

- [ローミングしている音声クライアントのリアンカーの設定に関する制約事項](#)、739 ページ
- [ローミングしている音声クライアントのリアンカーについて](#)、739 ページ
- [ローミングしている音声クライアントのリアンカーの設定 \(GUI\)](#)、740 ページ
- [ローミングしている音声クライアントのリアンカーの設定 \(CLI\)](#)、740 ページ

ローミングしている音声クライアントのリアンカーの設定に関する制約事項

- 継続中のデータセッションは、アソシエーション解除とその後の再アソシエーションによる影響を受ける場合があります。
- この機能は、アドミッション制御を有効にしている場合のみ、TSPEC-based コールおよび非 TSPEC SIP-based コールに対してサポートされます。
- この機能を Cisco 792x 電話機で使用することは推奨されません。

ローミングしている音声クライアントのリアンカーについて

音声クライアントが、最も適切で最も近くの使用可能コントローラにアンカーされるようにすることができます。この機能は、コントローラ間ローミングが発生したときに役立ちます。この機能を使用することにより、トラフィックの伝送に外部コントローラとアンカーコントローラ間のトンネルを使用せずに済み、ネットワークから不要なトラフィックを削除できます。

ローミング中のコールは影響を受けず、問題なく継続できます。トラフィックは、外部コントローラとアンカーコントローラ間に確立される適切なトンネルを通過します。アソシエーション

解除は、コールの終了後のみに行われ、その後、クライアントは新規のコントローラに再アソシエートされます。



(注) WLAN ごとに音声クライアントのローミングのリアンカーが可能です。

ローミングしている音声クライアントのリアンカーの設定 (GUI)

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 ローミングしている音声クライアントのリアンカーを設定する WLAN の ID 番号をクリックします。
- ステップ 3 [WLANs > Edit] ページが表示されたら、[Advanced] タブを選択して [WLANs > Edit] ([Advanced]) ページを開きます。
- ステップ 4 [Voice] エリアで、[Re-anchor Roamed Clients] チェックボックスを選択します。
- ステップ 5 [Apply] をクリックして、変更を確定します。
- ステップ 6 [Save Configuration] をクリックして、変更を保存します。

ローミングしている音声クライアントのリアンカーの設定 (CLI)

- ステップ 1 特定の WLAN に対して、ローミングしている音声クライアントのリアンカーを有効または無効にするには、次のコマンドを入力します。
config wlan roamed-voice-client re-anchor {enable | disable} wlan id
- ステップ 2 次のコマンドを入力して、変更を保存します。
save config
- ステップ 3 特定の WLAN におけるローミングしている音声クライアントのリアンカーのステータスを表示するには、次のコマンドを入力します。
show wlan wlan_id
以下に類似した情報が表示されます。

```
WLAN Identifier..... 1
Profile Name..... wpa2-psk
Network Name (SSID)..... wpa2-psk
Status..... Enabled
...
Call Snooping..... Enabled
Roamed Call Re-Anchor Policy..... Enabled
```

```
Band Select..... Disabled
Load Balancing..... Disabled
```

ステップ 4 次のコマンドを入力して、変更を保存します。
save config



第 93 章

シームレスな IPv6 モビリティの設定

- [IPv6 モビリティを設定するための前提条件, 743 ページ](#)
- [IPv6 モビリティの設定に関する制約事項, 744 ページ](#)
- [IPv6 モビリティについて, 744 ページ](#)
- [IPv6 のグローバルな設定, 745 ページ](#)
- [IPv6 クライアントのための RA ガードの設定, 745 ページ](#)
- [IPv6 クライアントのための RA スロットリングの設定, 746 ページ](#)
- [IPv6 ネイバー ディスカバリ キャッシングの設定, 748 ページ](#)

IPv6 モビリティを設定するための前提条件

- クライアントごとに最大 8 個のクライアントアドレスを追跡できます。
- ステートフル DHCPv6 IP アドレス指定を正常に動作させるには、DHCPv6 サーバとして機能するように設定された、DHCP for IPv6 機能をサポートするスイッチまたはルータを設置する必要があります。または、組み込みの DHCPv6 サーバを備えた、Windows 2008 サーバなどの専用サーバが必要です。

シームレスな IPv6 モビリティをサポートするには、次の設定が必要になる場合があります。

- [IPv6 クライアントのための RA ガードの設定](#)
- [IPv6 クライアントのための RA スロットリングの設定](#)
- [IPv6 ネイバー ディスカバリ キャッシングの設定](#)

IPv6 モビリティの設定に関する制約事項

- クライアントは、スタティック ステートレス自動設定 (Windows XP クライアントなど) またはステートフル DHCPv6 IP アドレス指定 (Windows Vista クライアントなど) のいずれかで IPv6 をサポートする必要があります。



(注) 現在、DHCPv6 は Windows Vista クライアントでの使用についてのみサポートされています。これらのクライアントについては、VLAN がクライアントによって変更された後で DHCPv6 IP アドレスを手動で更新する必要があります。



(注) IPv6 のダイナミック VLAN 機能はサポートされていません。

- タグなしインターフェイスにマッピングされている WLAN に関連付けられた IPv6 クライアントが、タグなしインターフェイスにマッピングされている別の WLAN にローミングすることはサポートされていません。
- 7.4 リリースでは、同じモビリティグループ、同じ VLAN ID、および異なる IPv4 および IPv6 サブネットがある WLC は、それぞれの IPv6 ルータ アドバタイズメントを生成します。これらの WLC の WLAN は、すべてのコントローラで同じ VLAN ID を持つ同じ動的インターフェイスに割り当てられます。クライアントは正しい IPv4 アドレスを受信します。ただし他の WLC に到達する別のサブネットからルータ アドバタイズメントを受信します。クライアントに最初に渡された IPv6 アドレスが IPv4 アドレスのサブネットに一致しないため、クライアントからのトラフィックがないという問題が生じる可能性があります。これを解決するために、異なるモビリティグループの WLC を設定できます。



(注) IPv6 モビリティ ピアの追加または削除時に、トラフィックをバイパスするための SSH ルールが 16666 ポートおよびモビリティ ピアの IP ペアに適用されます。

IPv6 モビリティについて

インターネットプロトコルバージョン 6 (IPv6) は、プロトコルの TCP/IP スイートのバージョン 4 (IPv4) の後継となることを意図された次世代のネットワーク層インターネットプロトコルです。この新しいバージョンでは、一意なグローバル IP アドレスを必要とするユーザとアプリケーションを収容するためのインターネットグローバルアドレス空間が拡張されています。IPv6 は、128 ビットの送信元アドレスおよび宛先アドレスを組み込むことにより、32 ビットの IPv4 アドレスよりも格段に多くのアドレスを提供します。

コントローラをまたいだ IPv6 クライアントをサポートするには、IPv6 クライアントが同じレイヤ 3 ネットワーク上にとどまるように、ICMPv6 メッセージを特別に処理する必要があります。コントローラは、ICMPv6 メッセージを代行受信することで IPv6 クライアントを追跡し、シームレスなモビリティを提供して、ネットワーク攻撃からネットワークを保護します。ICMPv6 パケットは、マルチキャストからユニキャストに変換され、クライアントごとに個別に配信されます。このプロセスによって、より詳細な制御が可能になります。特定のクライアントは、特定のネイバーディスカバリ パケットおよびルータ アドバタイズメント パケットを受信することで IPv6 アドレス指定が適切であることを確認し、不要なマルチキャストトラフィックを回避します。

IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。コントローラは、同じモビリティ グループに属している必要があります。IPv4 と IPv6 の両クライアント モビリティが、デフォルトで有効になります。

IPv6 のグローバルな設定

IPv6 のグローバルな設定 (GUI)

-
- ステップ 1 [Controller] > [General] を選択します。
 - ステップ 2 [Global IPv6 Config] ドロップダウン リストから、[Enabled] または [Disabled] 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 [Save Configuration] をクリックします。
-

IPv6 のグローバルな設定 (CLI)

IPv6 をグローバルに設定するには、次のコマンドを使用します。

- 次のコマンドを入力して、IPv6 をグローバルに有効または無効にします。
config ipv6 {enable | disable}

IPv6 クライアントのための RA ガードの設定

RA ガードについて

IPv6 クライアントは、IPv6 アドレスを設定し、IPv6 ルータ アドバタイズメント (RA) パケットに基づいてルータ テーブルにデータを入力します。RA ガード機能は、有線ネットワークの RA ガード機能に類似しています。RA ガードは、ワイヤレス クライアントから発信される不要な、または不正な RA パケットをドロップすることによって、IPv6 ネットワークのセキュリティを強

化します。この機能が設定されていないと、悪意のある IPv6 クライアントが、それ自体をネットワークのルータとして通知する可能性があり、そのため、正規の IPv6 ルータよりも優先されることになります。

RA ガードは、コントローラで実行されます。アクセス ポイントまたはコントローラで RA メッセージをドロップするように、コントローラを設定できます。デフォルトでは、RA ガードはアクセス ポイントで設定され、コントローラでも有効になります。すべての IPv6 RA メッセージがドロップされ、それによって他のワイヤレス クライアントおよびアップストリーム有線ネットワークが悪意のある IPv6 クライアントから保護されます。



(注) RA ガードは、FlexConnect ローカル スイッチング モードでもサポートされています。

RA ガードの設定 (GUI)

- ステップ 1 [Controller] > [IPv6] > [RA Guard] を選択して、[IPv6 RA Guard] ページを開きます。デフォルトでは、[IPv6 RA Guard on AP] が有効になります。
- ステップ 2 RA ガードを無効にするには、ドロップダウンリストから、[Disable] を選択します。コントローラは、RA パケットの送信側として識別されたクライアントも表示します。
- ステップ 3 [Apply] をクリックして、変更を確定します。
- ステップ 4 [Save Configuration] をクリックして、変更を保存します。

RA ガードの設定 (CLI)

RA ガードを設定するには、次のコマンドを使用します。

```
config ipv6 ra-guard ap {enable | disable}
```

IPv6 クライアントのための RA スロットリングの設定

RA スロットリングについて

RA スロットリングは、コントローラがワイヤレス ネットワーク宛での RA パケットを強制的に制限できるようにします。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。これは、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミングクライアントが RA スロットリングの影響を受けないようにすることができます。

RA スロットリングの設定 (GUI)

ステップ 1 [Controll] > [IPv6] > [RA Throttle Policy] ページを選択します。デフォルトでは、[IPv6 RA Throttle Policy] が無効になります。このチェックボックスをオフにして、RA スロットリングポリシーを無効にします。

ステップ 2 次のパラメータを設定します。

- [Throttle period] : スロットリングの期間。RA スロットリングは、VLAN に対する [Max Through] 制限に達した後、または特定のルータに対する [Allow At-Most] 値に達した後のみ実行されます。範囲は 10 ~ 86400 秒です。デフォルトは 600 秒です。
 - [Max Through] : スロットリングが実行される前に送信可能な、VLAN 上の RA パケットの最大数。[No Limit] オプションは、スロットリングを使用せずに、無制限の RA パケット数を許可します。範囲は 0 ~ 256 RA パケットです。デフォルトは 10 RA パケットです。
 - [Interval Option] : このオプションは、IPv6 RA パケットに設定された RFC 3775 値に基づいた、さまざまなコントローラの動作を許可します。
 - [Passthrough] : RFC 3775 インターバル オプションが指定された RA メッセージが、スロットリングなしで通過することを許可します。
 - [Ignore] : RA スロットルが、インターバル オプションの指定されたパケットを通常の RA として処理し、有効である場合はスロットリングが適用されるようにします。
 - [Throttle] : インターバル オプションが指定された RA パケットに、常にレート制限が適用されるようにします。
 - [Allow At-least] : スロットリングが実行される前にマルチキャストとして送信できる、ルータごとの RA パケットの最小数。範囲は 0 ~ 32 RA パケットです。
 - [Allow At-most] : スロットリングが実行される前にマルチキャストとして送信できる、ルータごとの RA パケットの最大数。[No Limit] オプションは、ルータの通過する無制限の RA パケット数を許可します。範囲は 0 ~ 256 RA パケットです。
- (注) RA スロットリングが実行されると、最初の IPv6 対応ルータのみの通過が許可されます。異なるルータが複数の IPv6 プレフィックスを処理しているネットワークについては、RA スロットリングを無効にしてください。

ステップ 3 [Apply] をクリックして、変更を確定します。

ステップ 4 [Save Configuration] をクリックして、変更を保存します。

RA スロットルポリシーの設定 (CLI)

RA スロットルポリシーを設定するには、次のコマンドを使用します。

```
config ipv6 neighbor-binding ra-throttle {allow at-least at-least-value | enable | disable | interval-option
{ ignore | passthrough | throttle } | max-through {max-through-value | no-limit}}
```

IPv6 ネイバー ディスカバリ キャッシングの設定

IPv6 ネイバー ディスカバリについて

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー ディスカバリ 検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。コントローラ内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

ネイバー バインディングの設定 (GUI)

ステップ 1 [Controller] > [IPv6] > [Neighbor Binding] ページを選択します。

ステップ 2 次を設定します。

- [Down-Lifetime] : インターフェイスがダウンした場合に、IPv6 キャッシュ エントリを保持する時間を指定します。範囲は 0 ~ 86400 秒です。
- [Reachable-Lifetime] : IPv6 アドレスがアクティブである時間を指定します。範囲は 0 ~ 86400 秒です。
- [Stale-Lifetime] : IPv6 アドレスをキャッシュに保持する時間を指定します。範囲は 0 ~ 86400 秒です。

ステップ 3 [Unknown Address Multicast NS Forwarding] を有効または無効にします。

ステップ 4 [NA Multicast Forwarding] を有効または無効にします。

[NA Multicast Forwarding] を有効にすると、有線/無線からのすべての未承認マルチキャスト NA は無線に転送されません。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

ネイバー バインディングの設定 (CLI)

- 次のコマンドを入力して、ネイバー バインディング パラメータを設定します。
config ipv6 neighbor-binding timers {down-lifetime | reachable-lifetime | stale-lifetime} {enable | disable}
- 次のコマンドを入力して、不明なアドレス マルチキャスト NS の転送を設定します。
config ipv6 ns-mcast-fwd {enable | disable}
- 次のコマンドを入力して、NA マルチキャストの転送を設定します。
config ipv6 na-mcast-fwd {enable | disable}

[NA Multicast Forwarding] を有効にすると、有線/無線からのすべての未承認マルチキャスト NA は無線に転送されません。



第 94 章

Cisco Client Extensions の設定

- [Cisco Client Extensions を設定するための前提条件](#), 751 ページ
- [Cisco Client Extensions の設定に関する制約事項](#), 751 ページ
- [Cisco Client Extensions について](#), 752 ページ
- [CCX Aironet IE の設定 \(GUI\)](#), 752 ページ
- [クライアントの CCX バージョンの表示 \(GUI\)](#), 752 ページ
- [CCX Aironet IE の設定 \(CLI\)](#), 753 ページ
- [クライアントの CCX バージョンの表示 \(CLI\)](#), 753 ページ

Cisco Client Extensions を設定するための前提条件

- ソフトウェアは、CCX バージョン 1～5 をサポートします。これによって、コントローラとそのアクセス ポイントは、CCX をサポートするサードパーティ製クライアントデバイスと無線で通信できます。CCX サポートは、コントローラ上の各 WLAN に対して自動的に有効になり、無効にすることはできません。ただし、Aironet Information Element (IE) を設定できます。
- Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85 (アクセス ポイント名、ロード、アソシエートされたクライアントの数などを含む) をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、コントローラは、Aironet IEs 0x85 および 0x95 (コントローラの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む) を再アソシエーション要求に格納して送信します。

Cisco Client Extensions の設定に関する制約事項

- CCX は、Cisco OEAP 600 アクセス ポイントではサポートされず、CCX に関連する要素もすべてがサポートされるわけではありません。

- Cisco OEAP 600 では、Cisco Aeronet IE をサポートしていません。
- 7.2 リリースでは、CCX Lite と呼ばれる新規バージョンの CCX を使用できます。CCX Lite の詳細については、http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html を参照してください。

Cisco Client Extensions について

Cisco Client Extensions (CCX) ソフトウェアは、サードパーティ製クライアントデバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアントデバイスは、シスコ製のアクセスポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアントデバイスがサポートしていないシスコの機能もサポートできるようになります。

CCX Aironet IE の設定 (GUI)

-
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
 - ステップ 2 必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。
 - ステップ 3 [Advanced] タブを選択して、[WLANs > Edit] ([Advanced] タブ) ページを開きます。
 - ステップ 4 この WLAN で Aironet IE のサポートを有効にする場合は、[Aironet IE] チェックボックスをオンにします。有効にしない場合には、このチェックボックスをオフにします。デフォルト値が有効 (オン) になっています。
 - ステップ 5 [Apply] をクリックして、変更を確定します。
 - ステップ 6 [Save Configuration] をクリックして、変更を保存します。
-

クライアントの CCX バージョンの表示 (GUI)

クライアントデバイスは、アソシエーション要求パケットに CCX バージョンを格納してアクセスポイントに送信します。コントローラは、クライアントの CCX バージョンをデータベースに格納し、これを使用してこのクライアントの機能を制限します。たとえば、クライアントが CCX バージョン 2 をサポートしている場合、コントローラは、CCX バージョン 4 の機能を使用することをクライアントに許可しません。

-
- ステップ 1 [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。
 - ステップ 2 目的のクライアントデバイスの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。

[CCX Version] テキスト ボックスに、このクライアント デバイスでサポートされる CCX バージョンが表示されます。クライアントで CCX がサポートされていない場合は、*Not Supported* が表示されます。

ステップ 3 前の画面に戻るには、[Back] をクリックします。

ステップ 4 他のクライアント デバイスでサポートされる CCX バージョンを表示するには、この手順を繰り返します。

CCX Aironet IE の設定 (CLI)

CCX Aironet IE を設定するには、次のコマンドを使用します。

```
config wlan ccx aironet-ie {enable | disable} wlan_id
```

デフォルト値はイネーブルです。

クライアントの CCX バージョンの表示 (CLI)

コントローラの CLI を使用して、特定のクライアント デバイスでサポートされる CCX バージョンを表示するには、次のコマンドを入力します。

```
show client detail client_mac
```




第 95 章

リモート LAN の設定

- [リモート LAN を設定するための前提条件](#), 755 ページ
- [リモート LAN の設定に関する制約事項](#), 755 ページ
- [リモート LAN について](#), 756 ページ
- [リモート LAN の設定 \(GUI\)](#), 756 ページ
- [リモート LAN の設定 \(CLI\)](#), 757 ページ

リモート LAN を設定するための前提条件

- リモート LAN 機能をサポートしないリリースに移行する前に、コントローラの設定からすべてのリモート LAN を削除する必要があります。以前のリリースでは、リモート LAN が WLAN に変わり、そのことが、ワイヤレス ネットワーク上で不要な WLAN または安全でない WLAN をブロードキャストする原因となっていました。リモート LAN は、リリース 7.0.116.0 以降でのみサポートされています。
- リモート LAN は、OEAP 600 シリーズ アクセス ポイントの専用の LAN ポートに適用できません。

リモート LAN の設定に関する制約事項

- OEAP 600 シリーズ アクセス ポイントにリモート LAN ポートを介して接続できるクライアントは、4 つのみです。この接続クライアントの数は、コントローラ WLAN での WLAN の制限数 (15) には影響しません。リモート LAN のクライアント制限では、リモート LAN ポートにスイッチまたはハブを接続して複数のデバイスを接続することや、このポートに接続している Cisco IP フォンに直接接続することは可能です。接続できるデバイスは 4 つまでです。これは、この 4 つのデバイスの 1 つのアイドル時間が 1 分を超えるまで適用されます。

- コントローラの GUI を使用してリモート LAN に 802.1X を設定することはできません。CLI を使用した設定のみがサポートされています。

リモート LAN について

このセクションでは、リモート LAN の設定方法について説明します。

リモート LAN の設定 (GUI)

- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
このページでは、コントローラ上で現在設定されているすべての WLAN およびリモート LAN が表示されます。各 WLAN について、WLAN/リモート LAN ID、プロファイル名、タイプ、SSID、ステータス、およびセキュリティ ポリシーを表示できます。
- WLAN/リモート LAN の合計数がページの右上隅に表示されます。WLAN/リモート LAN のリストが複数ページにわたる場合は、ページ番号のリンクをクリックすることで、目的のページにアクセスできます。
- (注) リモート LAN を削除する場合は、カーソルを目的の WLAN の青いドロップダウン矢印の上に置いて、[Remove] を選択するか、または行の左側のチェックボックスをオンにして、ドロップダウンリストから [Remove Selected] を選択し、[Go] をクリックします。決定を確認するメッセージが表示されます。作業を続行すると、割り当てられているアクセスポイントグループおよびアクセスポイント無線からそのリモート LAN が削除されます。
- ステップ 2** ドロップダウンリストから [Create New] を選択し、[Go] をクリックして新規の Remote-LAN を作成します。[WLANs > New] ページが表示されます。
- ステップ 3** [Type] ドロップダウンリストから、[Remote LAN] を選択してリモート LAN を作成します。
- ステップ 4** [Profile Name] テキストボックスに、このリモート WLAN に割り当てるプロファイル名に対する最大 32 文字の英数字を入力します。プロファイル名は固有である必要があります。
- ステップ 5** [WLAN ID] ドロップダウンリストから、この WLAN の ID 番号を選択します。
- ステップ 6** [Apply] をクリックして、変更を確定します。[WLANs > Edit] ページが表示されます。
- (注) 編集する WLAN の ID 番号をクリックすることにより、[WLANs] ページから [WLANs > Edit] ページを開くこともできます。
- ステップ 7** [General] タブ、[Security] タブ、および [Advanced] タブ上でパラメータを使用してこのリモート LAN を設定します。特定の機能を設定する手順については、この章の後の項を参照してください。
- ステップ 8** [General] タブの [Status] チェックボックスをオンにして、このリモート LAN を有効にします。リモート LAN に対する設定変更が終了するまで、チェックボックスをオフにしておいてください。
- (注) また、[WLANs] ページから、有効化または無効化する ID の左側のチェックボックスをオンにして、ドロップダウンリストから [Enable Selected] または [Disable Selected] を選択し、[Go] をクリックすることでも、リモート LAN を有効化または無効化できます。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

リモート LAN の設定 (CLI)

- リモート LAN の現在の設定を表示するには、次のコマンドを入力します。

```
show remote-lan remote-lan-id
```

- リモート LAN を有効または無効にするには、次のコマンドを入力します。

```
config remote-lan {enable | disable} remote-lan-id
```

- リモート LAN に対して 802.1X 認証を有効または無効にするには、次のコマンドを入力します。

```
config remote-lan security 802.1X {enable | disable} remote-lan-id
```



(注) リモート LAN 上の暗号化は、常に「none」になります。

- 認証サーバとしてコントローラを使用するローカル EAP を有効または無効にするには、次のコマンドを入力します。

```
config remote-lan local-auth enable profile-name remote-lan-id
```

- 外部の AAA 認証サーバを使用している場合は、次のコマンドを使用します。

```
config remote-lan radius_server auth {add | delete} remote-lan-id server id
```

```
config remote-lan radius_server auth {enable | disable} remote-lan-id
```




第 96 章

AP グループの設定

- [AP グループを設定するための前提条件, 759 ページ](#)
- [アクセス ポイント グループの設定に関する制約事項, 760 ページ](#)
- [アクセス ポイント グループについて, 761 ページ](#)
- [アクセス ポイント グループの設定, 762 ページ](#)
- [アクセス ポイント グループの作成 \(GUI\) , 763 ページ](#)
- [アクセス ポイント グループの作成 \(CLI\) , 765 ページ](#)
- [アクセス ポイント グループの表示 \(CLI\) , 766 ページ](#)

AP グループを設定するための前提条件

次に、コントローラでアクセス ポイント グループを作成するための前提条件を示します。

- VLAN またはサブネットにサービスを提供するルータ上で、必要なアクセス コントロール リスト (ACL) を定義する必要があります。
- アクセス ポイント グループ VLAN では、マルチキャスト トラフィックがサポートされません。ただし、クライアントがあるアクセス 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、IGMP スヌーピングが有効になっていないと、クライアントによってマルチキャスト トラフィックの受信が停止されることがあります。

コントローラ プラットフォームでサポートされる AP グループ

次の表に、各種コントローラ プラットフォームでサポートされる AP グループを示します。

| コントローラ プラットフォーム | サポートされる AP グループ |
|------------------------------|-----------------|
| Cisco 2500 シリーズ ワイヤレス コントローラ | 50 |
| Cisco 5500 シリーズ ワイヤレス コントローラ | 500 |

| コントローラ プラットフォーム | サポートされる AP グループ |
|----------------------------------|-----------------|
| シスコ仮想ワイヤレス コントローラ | 200 |
| Cisco 7500 シリーズ ワイヤレス コントローラ | 6000 |
| Cisco 8500 シリーズ ワイヤレス コントローラ | 6000 |
| Cisco Wireless Services Module 2 | 1000 |

アクセス ポイント グループの設定に関する制約事項

- APグループテーブル内のWLANに対するインターフェイスマッピングが、WLANインターフェイスと同じであるとしてします。WLANインターフェイスが変更されると、APグループテーブル内のWLANに対するインターフェイスマッピングも新しいWLANインターフェイスに変わります。
APグループテーブル内のWLANに対するインターフェイスマッピングが、WLANに定義されたインターフェイスと異なるとしてします。WLANインターフェイスが変更されても、APグループテーブル内のWLANに対するインターフェイスマッピングは新しいWLANインターフェイスに変わりません。
- コントローラ上の設定をクリアすると、アクセスポイントグループのすべてが非表示となります。ただし、デフォルトのアクセスポイントグループである「default-group」（自動的に作成される）は例外です。
- デフォルトのアクセスポイントグループには、最大16のWLANを関連付けることができます。デフォルトのアクセスポイントグループのWLAN IDは、16以下である必要があります。大規模なデフォルトのアクセスポイントグループ内でIDが16以上のWLANが作成されると、WLAN SSIDはブロードキャストされません。デフォルトのアクセスポイントグループのすべてのWLAN IDでIDが16以下であることが必要です。16を超えるIDを含むWLANは、カスタムアクセスポイントグループに割り当てることができます。
- OEAP 600 シリーズ アクセスポイントでは、最大で2つのWLANと1つのリモートLANがサポートされます。3つ以上のWLANと1つのリモートLANを設定した場合は、APグループに600シリーズアクセスポイントを割り当てることができます。2つのWLANと1つのリモートLANのサポートもAPグループに適用されますが、600シリーズOEAPがデフォルトグループにある場合、WLANまたはリモートLAN IDを7以下にする必要があります。
- OfficeExtend アクセスポイントはすべて同じアクセスポイントグループ内にあり、このグループに含まれるWLANは最大15個にする必要があります。アクセスポイントグループ内のOfficeExtendアクセスポイントを持つコントローラは、パーソナルなSSIDに対して割り当てられるWLANが1つであるため、接続されている各OfficeExtendアクセスポイントに最大15個のWLANしか公開しません。



- (注) アクセスポイントグループ内の OfficeExtend アクセスポイントを持つコントローラは、パーソナルな SSID に対して割り当てられる WLAN が 1 つであるため、接続されている各 OfficeExtend アクセスポイントに最大 15 の WLAN を公開します。

アクセスポイントグループについて

コントローラ上に最大 512 の WLAN を作成した後では、さまざまなアクセスポイントに WLAN を選択的に公開（アクセスポイントグループを使用して）することで、ワイヤレスネットワークをより適切に管理できます。一般的な展開では、WLAN 上のすべてのユーザはコントローラ上の 1 つのインターフェイスにマップされます。したがって、WLAN に関連付けられているすべてのユーザは、同じサブネットまたは VLAN に存在します。しかし、複数のインターフェイス間で負荷を分散すること、またはアクセスポイントグループを作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループユーザへと負荷を分配することを選択できます。さらに、ネットワーク管理を簡素化するために、これらのアクセスポイントグループを別個の VLAN で設定できます。

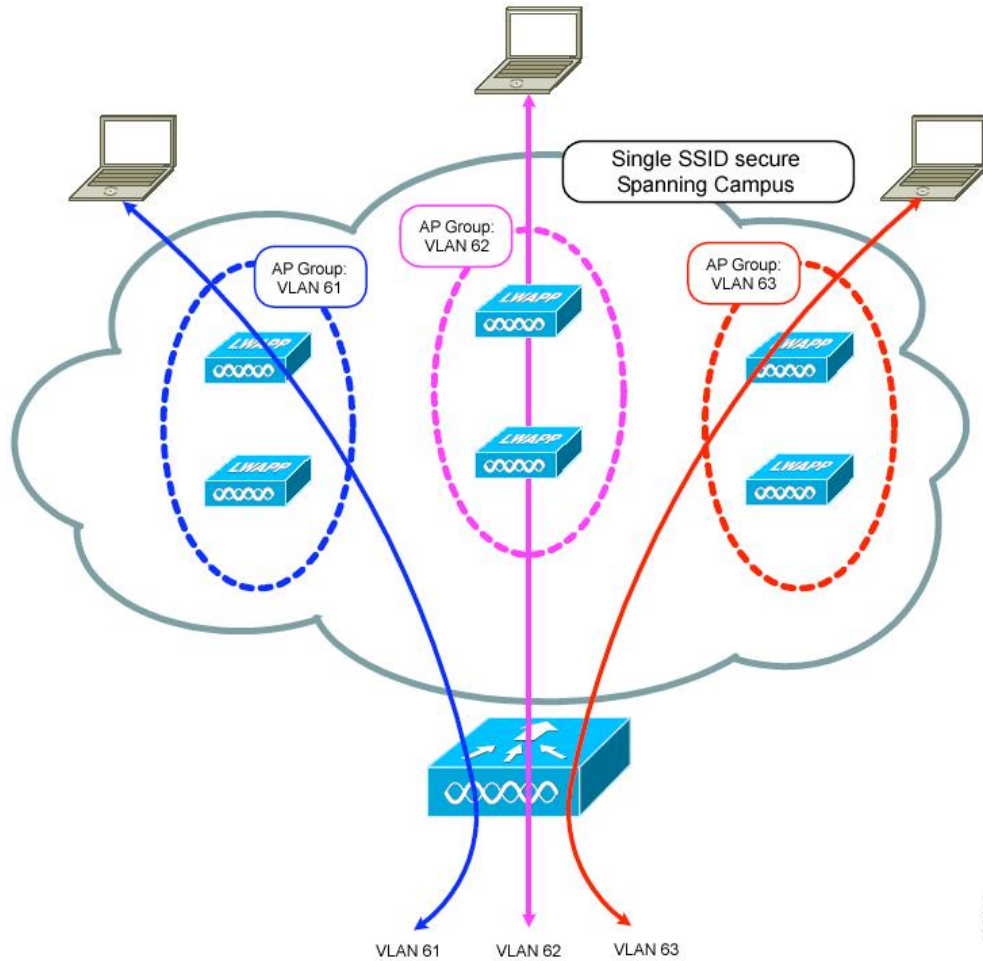
図では、3 つの設定された動的インターフェイスが、3 つの異なる VLAN（VLAN 61、VLAN 62、および VLAN 63）にマップされています。3 つのアクセスポイントグループが定義されており、各グループは異なる VLAN のメンバですが、すべてのグループが同じ SSID のメンバとなっています。ワイヤレス SSID 内のクライアントには、そのアクセスポイントがメンバとなっている VLAN サブネットから IP アドレスが割り当てられています。たとえば、アクセスポイントグループ VLAN 61 のメンバであるアクセスポイントにアソシエートする任意のユーザには、そのサブネットから IP アドレスが割り当てられます。

図では、スイッチは内部的にレイヤ 3 ローミングイベントとしてアクセスポイント間のローミングを扱っています。こうすることで、WLAN クライアントは元の IP アドレスを保持します。

すべてのアクセスポイントがスイッチに join された後は、アクセスポイントグループを作成して、最大 16 の WLAN を各グループに割り当てることができます。各アクセスポイントは、有効化されている WLAN のうち、そのアクセスポイントグループに属する WLAN だけをアドバタイ

ズします。アクセス ポイントグループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

図 48: アクセス ポイント グ



アクセス ポイントグループの設定

ステップ1 適切な動的インターフェイスを設定し、必要な VLAN にマップします。

たとえば、「アクセスポイントグループについて」セクションで説明するネットワークを設定するには、コントローラに VLAN 61、62、および 63 の動的インターフェイスを作成します。動的インターフェイスを設定する方法の詳細については、「動的インターフェイスの設定」の項を参照してください。

- ステップ 2 アクセスポイントグループを作成します。「アクセスポイントグループの作成」の項を参照してください。
- ステップ 3 RF プロファイルを作成します。「RF プロファイルの作成」の項を参照してください。
- ステップ 4 適切なアクセスポイントグループにアクセスポイントを割り当てます。「アクセスポイントグループの作成」の項を参照してください。
- ステップ 5 AP グループの RF プロファイルを適用します。「AP グループへの RF プロファイルの適用」の項を参照してください。

アクセスポイントグループの作成 (GUI)

- ステップ 1 [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
このページには、コントローラで現在作成されているすべてのアクセスポイントグループが表示されます。デフォルトでは、アクセスポイントは、他のアクセスポイントグループに割り当てられない限り、すべて、デフォルトのアクセスポイントグループ「default-group」に属します。

(注) コントローラによってデフォルトのアクセスポイントグループが作成され、その中に、最初の 16 の WLAN (1 ~ 16 の ID を持つ WLAN、設定された WLAN の数が 16 に満たない場合は、さらに少なくなる) が自動的に入力されます。このデフォルトのグループは変更できません (このグループに WLAN を追加したり、このグループから WLAN を削除することはできません)。先頭の 16 の WLAN が追加または削除されるたびに、グループの内容は動的に更新されます。アクセスポイントは、アクセスポイントグループに属していない場合には、デフォルトグループに割り当てられ、そのデフォルトグループ内の WLAN を使用します。アクセスポイントは、未定義のアクセスポイントグループ名を有するコントローラと join した場合、そのグループ名を保持しますが、default-group アクセスポイントグループ内の WLAN を使用します。
- ステップ 2 [Add Group] をクリックして、新しいアクセスポイントグループを作成します。[Add New AP Group] のセクションがページ上部に表示されます。
- ステップ 3 [AP Group Name] テキストボックスに、グループの名前を入力します。
- ステップ 4 [Description] テキストボックスに、グループの説明を入力します。
- ステップ 5 [NAS-ID] テキストボックスに、AP グループのネットワークアクセスサーバの ID を入力します。
- ステップ 6 [Add] をクリックします。新たに作成したアクセスポイントグループが、[AP Groups] ページのアクセスポイントグループのリストに表示されます。

(注) このグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて、[Remove]を選択します。1つ以上のアクセスポイントで使用しているアクセスポイントグループを削除しようとする、エラーメッセージが表示されます。コントローラソフトウェアリリース 6.0以降では、アクセスポイントグループを削除する前に、そのグループ内のすべてのアクセスポイント別のグループに移動させます。以前のリリースのように、アクセスポイントが default-group アクセスポイントグループに移動されることはありません。

- ステップ 7** グループの名前をクリックして、この新しいグループを編集します。[AP Groups > Edit] ([General]) ページが表示されます。
- ステップ 8** このアクセスポイントグループの説明を変更するには、[AP Group Description] テキストボックスに新しいテキストを入力して、[Apply] をクリックします。
- ステップ 9** [WLANs] タブを選択して、[AP Groups > Edit] ([WLANs]) ページを開きます。このページでは、このアクセスポイントグループに現在割り当てられている WLAN が表示されます。
- ステップ 10** [Add New] をクリックして、このアクセスポイントグループに WLAN を割り当てます。[Add New] のセクションがページ上部に表示されます。
- ステップ 11** [WLAN SSID] ドロップダウンリストから、この WLAN の SSID を選択します。
- ステップ 12** [Interface Name] ドロップダウンリストから、アクセスポイントグループをマップするインターフェイスを選択します。Network Admission Control (NAC; ネットワークアドミッションコントロール) のアウトオブバンドのサポートを有効にする場合は、隔離 VLAN を選択します。
- (注) default-group アクセスポイントグループ内のインターフェイス名は、WLAN インターフェイスと一致します。
- ステップ 13** [NAC State] チェックボックスをオンして、このアクセスポイントグループに対する NAC アウトオブバンドのサポートを有効にします。NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ (デフォルト値) のままとします。
- ステップ 14** [Add] をクリックして、この WLAN をアクセスポイントグループに追加します。この WLAN が、このアクセスポイントグループに割り当てられている WLAN のリストに表示されます。
- (注) この WLAN をアクセスポイントグループから削除する場合は、カーソルをこの WLAN の青のドロップダウン矢印の上に置いて、[Remove] を選択します。
- ステップ 15** ステップ 9 ~ ステップ 13 を繰り返して、このアクセスポイントグループに WLAN をさらに追加します。
- ステップ 16** [APs] タブを選択して、このアクセスポイントグループにアクセスポイントを割り当てます。[AP Groups > Edit] ([APs]) ページには、このグループに現在割り当てられているアクセスポイントと、グループへの追加が可能なアクセスポイントが一覧されます。アクセスポイントがグループに現在割り当てられていない場合、そのアクセスポイントのグループ名は「default-group」として表示されます。
- ステップ 17** アクセスポイント名の左側にあるチェックボックスをオンにして [Add APs] をクリックし、このアクセスポイントグループにアクセスポイントを追加します。すると、該当するアクセスポイントが、このアクセスポイントグループに現在属しているアクセスポイントのリストに表示されます。
- (注) 使用可能なアクセスポイントを一度にすべて選択するには、[AP Name] チェックボックスをオンにします。これで、すべてのアクセスポイントが選択されます。
- (注) グループからアクセスポイントを削除する場合は、アクセスポイント名の左側のチェックボックスをオンにし、[Remove APs] をクリックします。一度にすべてのアクセスポイントを選択するには、[AP Name] チェックボックスをオンにします。これで、このグループからすべてのアクセスポイントが削除されます。

(注) アクセスポイントが属するアクセスポイントグループを変更する場合は、[Wireless] > [Access Points] > [All APs] > [ap_name] > [Advanced] タブを選択し、[AP Group Name] ドロップダウンリストから別のアクセスポイントグループの名前を選択し、[Apply] をクリックします。

ステップ 18 [802.11u] タブでは、次のことを実行できます。

- a) 類似のホットスポットの場所をグループ化するホットスポットグループを選択します。
- b) 選択するホットスポットの場所グループに基づく場所タイプを選択します。
- c) 新しい場所を追加するには、[Add New Venue] をクリックし、その場所で使用される言語名と、基本サービスセット (BSS) と関連付けられる場所の名前を入力します。この名前は、場所に関する十分な情報を SSID が提供していない場合に使用します。
- d) AP グループの動作クラスを選択します。
- e) [Apply] をクリックします。

ステップ 19 [Save Configuration] をクリックします。

アクセスポイントグループの作成 (CLI)

ステップ 1 アクセスポイントグループを作成するには、次のコマンドを入力します。

```
config wlan apgroup add group_name
```

(注) アクセスポイントグループを削除するには、**config wlan apgroup delete group_name** コマンドを入力します。1つ以上のアクセスポイントで使用しているアクセスポイントグループを削除しようとする、エラーメッセージが表示されます。コントローラソフトウェアリリース 6.0以降では、アクセスポイントグループを削除する前に、そのグループ内のすべてのアクセスポイントを別のグループに移動させます。以前のリリースのように、アクセスポイントが default-group アクセスポイントグループに移動されることはありません。グループ内のアクセスポイントを表示するには、**show wlan apgroups** コマンドを入力します。アクセスポイントを別のグループに移動させるには、**config ap group-name group_name Cisco_AP** コマンドを入力します。

ステップ 2 アクセスポイントグループに説明を追加するには、次のコマンドを入力します。

```
config wlan apgroup description group_name description
```

ステップ 3 アクセスポイントグループに WLAN を割り当てるには、次のコマンドを入力します。

```
config wlan apgroup interface-mapping add group_name wlan_id interface_name
```

(注) アクセスポイントグループから WLAN を削除するには、**config wlan apgroup interface-mapping delete group_name wlan_id** コマンドを入力します。

ステップ 4 このアクセスポイントグループに対して、NAC アウトオブバンドのサポートを有効または無効にするには、次のコマンドを入力します。

```
config wlan apgroup nac {enable | disable} group_name wlan_id
```

ステップ 5 次のコマンドを入力して、アクセスポイントグループで WLAN 無線ポリシーを設定します。

```
config wlan apgroup wlan-radio-policy apgroup_name wlan_id {802.11a-only | 802.11bg | 802.11g-only | all}
```

ステップ 6 アクセスポイントをアクセスポイントグループに割り当てるには、次のコマンドを入力します。

```
config ap group-name group_name Cisco_AP
```

(注) アクセスポイントグループからアクセスポイントを削除するには、このコマンドを再度入力して、そのアクセスポイントを別のグループに割り当てます。

ステップ 7 APグループのホットスポットを設定するには、次のコマンドを入力します。

```
config wlan apgroup hotspot {venue | operating-class}
```

ステップ 8 次のコマンドを入力して、変更を保存します。

```
save config
```

アクセスポイントグループの表示 (CLI)

アクセスポイントグループについて情報を表示する、またはトラブルシューティングするには、次のコマンドを使用します。

- コントローラのすべてのアクセスポイントグループのリストを表示するには、次のコマンドを入力します。

```
show wlan apgroups
```

- アクセスポイントグループに割り当てられている各 WLAN の BSSID を表示するには、次のコマンドを入力します。

```
show ap wlan {802.11a | 802.11b} Cisco_AP
```

- アクセスポイントグループに対して有効になっている WLAN の数を表示するには、次のコマンドを入力します。

```
show ap config {802.11a | 802.11b} Cisco_AP
```

- アクセスポイントグループのデバッグを有効または無効にするには、次のコマンドを入力します。

```
debug group {enable | disable}
```



第 97 章

RF プロファイルの設定

- [RF プロファイルを設定するための前提条件](#), 767 ページ
- [RF プロファイルの設定に関する制約事項](#), 767 ページ
- [RF プロファイルについて](#), 768 ページ
- [RF プロファイルの設定 \(GUI\)](#), 771 ページ
- [RF プロファイルの設定 \(CLI\)](#), 773 ページ
- [AP グループへの RF プロファイルの適用 \(GUI\)](#), 776 ページ
- [AP グループへの RF プロファイルの適用 \(CLI\)](#), 776 ページ

RF プロファイルを設定するための前提条件

いったん AP グループを作成して RF プロファイルを適用するか、既存の AP グループを変更すると、新しい設定が有効になり、次のルールが有効になります。

- AP グループのすべてのコントローラに、同一の RF プロファイルが適用され、存在する必要があります。そうしないと、コントローラに対するアクションが失敗します。
- 同一の RF プロファイルを複数の AP グループに割り当てることができます。

RF プロファイルの設定に関する制約事項

- いったん AP グループを作成して RF プロファイルを適用するか、既存の AP グループを変更すると、新しい設定が有効になり、次のルールが有効になります。
 - AP 電力にカスタム電力設定が適用されている AP は、グローバルモード設定ではなく、この AP に対して RF プロファイルの効果はありません。RF プロファイリングを作用させるには、すべての AP のチャンネルと電力が RRM によって管理されている必要があります。

- AP グループ内で、いずれかの帯域での RF プロファイルの割り当てを変更すると、AP がリブートします。
 - RF プロファイルを AP グループに割り当てた後は、その RF プロファイルを変更することはできません。RF プロファイルを変更してから、AP グループに再び追加するには、AP グループの RF プロファイルの設定を [none] に変更する必要があります。また、802.11a と 802.11b のいずれの場合も、変更した場合に影響を受けるネットワークを無効にすることによって、この制限を回避できます。
 - AP が割り当てられている AP グループは削除できません。
 - AP グループに適用されている RF プロファイルは削除できません。
- [Out of Box] を有効にする場合、設定を保存して Cisco WLC をリブートすると、[Out of Box] のステータスが無効に変更されます。この動作は、Cisco WiSM2、Cisco 5500 シリーズ WLC、および Cisco 2500 シリーズ WLC で監視されます。回避策は、Cisco WLC の再起動後に [Out of Box] を再度有効にすることです。

RF プロファイルについて

RF プロファイルを使用すると、共通のカバレッジゾーンを共有する AP グループを調整し、そのカバレッジゾーン内の AP に対する RRM の動作を選択的に変更できます。

たとえば、多くのユーザが集まる、または会合するエリアに、大学が高密度の AP を展開する場合があります。この場合は、同一チャネル干渉を管理しながら、セル密度に対処するために、データレートと電力の両方を操作する必要があります。隣接エリアでは、通常のカバレッジが提供されますが、そのような操作によってカバレッジが失われます。

RF プロファイルと AP グループを使用すると、異なる環境やカバレッジゾーンで動作する AP グループに対する RF 設定を最適化できます。RF プロファイルは、802.11 無線用に作成されます。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。

RF プロファイルを使用して、データレートおよび電力 (TPC) 値を制御できます。



- (注) RF プロファイルの適用によって、RRM 内の AP のステータスが変わることはありません。ステータスは、RRM によって制御されるグローバル コンフィギュレーション モードのままです。

高密度で複雑な RF トポロジに対処するには、次の設定を使用できます。

- 高密度設定：密集ワイヤレス ネットワークの RF 環境を最適化するために、次の設定を使用できます。
- WLAN または無線ごとのクライアントの制限：高密度環境の AP と通信できるクライアントの最大数。

- クライアント トラップしきい値：アクセス ポイントにアソシエートされるクライアント数のしきい値。この値以降、SNMP トラップがコントローラと Cisco Prime Infrastructure に送信されます。
- スタジアム ビジョン設定：次のパラメータを設定できます。
 - マルチキャスト データ レート：AP の RF 条件に基づく、設定可能なマルチキャストトラフィックのデータ レート。
- アウトオブボックス AP 設定：デフォルト AP グループに属する新しく設置したアクセス ポイントで構成されるアウトオブボックス AP グループの作成。この機能を有効にすると、次のように動作します。
 - デフォルト AP グループの一部である、新しくインストールしたアクセス ポイントは、アウトオブボックス AP グループに属し、その無線はスイッチ オフされます。これによって、新しいアクセス ポイント原因となって RF 不安定が発生するおそれはありません。
 - グループ名を持たないすべてのアクセス ポイントは、アウトオブボックス AP グループの一部になります。
 - 特別な RF プロファイルは 802.11 帯域ごとに作成されます。これらの RF プロファイルには、既存のすべての RF パラメータのデフォルト設定、および追加の新しい設定があります。



(注) この機能を有効にした後に無効にすると、アウトオブザボックス AP グループへの新しい AP のサブスクリプションだけが停止します。アウトオブザボックス AP グループへサブスクリプションされたすべての AP が、この AP グループに残ります。ネットワーク管理者は、ネットワークのコンバージェンスの際に、このような AP をデフォルト グループまたはカスタム AP グループに移動できます。

- 帯域選択設定：帯域選択を利用することで、2.4 GHz と 5 GHz の帯域間でのクライアントの分散に対応できます。まずクライアントの機能を把握し、クライアントが 2.4 GHz および 5 GHz の両方の周波数帯にアソシエートすることができるかどうかを確認します。WLAN で帯域選択を有効にすると、2.4 GHz 帯域のプローブを AP に抑制させ、最終的にデュアルバンドクライアントを 5 GHz 帯域に移動することができます。次の帯域選択パラメータを AP グループごとに設定できます。
 - プローブ応答：クライアントへのプローブ応答。有効または無効にできます。
 - プローブサイクル回数：RF プロファイルのプローブサイクル回数。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。
 - サイクルしきい値：RF プロファイル帯域選択を新しくスキャンするサイクル期間の時間しきい値。この設定は、クライアントからの新しいプローブ要求が新しいスキャンサイクルで送信される間の時間しきい値を決定します。

- 失効抑制期間：以前に認識されていた 802.11b/g クライアントをプルーニングするための期限切れ時間。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
- デュアルバンドの失効：以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。
- クライアント RSSI：クライアントがプローブに応答するための最小 RSSI。
- ロードバランシングの設定：ロードバランシングは、AP にわたるクライアントの適正な分散を維持します。次のパラメータを設定できます。
 - ウィンドウ：ロードバランシングは、クライアントのウィンドウ サイズを適用することによって、クライアントアソシエーションの制限を設定します。たとえば、ウィンドウサイズが3として定義されている場合、フロア領域にわたって適正なクライアントの分散を想定し、グループ平均と比較して、AP には3つ以上のアソシエートされたクライアントがあってはなりません。
 - 拒否：拒否数は、ロードバランシング中のアソシエーション拒否の最大数を設定します。
- カバレッジ ホールの軽減設定：次のパラメータを設定できます。
 - データ RSSI：アクセスポイントで受信されたデータパケットの最小の受信信号強度インジケータ (RSSI) 値。入力する値は、ネットワーク内のカバレッジホール（またはカバレッジが不完全な領域）を特定するのに使用されます。
 - Voice RSSI：アクセスポイントで受信された音声パケットの最小の受信信号強度インジケータ (RSSI) 値。
 - カバレッジ例外：カバレッジホール例外をトリガーする、データまたは音声 RSSI しきい値以下の RSSI 値を持つアクセスポイント上のクライアントの最小数。
 - カバレッジレベル：アクセスポイント上で、信号レベルが低くなっているにもかかわらず、別のアクセスポイントにローミングできないクライアントの割合。アクセスポイントに設定されたカバレッジレベルよりも多くこのようなクライアントが存在する場合、カバレッジホールイベントがトリガーされます。
- DCA：次の DCA パラメータを設定できます。
 - Avoid foreign AP interference：DCA アルゴリズムは、外部 802.11 トラフィックのアクセスポイントから検出されたトラフィックや干渉など、複数の入力での最適化に基づいています。各アクセスポイントでは定期的に干渉、ノイズレベル、外部干渉および負荷を測定し、ネイバー AP のリストを管理します。つまり外部 AP 干渉は、802.11 のネイバー以外（同じ RF ドメインに含まれていない 802.11 AP、たとえば外部 802.11 ネットワーク）から受信されます。この干渉は、ノイズレベルと同じメカニズムを使用して測定されます。

現在導入されている無線リソース管理モジュールでは対応できないため、このような AP は RRM に悪影響を与える可能性があります。したがって、ユーザは RF プロファイルの DCA の使用を選択せずにこの機能を無効にすることができます。

° Channel width : 次のチャンネル幅のオプションのいずれかを選択して、5 GHz 帯域のすべての 802.11n および 802.11ac 無線でサポートするチャンネル帯域幅を指定できます。

° [20 MHz] : 20 MHz のチャンネル帯域幅 (デフォルト)



(注) 2.4GHz 帯域で使用できる最大帯域幅は 20MHz です。

° [40 MHz] : 40 MHz のチャンネル帯域幅

° [80 MHz] : 80 MHz のチャンネル帯域幅

° DCA channel list : DCA がアクセスポイント無線にチャンネルを割り当てるために使用するチャンネルのリストを選択できます。使用可能なチャンネルはグローバルに設定されている国に基づいて事前に選択されています。DCA は、これらのチャンネル上で測定されるメトリックを比較して、最適なチャンネルを選択します。帯域幅が 20 MHz を超える場合、チャンネルボンディングは連続するチャンネルで実行されます。たとえば、帯域幅が 40 MHz の場合、チャンネルに適したペアが選択されます。40 MHz の帯域幅の場合、選択されるペアは 36 および 40 MHz です。80MHz などの広帯域幅では、適切な帯域幅として、36、40、44、および 48 MHz の四つ組が選択されます。

° Trap thresholds : トラップのプロファイルしきい値は、RF プロファイルに基づいて特定の AP グループに対して設定できます。

RF プロファイルの設定 (GUI)

- ステップ 1 [Wireless] > [RF Profiles] の順に選択して [RF Profiles] ページを開きます。
- ステップ 2 すべての RF プロファイルのアウトオブボックス ステータスを設定するには、[Enable Out Of Box] チェックボックスをオンまたはオフにします。
- ステップ 3 [New] をクリックします。
- ステップ 4 [RF Profile Name] を入力し、無線帯域を選択します。
- ステップ 5 [Apply] をクリックして、電力およびデータ レート パラメータのカスタマイズを設定します。
- ステップ 6 [General] タブで、[Description] テキスト ボックスに RF プロファイルの説明を入力します。
- ステップ 7 [802.11] タブで、このプロファイルの AP に適用するデータ レートを設定します。
- ステップ 8 [RRM] タブでは、次のことを実行できます。
 - a) [TPC] 領域で、[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定します。これは、この RF プロファイル内の AP が使用できる最大電力と最小電力です。

- b) [TPC] 領域で、TPC のバージョン 1 またはバージョン 2 に対するカスタム TPC 電力しきい値を設定します。
- (注) TPC の 1 種類のバージョンだけが、特定のコントローラバージョン 1 の RRM に使用でき、バージョン 2 は同じ RF プロファイル内で相互運用性はありません。TPCv2 に対してしきい値を選択した場合に、その値が RF プロファイルに選択した TPC アルゴリズムにないと、その値は無視されます。
- c) [Coverage Hole Detection] 領域で、音声およびデータ RSSI を設定します。
- d) [Coverage Exception] テキスト ボックスに、クライアントの数を入力します。
- e) [the Coverage Level] テキスト ボックスに、割合を入力します。
- f) [Traps] 領域の [Profile threshold] に、干渉の割合、クライアント数、ノイズ レベルおよび使用率を入力します。
- g) [DCA] 領域で [Avoid Foreign AP interference Enabled] チェックボックスを選択して、外部 AP の干渉を回避します。
- h) [DCA] 領域で次のチャンネル幅オプションのいずれかを選択して、5 GHz 帯域のすべての 802.11n および 802.11 ac 無線でサポートするチャンネル帯域幅を指定します。
- [20 MHz] : 20 MHz のチャンネル帯域幅 (デフォルト)
 - [40 MHz] : 40 MHz のチャンネル帯域幅
 - [80 MHz] : 80 MHz のチャンネル帯域幅
- i) [DCA] 領域の [DCA Channels] テキスト ボックスには、現在選択されているチャンネルが表示されます。チャンネルを選択するには、[Select] カラムでそのチャンネルのチェックボックスをオンにします。チャンネルの選択を解除するには、チャンネルのチェックボックスをオフにします。リストされているチャンネル番号はその特定の RF プロファイルにだけ適用されます。範囲は次のとおりです。
- 802.11a : 36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165、190、196
 - 802.11b/g : 1、2、3、4、5、6、7、8、9、10、11
- デフォルトの設定は次のとおりです。
- 802.11a : 36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161
 - 802.11b/g : 1、6、11
- (注) 以前のリリースからアップグレードしている場合は、これらのチャンネルが DCA チャンネル リストに含まれていることを確認します。チャンネルリストにこれらのチャンネルを含めるには、[Extended UNII-2 Channels Enabled] チェックボックスをオンにします。

ステップ 9 [High Density] タブでは、次のことを実行できます。

- a) [High Density Parameters] 領域で、AP 無線ごとに許可されるクライアントの最大数、およびクライアント トラップしきい値を入力します。

- b) [Multicast Parameters] 領域で、[Multicast Data Rates] ドロップダウン リストからデータ レートを選択します。

ステップ 10 [Client Distribution] タブでは、次のことを実行できます。

- a) [Load Balancing] 領域で、クライアントのウィンドウ サイズおよび拒否数を入力します。
このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。
- ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシング しきい値
- 特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアント ウィンドウ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこのしきい値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数がしきい値を下回るアクセス ポイントだけとなります。
- 拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。
- b) [Band Select] 領域で、[Probe Response] チェックボックスをオンまたはオフにします。
(注) 帯域選択設定は、802.11b/g RF プロファイルだけに使用できません。
- c) [Cycle Count] テキスト ボックスに、新しいクライアントの抑制サイクルの回数を入力します。デフォルトの数は 2 です。
- d) [Cycle Threshold] テキスト ボックスに、クライアントから新しいプローブ要求が送信される、新しいスキャンサイクルからの時間しきい値を決定する時間をミリ秒単位で入力します。デフォルトのサイクル閾値は 200 ミリ秒です。
- e) [Suppression Expire] テキスト ボックスに、期限切れになると 802.11 b/g クライアントが新規となり、プローブ応答抑制の対象となる期限を入力します。
- f) [Dual Band Expire] テキスト ボックスに、期限切れになるとデュアルバンド クライアントが新規となり、プローブ応答抑制の対象となる期限を入力します。
- g) [Client RSSI] テキスト ボックスに、クライアントがプローブに応答するための最小 RSSI を入力します。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

RF プロファイルの設定 (CLI)

- ステップ 1** すべての RF プロファイルのアウトオブボックス ステータスを設定するには、次のコマンドを入力します。

config rf-profile out-of-box {enable | disable}

ステップ 2 RF プロファイルを作成または削除するには、次のコマンドを入力します。

config rf-profile {create {802.11a | 802.11b} | delete} profile-name

ステップ 3 RF プロファイルの説明を指定するには、次のコマンドを入力します。

config rf-profile description text profile-name

ステップ 4 このプロファイルの AP にデータ レートが適用されるように設定するには、次のコマンドを入力します。

config rf-profile data-rates {802.11a | 802.11b} {disabled | mandatory | supported} rate profile-name

ステップ 5 最大電力レベル割り当ておよび最小電力レベル割り当て（この RF プロファイル内の AP が使用できる最大電力と最小電力）を設定するには、次のコマンドを入力します。

config rf-profile {tx-power-max | tx-power-min} power-value profile-name

ステップ 6 TPC のバージョン 1 またはバージョン 2 に対するカスタム TPC 電力しきい値を設定するには、次のコマンドを入力します。

config rf-profile {tx-power-control-thresh-v1 | tx-power-control-thresh-v2} power-threshold profile-name

ステップ 7 カバレッジ ホール検出パラメータを設定する

a) カバレッジ データを設定するには、次のコマンドを入力します。

config rf-profile coverage data value-in-dBm profile-name

b) 最小クライアント カバレッジ例外レベルを設定するには、次のコマンドを入力します。

config rf-profile coverage exception clients profile-name

c) カバレッジ例外レベルの割合を設定するには、次のコマンドを入力します。

config rf-profile coverage level percentage-value profile-name

d) 音声のカバレッジを設定するには、次のコマンドを入力します。

config rf-profile coverage voice value-in-dBm profile-name

ステップ 8 AP 無線ごとに許可されるクライアントの最大数を設定するには、次のコマンドを入力します。

config rf-profile max-clients num-of-clients profile-name

ステップ 9 クライアント トラップしきい値を設定するには、次のコマンドを入力します。

config rf-profile client-trap-threshold threshold-value profile-name

ステップ 10 マルチキャストを設定するには、次のコマンドを入力します。

config rf-profile multicast data-rate rate profile-name

ステップ 11 ロード バランシングを設定するには、次のコマンドを入力します。

config rf-profile load-balancing {window num-of-clients | denial value} profile-name

ステップ 12 帯域選択を設定する

a) 帯域選択サイクル数を設定するには、次のコマンドを入力します。

config rf-profile band-select cycle-count max-num-of-cycles profile-name

b) サイクルしきい値を設定するには、次のコマンドを入力します。

config rf-profile band-select cycle-threshold time-in-milliseconds profile-name

c) 帯域選択の有効期限を設定するには、次のコマンドを入力します。

config rf-profile band-select expire {dual-band | suppression} time-in-seconds profile-name

- d) プローブ応答を設定するには、次のコマンドを入力します。

config rf-profile band-select probe-response {enable | disable} profile-name

- e) プローブに反応する条件となる、クライアントのRSSIの最小値を設定するには、次のコマンドを入力します。

config rf-profile band-select client-rssi value-in-dBm profile-name

- ステップ 13** アクセス ポイント グループ ベースに対して 802.11n のみのモードを設定するには、次のコマンドを入力します。

config rf-profile 11n-client-only {enable | disable} rf-profile-name

802.11n のみのモードでは、アクセス ポイント ブロードキャストによって 802.11n の速度がサポートされます。802.11n クライアントのみを、アクセス ポイントと関連付けることができます

- ステップ 14** RF プロファイルの DCA パラメータを設定する方法

- a) 外部 AP 干渉を設定するには、次のコマンドを入力します。

config rf-profile channel foreign { enable | disable }

- b) チャネル幅を設定するには、次のコマンドを入力します。

config rf-profile channel chan-width { 20 | 40 | 80 }

- c) DCA チャネル リストを設定するには、次のコマンドを入力します。

config rf-profile channel { add | delete } chan profile_name

- d) トラップしきい値を設定するには、次のコマンドを入力します。

config rf-profile trap-threshold { clients | interference | noise | utilization }

- Clients : トラップ用のアクセス ポイントの無線のクライアント数は 1 ~ 200 です。デフォルトは 12 クライアントです。
- Interference : トラップ用の干渉しきい値の割合は 0 ~ 100% です。デフォルトは 10% です。
- Noise : トラップ用のノイズしきい値のレベルは -127 ~ 0 dBm です。デフォルトは -17 dBm です。
- Utilization : アクセス ポイントしきい値で使用されるトラップ用の帯域幅の割合は 0 ~ 100% です。デフォルトは 80% です。

AP グループへの RF プロファイルの適用 (GUI)

-
- ステップ 1** [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
- ステップ 2** [AP Group Name] をクリックして、[AP Groups > Edit] ページを開きます。
- ステップ 3** [RF Profile] タブをクリックし、RF プロファイルの詳細を設定します。各帯域 (802.11a/802.11b) の RF プロファイルを選択することも、このグループに適用する 1 つのプロファイルまたは [none] を選択することもできます。
- (注) AP を選択して新しいグループに追加するまで、設定は適用されません。新しい設定はそのまま保存できますが、プロファイルは適用されません。AP グループに移動する AP を選択した後で、それらの AP を新しいグループに移動すると AP がリブートし、RF プロファイルの設定がその AP グループの AP に適用されます。
- ステップ 4** [APs] タブをクリックし、AP グループに追加する AP を選択します。
- ステップ 5** [Add APs] をクリックし、選択した AP を AP グループに追加します。AP グループがリブートし、AP がコントローラに再 join することを示す、警告メッセージが表示されます。
- (注) AP は、一度に 2 つの AP グループに属することはできません。
- ステップ 6** [Apply] をクリックします。AP が、AP グループに追加されます。
-

AP グループへの RF プロファイルの適用 (CLI)

次の作業

次のコマンドを使用して、AP グループに RF プロファイルを適用します。

- `config wlan apgroup profile-mapping {add | delete} ap-group-name rf-profile-name`



第 98 章

802.1X 認証を使用した Web リダイレクトの設定

- [802.1X 認証を使用した Web リダイレクトについて, 777 ページ](#)
- [RADIUS サーバの設定 \(GUI\) , 779 ページ](#)
- [Web リダイレクトの設定, 780 ページ](#)
- [WLAN ごとのアカウントिंग サーバの無効化 \(GUI\) , 781 ページ](#)
- [WLAN ごとのカバレッジ ホールの検出の無効化, 781 ページ](#)

802.1X 認証を使用した Web リダイレクトについて

802.1X 認証が正常に完了した後に、ユーザを特定の Web ページにリダイレクトするように WLAN を設定できます。Web リダイレクトを設定して、ユーザにネットワークへの部分的または全面的なアクセス権を与えることができます。

条件付き Web リダイレクト

条件付き Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは条件付きで特定の Web ページにリダイレクトされます。RADIUS サーバ上で、リダイレクト先のページとリダイレクトが発生する条件を指定できます。条件には、ユーザのパスワードの有効期限が近づいている場合、または使用を継続するためにユーザが料金を支払う必要がある場合などがあります。

RADIUS サーバが Cisco AV ペア「url-redirect」を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。さらにサーバから Cisco AV ペア「url-redirect-acl」も返された場合は、指定されたアクセスコントロールリスト (ACL) が、そのクライアントの事前認証 ACL としてインストールされます。クライアントはこの時点で完全に認証されていないと見なされ、事前認証 ACL によって許可されるトラフィックのみを送信できます。

指定された URL（たとえば、パスワードの変更、請求書の支払い）でクライアントが特定の操作を完了すると、クライアントの再認証が必要になります。RADIUS サーバから「url-redirect」が返されない場合、クライアントは完全に認証されたものと見なされ、トラフィックを渡すことを許可されます。



- (注) 条件付き Web リダイレクト機能は、802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上で条件付き Web リダイレクトを設定できます。

スプラッシュ ページ Web リダイレクト

スプラッシュ ページ Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは特定の Web ページにリダイレクトされます。ユーザは、リダイレクト後、ネットワークに完全にアクセスできます。RADIUS サーバでリダイレクト ページを指定できます。RADIUS サーバが Cisco AV ペア「url-redirect」を返す場合、ユーザがブラウザを開くと指定された URL へリダイレクトされます。クライアントは、この段階で完全に認証され、RADIUS サーバが「url-redirect」を返さなくても、トラフィックを渡すことができます。



- (注) スプラッシュ ページ Web リダイレクト機能は、802.1x キー管理を使用する 802.1X または WPA+WPA2 レイヤ 2 セキュリティに対して設定されている WLAN でのみ利用できます。事前共有キー管理は、レイヤ 2 セキュリティ方式ではサポートされません。

無線クライアントで実行するバックエンドアプリケーションがあり、通信に HTTP または HTTPS ポートを使用したとします。実際の Web ページが開く前にアプリケーションが通信を開始すると、リダイレクト機能が Web パススルーで機能しません。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上でスプラッシュ ページ Web リダイレクトを設定できます。

RADIUS サーバの設定 (GUI)



(注) 次の手順は、CiscoSecure ACS 固有の手順ですが、その他の RADIUS サーバでも同様の手順を使用します。

-
- ステップ 1** CiscoSecure ACS メインメニューから、[Group Setup] を選択します。
- ステップ 2** [Edit Settings] をクリックします。
- ステップ 3** [Jump To] ドロップダウンリストから [RADIUS (Cisco IOS/PIX 6.0)] を選択します。
- ステップ 4** [[009\001] cisco-av-pair] チェックボックスをオンにします。
- ステップ 5** [[009\001] cisco-av-pair] 編集ボックスに次の Cisco AV ペアを入力して、ユーザをリダイレクトする URL を指定するか、条件付き Web リダイレクトを設定する場合は、ダイレクトが発生する条件をそれぞれ指定します。
- ```
url-redirect=http://url
url-redirect-acl=acl_name
```
-

## Web リダイレクトの設定

### Web リダイレクトの設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
  - ステップ 2 必要な WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。
  - ステップ 3 [Security] タブおよび [Layer 2] タブを選択して、[WLANs > Edit] ([Security] > [Layer 2]) ページを開きます。
  - ステップ 4 [Layer 2 Security] ドロップダウン リストから、[802.1X] または [WPA+WPA2] を選択します。
  - ステップ 5 802.1X または WPA+WPA2 に対して任意の追加パラメータを設定します。
  - ステップ 6 [Layer 3] タブを選択して、[WLANs > Edit] ([Security] > Layer 3) ページを開きます。
  - ステップ 7 [Layer 3 Security] ドロップダウン リストから、[None] を選択します。
  - ステップ 8 [Web Policy] チェックボックスをオンにします。
  - ステップ 9 条件付き Web リダイレクトまたはスプラッシュ ページ Web リダイレクトを有効化するオプションとして、[Conditional Web Redirect] または [Splash Page Web Redirect] のいずれかを選択します。 デフォルトでは、両方のパラメータが無効になっています。
  - ステップ 10 ユーザをコントローラ外部のサイトにリダイレクトする場合、[Preauthentication ACL] ドロップダウン リストから RADIUS サーバ上で設定された ACL を選択します。
  - ステップ 11 [Apply] をクリックして、変更を確定します。
  - ステップ 12 [Save Configuration] をクリックして、変更を保存します。
- 

### Web リダイレクトの設定 (CLI)

- 
- ステップ 1 条件付き Web リダイレクトを有効または無効にするには、次のコマンドを入力します。  
**config wlan security cond-web-redir {enable | disable} wlan\_id**
  - ステップ 2 スプラッシュ ページ Web リダイレクトを有効または無効にするには、次のコマンドを入力します。  
**config wlan security splash-page-web-redir {enable | disable} wlan\_id**
  - ステップ 3 次のコマンドを入力して、設定を保存します。  
**save config**
  - ステップ 4 特定の WLAN の Web リダイレクト機能のステータスを表示するには、次のコマンドを入力します。  
**show wlan wlan\_id**

以下に類似した情報が表示されます。

```

WLAN Identifier..... 1
Profile Name..... test
Network Name (SSID)..... test
...
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Enabled
...

```

## WLAN ごとのアカウントング サーバの無効化 (GUI)



(注) アカウントング サーバを無効にすると、すべてのアカウントング動作が無効となり、コントローラが WLAN に対するデフォルトの RADIUS サーバにフォールバックしなくなります。

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 変更する WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。
- ステップ 3 [Security] タブおよび [AAA Servers] タブを選択して、[WLANs > Edit] ([Security > AAA Servers]) ページを開きます。
- ステップ 4 [Accounting Servers] の [Enabled] チェックボックスをオフにします。
- ステップ 5 [Apply] をクリックして、変更を確定します。
- ステップ 6 [Save Configuration] をクリックして、変更を保存します。

## WLAN ごとのカバレッジ ホールの検出の無効化



(注) カバレッジ ホールの検出は、コントローラでグローバルに有効になっています。



- (注) WLAN ごとにカバレッジホールの検出を無効にできます。WLAN でカバレッジホールの検出を無効にした場合、カバレッジホールの警告はコントローラに送信されますが、カバレッジホールを解消するためのそれ以外の処理は行われません。この機能については、ゲストのネットワーク接続時間は短く、モビリティが高いと考えられるようなゲスト WLAN に有効です。

## WLAN 上のカバレッジホールの検出の無効化 (GUI)

- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 変更する WLAN のプロファイル名をクリックします。[WLANs > Edit] ページが表示されます。
- ステップ 3 [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを表示します。
- ステップ 4 [Coverage Hole Detection Enabled] チェックボックスをオフにします。  
(注) OEAP 600 シリーズ アクセス ポイントでは、カバレッジホールの検出はサポートされません。
- ステップ 5 [Apply] をクリックします。
- ステップ 6 [Save Configuration] をクリックします。

## WLAN 上のカバレッジホールの検出の無効化 (CLI)

- ステップ 1 カバレッジホールの検出を無効にするには、次のコマンドを入力します。  
**config wlan chd *wlan-id* disable**  
(注) OEAP 600 シリーズ アクセス ポイントでは、カバレッジホールの検出はサポートされません。
- ステップ 2 次のコマンドを入力して、設定を保存します。  
**save config**
- ステップ 3 特定の WLAN のカバレッジホールの検出ステータスを表示するには、次のコマンドを入力します。  
**show wlan *wlan-id***  
以下に類似した情報が表示されます。

```
WLAN Identifier..... 2
Profile Name..... wlan2
Network Name (SSID)..... 2
. . .
```

CHD per WLAN..... Disabled

---





# 第 99 章

## NAC アウトオブバンド統合の設定

- [NAC アウトオブバンドの前提条件, 785 ページ](#)
- [NAC アウトオブバンドの制限, 786 ページ](#)
- [NAC アウトオブバンド統合について, 787 ページ](#)
- [NAC アウトオブバンド統合の設定 \(GUI\) , 788 ページ](#)
- [NAC アウトオブバンド統合の設定 \(CLI\) , 789 ページ](#)

### NAC アウトオブバンドの前提条件

- NAC アウトオブバンド統合には、CCA のソフトウェア リリース 4.5 以降が必要です。
- NAC アプライアンスでは静的な VLAN マッピングがサポートされているため、コントローラ上で設定されているインターフェイスごとに一意の隔離 VLAN を設定する必要があります。たとえば、コントローラ 1 で 110 という隔離 VLAN を設定し、コントローラ 2 で 120 という隔離 VLAN を設定します。ただし、2つの WLAN またはゲスト LAN が、コントローラのダイナミック インターフェイスとして同一の VLAN を使用している場合、ネットワーク内に導入された NAC アプライアンスが 1 つのときは、同じ隔離 VLAN を使用する必要があります。NAC アプライアンスは、一意の隔離 - アクセス VLAN マッピングをサポートします。
- セッションの失効に基づくポスチャ再評価の場合、NAC アプライアンスと WLAN の両方にセッションタイムアウトを設定し、WLAN でのセッションの失効が NAC アプライアンスでの失効より大きいことを確認します。
- オープン WLAN でセッションタイムアウトが設定されると、Quarantine 状態にあるクライアントのタイムアウトは NAC アプライアンスのタイマーによって判定されます。Web 認証を使用する WLAN においてセッションがタイムアウトすると、クライアントはコントローラから認証解除されるため、ポスチャ検証を再度実行する必要があります。
- レイヤ 2 およびレイヤ 3 認証はすべて、隔離 VLAN で実行されます。外部 Web 認証を使用するには、外部 Web サーバからの HTTP トラフィックおよび外部 Web サーバへの HTTP ト

ラフィックを許可するとともに、隔離 VLAN でのリダイレクト URL を許可するように NAC アプライアンスを設定する必要があります。



(注) 設定の手順については、『Cisco NAC appliance configuration guides』を参照してください：[http://www.cisco.com/en/US/products/ps6128/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html)。

- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。複数の NAC アプライアンスの導入を必要とする場合があります。
- アクセス ポイント グループ VLAN 上で NAC を有効にする場合は、WLAN で NAC をまず有効にする必要があります。アクセス ポイント グループ VLAN では、NAC を有効または無効にすることができます。WLAN で NAC を無効にすることに決めた場合は、アクセス ポイント グループ VLAN でも NAC を必ず無効にします。
- NAC アプライアンスは最大 3,500 のユーザをサポートし、コントローラは最大 5,000 のユーザをサポートします。複数の NAC アプライアンスの導入を必要とする場合があります。
- コントローラの 5.1 以前のソフトウェア リリースでは、コントローラはインバンドモードでのみ NAC アプライアンスと統合します。この場合、NAC アプライアンスはデータパス内になければなりません。インバンドモードでは、各認証場所で（たとえば、各ブランチで、またはコントローラごとに）、NAC アプライアンスが必要であり、すべてのトラフィックが NAC 適用ポイントを通過する必要があります。コントローラのソフトウェア リリース 5.1 以降では、コントローラはアウトオブバンドモードで NAC アプライアンスと統合できます。この場合、NAC アプライアンスは、クライアントが解析およびクリーニングされるまでデータパスに保持されます。アウトオブバンドモードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカルスイッチングを行うように設定されている WLAN での使用はサポートされていません。

## NAC アウトオブバンドの制限

- NAC アウトオブバンド統合は、WLAN AAA Override 機能では使用できません。
- コントローラの 5.1 以前のソフトウェア リリースでは、コントローラはインバンドモードでのみ NAC アプライアンスと統合します。この場合、NAC アプライアンスはデータパス内になければなりません。インバンドモードでは、各認証場所で（たとえば、各ブランチで、またはコントローラごとに）、NAC アプライアンスが必要であり、すべてのトラフィックが



NAC 適用ポイントを通過する必要があります。コントローラのソフトウェア リリース 5.1 以降では、コントローラはアウトオブバンドモードで NAC アプライアンスと統合できます。この場合、NAC アプライアンスは、クライアントが解析およびクリーニングされるまでデータパスに保持されます。アウトオブバンドモードでは NAC アプライアンスのトラフィック負荷が削減されるので、NAC 処理の集中化が可能になります。

- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカルスイッチングを行うように設定されている WLAN での使用はサポートされていません。

## NAC アウトオブバンド統合について

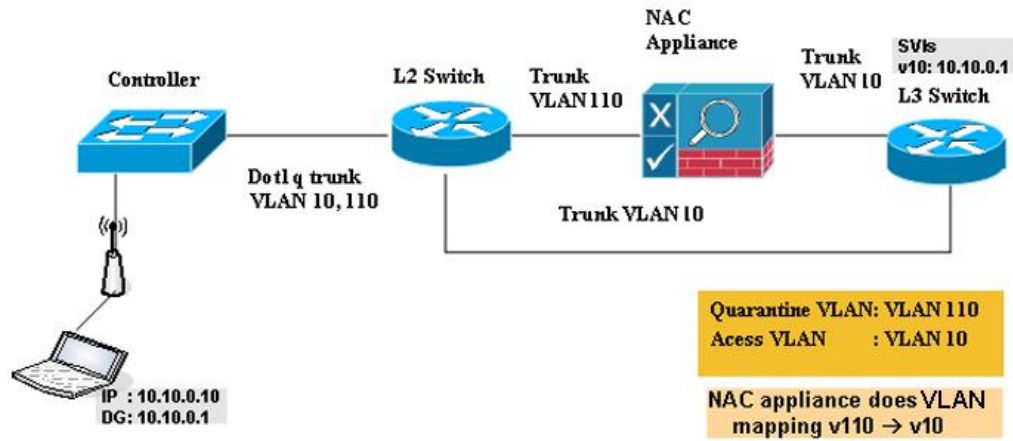
Cisco Clean Access (CCA) とも呼ばれる Cisco NAC アプライアンスはネットワーク アドミッション制御 (NAC) 製品です。この製品を使用して、ネットワーク管理者は、ユーザをネットワークに許可する前に、有線、無線、およびリモートユーザおよびマシンを認証、許可、評価、修正できます。NAC アプライアンスは、マシンがセキュリティ ポリシーに準拠しているかどうかを判別し、脆弱性を修復してから、ネットワークへのアクセスを許可します。

NAC アプライアンスは、インバンドモードとアウトオブバンドモードの 2 つのモードで利用できます。お客様は、必要ならば両方のモードを導入して、それぞれが特定のタイプのアクセスを担当するようにすることもできます。たとえば、インバンドで無線接続ユーザをサポートし、アウトオブバンドで有線接続ユーザを担当するといった構成も可能です。

コントローラ上に NAC アウトオブバンド機能を実装するには、WLAN またはゲスト LAN 上で NAC のサポートを有効にしてから、この WLAN またはゲスト LAN を、隔離 VLAN (信頼できない VLAN) およびアクセス VLAN (信頼できる VLAN) で設定されたインターフェイスにマッピングする必要があります。クライアントは、アソシエートしてレイヤ 2 認証を完了すると、アクセス VLAN サブネットから IP アドレスを取得しますが、クライアントの状態は Quarantine となります。NAC アウトオブバンド機能の導入中は、コントローラが接続されたレイヤ 2 スイッチと NAC アプライアンスとの間でのみ隔離 VLAN が許可されること、および NAC アプライアンスが一意的な隔離 - アクセス VLAN マッピングで設定されていることを確認します。クライアントのトラフィックは、NAC アプライアンスにトランクされた隔離 VLAN に渡されます。ポスチャ検証が終了すると、クライアントは修復のための処置を実行するように促されます。クリーニングが完了すると、NAC アプライアンスはコントローラを更新してクライアントの状態を Quarantine から Access へ変更します。

コントローラとスイッチとの間のリンクをトランクとして設定することにより、隔離 VLAN (110) とアクセス VLAN (10) を有効にしています。レイヤ 2 スイッチ上では、隔離トラフィックが NAC アプライアンスにトランクされ、アクセス VLAN トラフィックがレイヤ 3 スイッチに直接送信されます。NAC アプライアンス上の隔離 VLAN に到達するトラフィックは、静的なマッピング設定に基づいてアクセス VLAN にマップされます。

図 49: NAC アウトオブバンド統合の例



290/550

## NAC アウトオブバンド統合の設定 (GUI)

**ステップ 1** 次の手順で、動的インターフェイスに対して隔離 VLAN を設定します。

- [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。
- [New] をクリックして、新たに動的インターフェイスを作成します。
- [Interface Name] テキストボックスに、"quarantine" など、このインターフェイスの名前を入力します。
- [VLAN ID] テキストボックスでは、アクセス VLAN ID にゼロ以外の値（「10」など）を入力してください。
- [Apply] をクリックして、変更を確定します。[Interfaces > Edit] ページが表示されます。
- [Quarantine] チェックボックスをオンにして、隔離 VLAN ID に「110」などのゼロ以外の値を入力します。
 

(注) ネットワーク全体で一意的な隔離 VLAN を設定することを推奨します。同じモビリティグループ内に複数のコントローラが設定されており、すべてのコントローラのアクセスインターフェイスが同じサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、同じ隔離 VLAN を保持する必要があります。同じモビリティグループ内に複数のコントローラが設定されており、すべてのコントローラのアクセスインターフェイスが別々のサブネット内にある場合、ネットワークに NAC アプリケーションが 1 つだけならば、別々の隔離 VLAN を保持する必要があります。
- このインターフェイスの残りのテキストボックス (IP アドレス、ネットマスク、デフォルトゲートウェイなど) を設定します。
- [Apply] をクリックして変更内容を保存します。

**ステップ 2** 次の手順で、WLAN またはゲスト LAN に対して NAC アウトオブバンドのサポートを設定します。

- [WLANs] を選択して、[WLANs] ページを開きます。

- b) 必要な WLAN またはゲスト LAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。
- c) [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。
- d) この WLAN またはゲスト LAN に対して NAC アウトオブバンドのサポートを設定するには、[NAC State] チェックボックスをオンにします。NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ (デフォルト値) のままとします。
- e) [Apply] をクリックして、変更を確定します。

**ステップ 3** 次の手順で、特定のアクセス ポイント グループに対して NAC アウトオブバンドのサポートを設定します。

- a) [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
- b) 目的のアクセス ポイント グループの名前をクリックします。
- c) [WLANs] タブを選択して、[AP Groups > Edit] ([WLANs]) ページを開きます。
- d) [Add New] をクリックして、このアクセス ポイント グループに WLAN を割り当てます。[Add New] のセクションがページ上部に表示されます。
- e) [WLAN SSID] ドロップダウンリストから、この WLAN の SSID を選択します。
- f) [Interface Name] ドロップダウンリストから、アクセス ポイント グループをマップするインターフェイスを選択します。NAC アウトオブバンドのサポートを有効にする場合は、隔離 VLAN を選択します。
- g) このアクセス ポイント グループに対して NAC アウトオブバンドのサポートを有効にするには、[NAC State] チェックボックスをオンにします。NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ (デフォルト値) のままとします。
- h) [Add] をクリックして、この WLAN をアクセス ポイント グループに追加します。この WLAN が、このアクセス ポイント グループに割り当てられている WLAN のリストに表示されます。  
(注) この WLAN をアクセス ポイント グループから削除する場合は、カーソルをこの WLAN の青のドロップダウン矢印の上に置いて、[Remove] を選択します。

**ステップ 4** [Save Configuration] をクリックして、変更を保存します。

**ステップ 5** 次の手順で、クライアントの現在の状態 (Quarantine または Access) を表示します。

- a) [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。
- b) 目的のクライアントの MAC アドレスをクリックして、[Clients > Detail] ページを開きます。NAC 状態が、[Security Information] のセクションに表示されます。  
(注) クライアントがプロービングを行っている場合、クライアントが WLAN にまだアソシエートされていない場合、またはクライアントがレイヤ 2 認証を完了できない場合、クライアントの状態は「Invalid」として表示されます。

## NAC アウトオブバンド統合の設定 (CLI)

**ステップ 1** 動的インターフェイスに対して隔離 VLAN を設定するには、次のコマンドを入力します。

**config interface quarantine vlan interface\_name vlan\_id**

(注) コントローラ上のインターフェイスごとに一意の隔離 VLAN を設定する必要があります。

インターフェイスで隔離 VLAN を無効にするには、VLAN ID に 0 を入力します。

**ステップ 2** WLAN またはゲスト LAN に対して NAC アウトオブバンドサポートを有効または無効にするには、次のコマンドを入力します。

**config {wlan | guest-lan} nac {enable | disable} {wlan\_id | guest\_lan\_id}**

**ステップ 3** 特定のアクセス ポイント グループに対して NAC アウトオブバンドサポートを有効または無効にするには、次のコマンドを入力します。

**config wlan appgroup nac {enable | disable} group\_name wlan\_id**

**ステップ 4** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 5** NAC 状態など、WLAN またはゲスト LAN の構成を表示するには、次のコマンドを入力します。

**show {wlan wlan\_id | guest-lan guest\_lan\_id}**

以下に類似した情報が表示されます。

```
WLAN Identifier..... 1
Profile Name..... wlan
Network Name (SSID)..... wlan
Status..... Disabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control

 NAC-State..... Enabled
 Quarantine VLAN..... 110
 ...
```

**ステップ 6** クライアントの現在の状態 (Quarantine または Access) を表示するには、次のコマンドを入力します。

**show client detailed client\_mac**

以下に類似した情報が表示されます。

```
Client's NAC state..... QUARANTINE
```

(注) クライアントがプロービングを行っている場合、クライアントが WLAN にまだアソシエートされていない場合、またはクライアントがレイヤ 2 認証を完了できない場合、クライアントの状態は「Invalid」として表示されます。



# 第 100 章

## パッシブクライアントの設定

- [パッシブクライアントの制約事項](#), 791 ページ
- [パッシブクライアントについて](#), 791 ページ
- [パッシブクライアントの設定 \(GUI\)](#), 792 ページ
- [パッシブクライアントの設定 \(CLI\)](#), 794 ページ

### パッシブクライアントの制約事項

- パッシブクライアント機能は、AP グループおよび FlexConnect によって中央でスイッチされる WLAN ではサポートされません。

### パッシブクライアントについて

パッシブクライアントとは、固定 IP アドレスが設定されている、スケールやプリンタなどのワイヤレスデバイスです。これらのクライアントは、アクセスポイントにアソシエートするとき、IP アドレス、サブネットマスク、およびゲートウェイ情報などの IP 情報を送信しません。その結果、パッシブクライアントが使用された場合、それらのクライアントが DHCP を使用しない限り、コントローラではその IP アドレスは認識されません。

現在、Wireless LAN Controller は ARP 要求のプロキシとして動作します。ARP 要求を受信すると、コントローラは、クライアントに直接要求を渡す代わりに、ARP 応答で応答します。このシナリオには、次の 2 つの利点があります。

- クライアントに ARP 要求を送信するアップストリーム デバイスは、クライアントが配置されている場所を認識しません。
- 携帯電話やプリンタなどのバッテリー駆動デバイスでは、すべての ARP 要求に応答する必要がないため、電力が保持されます。

ワイヤレス コントローラには、パッシブ クライアントに関する IP 関連の情報がないため、ARP 要求に応答できません。現在の動作では、ARP 要求のパッシブクライアントへの転送は許可されていません。パッシブクライアントへのアクセスを試みるアプリケーションは、失敗します。

パッシブクライアント機能は、有線クライアントとワイヤレスクライアント間の ARP 要求および応答の交換を可能にします。この機能が有効である場合、コントローラは、目的のワイヤレスクライアントが RUN 状態になるまで、有線クライアントからワイヤレスクライアントへ ARP 要求を渡すことができます。



(注) ローカルにスイッチされる WLAN を持つ FlexConnect AP の場合、パッシブクライアント機能によって、ARP 要求のブロードキャストが有効になり、AP はクライアントの代わりに応答します。

## パッシブクライアントの設定 (GUI)

### はじめる前に

パッシブクライアントを設定するには、マルチキャスト-マルチキャストまたはマルチキャスト-ユニキャスト モードを有効にする必要があります。

**ステップ 1** [Controller] > [General] を選択して [General] ページを開きます。

**ステップ 2** [AP Multicast Mode] ドロップダウン リストで、次のいずれかのオプションを選択します。

- [Unicast] : ユニキャストを使用してマルチキャストパケットを送信するようにコントローラを設定します。これは、デフォルト値です。
- [Multicast] : マルチキャストを使用してマルチキャストパケットを CAPWAP マルチキャストグループに送信するようにコントローラを設定します。

**ステップ 3** [AP Multicast Mode] ドロップダウン リストから [Multicast] を選択します。[Multicast Group Address] テキストボックスが表示されます。

**ステップ 4** [Multicast Group Address] テキストボックスに、マルチキャストグループの IP アドレスを入力します。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** 次の手順で、グローバル マルチキャスト モードを有効にします。

- a) [Controller] > [Multicast] を選択します。
- b) [Enable Global Multicast Mode] チェックボックスをオンにします。

## マルチキャスト-マルチキャスト モードの有効化 (GUI)

### はじめる前に

パッシュクライアントを設定するには、マルチキャスト-マルチキャストまたはマルチキャスト-ユニキャスト モードを有効にする必要があります。

**ステップ 1** [Controller] > [General] の順に選択して、[General] ページを開きます。

**ステップ 2** [AP Multicast Mode] ドロップダウンリストで、次のいずれかのオプションを選択します。

- [Unicast] : ユニキャストを使用してマルチキャストパケットを送信するようにコントローラを設定します。これは、デフォルト値です。
- [Multicast] : マルチキャストを使用してマルチキャストパケットを CAPWAP マルチキャストグループに送信するようにコントローラを設定します。

**ステップ 3** [AP Multicast Mode] ドロップダウンリストから [Multicast] を選択します。[Multicast Group Address] テキストボックスが表示されます。

(注) ユニキャストだけがサポートされるため、Cisco Flex 7500 シリーズコントローラの AP マルチキャストモードを設定することはできません。

**ステップ 4** [Multicast Group Address] テキストボックスに、マルチキャストグループの IP アドレスを入力します。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** 次の手順で、グローバルマルチキャストモードを有効にします。

- a) [Controller] > [Multicast] を選択します。
- b) [Enable Global Multicast Mode] チェックボックスをオンにします。

## コントローラでのグローバルマルチキャストモードの有効化 (GUI)

**ステップ 1** [Controller] > [Multicast] の順に選択して [Multicast] ページを開きます。

(注) [Enable IGMP Snooping] テキストボックスは、[Enable Global Multicast Mode] を有効にしている場合のみ、強調表示されます。[IGMP Timeout (seconds)] テキストボックスは、[Enable IGMP Snooping] テキストボックスを有効にしている場合のみ、強調表示されます。

**ステップ 2** [Enable Global Multicast Mode] チェックボックスをオンにして、マルチキャストモードを有効にします。この手順では、マルチキャスト方法を使用してマルチキャストパケットを CAPWAP マルチキャストグループに送信するようにコントローラを設定します。

(注) Cisco Flex 7500 シリーズコントローラのグローバルなマルチキャストモードを設定することはできません。

- ステップ 3 [Enable IGMP Snooping] チェックボックスをオンにして、IGMP スヌーピングを有効にします。デフォルト値はディセーブルです。
- ステップ 4 IGMP タイムアウトを設定するための [IGMP Timeout] テキストボックスに、30 ~ 7200 秒の値を入力します。
- ステップ 5 [Apply] をクリックして、変更を確定します。
- 

## コントローラでのパッシブクライアント機能の有効化 (GUI)

---

- ステップ 1 [WLAN]>[WLANs]>[WLAN ID] を選択し、[WLANs>Edit] ページを開きます。デフォルトでは、[General] タブが表示されます。
- ステップ 2 [Advanced] タブを選択します。
- ステップ 3 [Passive Client] チェックボックスをオンにして、パッシブクライアント機能を有効にします。
- ステップ 4 [Apply] をクリックして、変更を確定します。
- 

## パッシブクライアントの設定 (CLI)

---

- ステップ 1 コントローラ上でマルチキャストを有効にするには、次のコマンドを入力します。  
**config network multicast global enable**  
デフォルト値はディセーブルです。
- ステップ 2 マルチキャストを使用して、アクセスポイントにマルチキャストを送信するようにコントローラを設定するには、次のコマンドを入力します。  
**config network multicast mode multicast multicast\_group\_IP\_address**
- ステップ 3 無線 LAN でパッシブクライアントを設定するには、次のコマンドを入力します。  
**config wlan passive-client {enable | disable} wlan\_id**
- ステップ 4 WLAN を設定するには、次のコマンドを入力します。  
**config wlan**
- ステップ 5 次のコマンドを入力して、変更を保存します。  
**save config**
- ステップ 6 特定の WLAN のパッシブクライアント情報を表示するには、次のコマンドを入力します。  
**show wlan 2**



- ステップ 7** パッシブクライアントが AP に正しくアソシエートされているかどうか、およびパッシブクライアントがコントローラで DHCP Required 状態に移行したかどうかを確認するには、次のコマンドを入力します。  
**debug client mac\_address**
- ステップ 8** クライアントの詳細情報を表示するには、次のコマンドを入力します。  
**show client detail mac\_address**
- ステップ 9** 有線クライアントがクライアントとの接続を試みたときに、クライアントが RUN 状態に移行したかどうかをチェックするには、次のコマンドを入力します。  
**debug client mac\_address**
- ステップ 10** ARP 要求が有線側からワイヤレス側に転送されるかどうかを設定してチェックするには、次のコマンドを入力します。  
**debug arp all enable**
-





## 第 101 章

# クライアント プロファイルの設定

- [クライアントプロファイルを設定するための前提条件](#), 797 ページ
- [クライアントプロファイルの設定に関する制約事項](#), 798 ページ
- [クライアントプロファイルについて](#), 798 ページ
- [クライアントプロファイルの設定 \(GUI\)](#), 798 ページ
- [クライアントプロファイルの設定 \(CLI\)](#), 799 ページ

## クライアント プロファイルを設定するための前提条件

- デフォルトで、クライアントのプロファイルはすべての WLAN 上で無効です。
- クライアントプロファイルは、ローカルモードと FlexConnect モードのアクセス ポイントでサポートされます。
- コントローラでは DHCP プロキシと DHCP ブリッジ モードの両方がサポートされます。
- WLAN のアカウントिंग サーバの設定は、1.1 MnR 以降のリリースを実行する ISE を指している必要があります。Cisco の ACS では、クライアントプロファイルはサポートされていません。
- 使用されている DHCP サーバのタイプは、クライアントのプロファイルに影響しません。
- DHCP\_REQUEST のパケットに ISE プロファイル済みデバイス リストで見つかった文字列が含まれている場合、クライアントは自動的にプロファイルされます。
- クライアントは、Accounting request パケットで送信される MAC アドレスに基づいて識別されます。
- プロファイルが有効になると MAC アドレスだけがアカウントング パケットの発信側ステーション ID として送信されます。
- クライアントプロファイルを有効にするには、DHCP Required フラグを有効にし、ローカル認証フラグを無効にする必要があります。

## クライアントプロフィールの設定に関する制約事項

- プロファイルは、次のシナリオのクライアントではサポートされません。
  - スタンドアロンモードで FlexConnect モード AP とアソシエートしているクライアント。
  - ローカルスイッチングが有効な状態でローカル認証が行われる場合に FlexConnect モード AP とアソシエートしているクライアント。
- ローカルスイッチングの FlexConnect モードの AP でプロファイルが有効である場合、VLAN オーバーライドだけが AAA Override 属性としてサポートされます。
- コントローラによる DHCP プロファイル情報の解析中にクライアントが要求を送信する度に、プロファイル情報は一度だけ ISE に送信されます。

## クライアントプロフィールについて

クライアントが WLAN にアソシエートしようとする場合、プロセスで受信した情報からクライアントタイプを決定することができます。コントローラは情報のコレクタとして機能し、必要なデータとともに最適な形式で ISE を送信します。

## クライアントプロフィールの設定 (GUI)

---

**ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。

**ステップ 2** [WLAN ID] をクリックします。[WLANs > Edit] ページが表示されます。

**ステップ 3** [Advanced] タブをクリックします。

**ステップ 4** RADIUS およびローカルのクライアントプロフィール領域で、次を行います。

- a) DHCP に基づいてクライアントをプロフィールするには、DHCP Profiling チェックボックスを選択します。
- b) HTTP に基づいてクライアントをプロフィールするには、HTTP Profiling チェックボックスを選択します。

WLAN では、RADIUS モードとローカルモードの両方でクライアントプロフィールを設定できます。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** [Save Configuration] をクリックします。

---

## クライアント プロファイルの設定 (CLI)

- 次のコマンドを入力して、DHCP に基づいて WLAN に対してクライアント プロファイルを有効または無効にします。

```
config wlan profiling radius dhcp {enable | disable} wlan-id
```

- 次のコマンドを入力して、HTTP、DHCP、またはそれらの両方に基づいて、WLAN に対して RADIUS モードでクライアント プロファイルを有効または無効にします。

```
config wlan profiling radius {dhcp | http | all} {enable | disable} wlan-id
```




---

(注) DHCP と HTTP の両方に基づいたクライアント プロファイルを設定するには、**all** パラメータを使用します。

---

- 次のコマンドを入力して、HTTP、DHCP、またはそれらの両方に基づいて、WLAN に対して ローカル モードでクライアント プロファイルを有効または無効にします。

```
config wlan profiling local {dhcp | http | all} {enable | disable} wlan-id
```

- WLAN でクライアント プロファイルのステータスを表示するには、次のコマンドを入力します。

```
show wlan wlan-id
```

- クライアント プロファイルのデバッグを有効または無効にするには、次のコマンドを入力します。

```
debug profiling {enable | disable}
```





# 第 102 章

## WLAN ごとの RADIUS 送信元サポートの設定

- [WLAN ごとの RADIUS 送信元サポートの前提条件](#), 801 ページ
- [WLAN ごとの RADIUS 送信元サポートの制約事項](#), 801 ページ
- [WLAN ごとの RADIUS 送信元サポートについて](#), 801 ページ
- [WLAN ごとの RADIUS 送信元サポートの設定 \(CLI\)](#), 802 ページ
- [WLAN ごとの RADIUS 送信元サポートのステータスのモニタリング \(CLI\)](#), 802 ページ

### WLAN ごとの RADIUS 送信元サポートの前提条件

- コントローラは選択されたインターフェイスのみからトラフィックを受信するので、認証サーバ (RADIUS) の新しい ID をフィルタする適切なルールを実行する必要があります。

### WLAN ごとの RADIUS 送信元サポートの制約事項

- `callStationID` は、RADIUS RFC での 802.1X に準拠するよう、常に `APMAC:SSID` 形式になります。これは、レガシー動作でもあります。web-auth では、`config radius callStationIDType` コマンドで使用可能なさまざまな形式を使用できます。
- AP グループまたは AAA オーバーライドが使用されると、送信元インターフェイスは WLAN インターフェイスのままとなり、新規の AP グループまたは RADIUS プロファイルの設定で指定されたインターフェイスにはなりません。

### WLAN ごとの RADIUS 送信元サポートについて

デフォルトで、コントローラは、グローバルリストの代わりに、管理インターフェイスの IP アドレスがのすべての RADIUS トラフィックの送信元になります。つまり、設定されている特定の

RADIUS サーバが WLAN に存在する場合でも、使用される ID は管理インターフェイスの IP アドレスです。

WLAN をフィルタする場合は RFC 3580 で APMAC SSID 形式に設定された `callStationID` を使用できます。また、`NAS-IP-Address` 属性を使用することで、認証サーバ上のフィルタリングを WLAN ごとの送信元インターフェイス上にまで拡張できます。

WLAN ごとの RADIUS 送信元サポートを有効にすると、コントローラは、設定されている動的インターフェイスを使用して特定の WLAN のすべての RADIUS トラフィックを送信します。また、それに応じて、RADIUS 属性が `Identity` に一致するように変更されます。この機能は、各 WLAN が別個のレイヤ 3 `Identity` を持つ可能性がある場合に、WLAN ごとの RADIUS トラフィックでコントローラを効果的に仮想化します。この機能は、ACS ネットワーク アクセス制限、およびネットワーク アクセス プロファイルと統合する展開に役立ちます。

アドレスの送信元として WLAN ごとの動的インターフェイスを用いる管理インターフェイスなどを使用するいくつかの WLAN および通常の RADIUS トラフィックの送信元と、WLAN ごとの RADIUS 送信元サポートを組み合わせたことができます。

## WLAN ごとの RADIUS 送信元サポートの設定 (CLI)

**ステップ 1** `config wlan disable wlan-id` コマンドを入力して、WLAN を無効にします。

**ステップ 2** 次のコマンドを入力して、WLAN ごとの RADIUS 送信元サポートを有効または無効にします。

```
config wlan radius_server overwrite-interface {enable | disable} wlan-id
```

(注) 有効にすると、コントローラは、その WLAN 上のすべての RADIUS 関連トラフィックの `Identity` および送信元として、WLAN の設定に指定されたインターフェイスを `Identity` として使用します。無効にすると、コントローラは、`NAS-IP-Address` 属性の `Identity` として管理インターフェイスを使用します。RADIUS サーバが直接接続された動的インターフェイスにある場合、RADIUS トラフィックはそのインターフェイスから送信されます。それ以外の場合は、管理 IP アドレスが使用されます。いずれのケースでも、機能が有効でない限り、`NAS-IP-Address` 属性は管理インターフェイスのままとなります。

**ステップ 3** `config wlan enable wlan-id` コマンドを入力して、WLAN を有効にします。

(注) CiscoSecure ACS を使用して、RADIUS サーバ側で要求をフィルタリングできます。要求は、ネットワーク アクセス制限ルールを介して、`NAS-IP-Address` 属性によってフィルタリング (受け入れまたは拒否) できます。使用されるフィルタリングは、CLI/DNIS フィルタリングです。

## WLAN ごとの RADIUS 送信元サポートのステータスのモニタリング (CLI)

機能が有効または無効かどうかを確認するには、次のコマンドを入力します。

```
show wlan wlan-id
```



例

次の例は、WLAN ごとの RADIUS 送信元サポートが WLAN 1 で有効であることを示しています。

**show wlan 1**

次のような情報が表示されます。

```
WLAN Identifier..... 4
Profile Name..... example
Network Name (SSID)..... example
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Enabled
AAA Policy Override..... Disabled
Network Admission Control
...
Radius Servers
 Authentication..... Global Servers
 Accounting..... Global Servers
 Overwrite Sending Interface..... Enabled
Local EAP Authentication..... Disabled
```





# 第 103 章

## モバイル コンシェルジュの設定

---

- [モバイル コンシェルジュについて](#), 805 ページ
- [802.11u Mobility Services Advertisement Protocol の設定](#), 808 ページ
- [802.11u HotSpot の設定](#), 809 ページ
- [802.1Q-in-Q VLAN タギングの情報](#), 816 ページ
- [802.1Q-in-Q VLAN タギングの制約事項](#), 817 ページ
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\)](#) , 818 ページ
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\)](#) , 819 ページ

### モバイル コンシェルジュについて

モバイル コンシェルジュは、外部ネットワークで相互運用できるように 802.1X 対応クライアントを有効にするソリューションです。モバイル コンシェルジュ機能は、クライアントにサービスのアベイラビリティに関する情報を提供し、使用可能なネットワークをアソシエートするのに役立ちます。

ネットワークから提供されるサービスは、次の 2 つのプロトコルに大きく分類できます。

- 802.11u MSAP
- 802.11u HotSpot 2.0

## モバイル コンシェルジュの設定 (802.11u)

### モバイル コンシェルジュの設定 (802.11u) (GUI)

- 
- ステップ 1** [WLAN] を選択して、[WLANs] ページを開きます。
- ステップ 2** 802.11u パラメータを設定する対象の WLAN の青いドロップダウンの矢印の上にカーソルを置いて、[802.11u] を選択します。[802.11u] ページが表示されます。
- ステップ 3** [802.11u Status] チェックボックスをオンにして WLAN の 802.11u を有効にします。
- ステップ 4** [802.11u General Parameters] 領域で、次の手順を実行します。
- [Internet Access] チェックボックスを選択して、この WLAN からインターネット サービスを提供できるようにします。
  - [Network Type] ドロップダウン リストから、この WLAN に設定する 802.11u を表すネットワーク タイプを選択します。
  - [Network Auth Type] ドロップダウン リストから、このネットワークの 802.11u パラメータに設定する認証タイプを選択します。
  - [HESSID] ボックスに、Homogenous Extended Service Set Identifier (HESSID) 値を入力します。HESSID は、HESS を識別する 6 オクテットの MAC アドレスです。
  - IP アドレスが IPv4 形式の場合は、[IPv4 Type] ドロップダウン リストから IPv4 アドレス タイプを選択します。
  - [IPv6 Type] ドロップダウン リストから、IPv6 アドレス タイプを使用できるようにするかどうかを選択します。
- ステップ 5** [OUI List] 領域で、次の手順を実行します。
- [OUI] テキスト ボックスに、組織固有識別子を、3 または 5 バイト (6 または 10 文字) の 16 進数で入力します。たとえば、AABBDF となります。
  - [Is Beacon] チェックボックスをオンにして、OUI ビーコン応答を有効にします。  
(注) このフィールドを有効にすると、最大 3 つの OUI を持つことができます。
  - [OUI Index] ドロップダウン リストから、1 から 32 までの値を選択します。デフォルトは 1 です。
  - [Add] をクリックして、この OUI エントリを WLAN に追加します。  
このエントリを削除するには、青いドロップダウン矢印画像の上にカーソルを移動し、[Remove] を選択します。
- ステップ 6** [Domain List] 領域で、次の手順を実行します。
- [Domain Name] ボックスに、WLAN で動作しているドメイン名を入力します。
  - [Domain Index] ドロップダウン リストで、ドメイン名のインデックスを 1 ~ 32 の値から選択します。デフォルトは 1 です。
  - [Add] をクリックして、このドメイン エントリを WLAN に追加します。  
このエントリを削除するには、青いドロップダウン矢印画像の上にカーソルを移動し、[Remove] を選択します。

**ステップ 7** [Realm List] 領域で、次の手順を実行します。

- a) [Realm] テキストボックスに、WLAN に割り当てるレルム名を入力します。
- b) [Realm Index] ドロップダウンリストで、レルムのインデックスを 1～32 の値から選択します。デフォルトは 1 です。
- c) [Add] をクリックして、ドメイン エントリをこの WLAN に追加します。  
このエントリを削除するには、青いドロップダウン矢印画像の上にカーソルを移動し、[Remove] を選択します。

**ステップ 8** [Cellular Network Information List] 領域で、次の手順を実行します。

- a) [Country Code] テキストボックスに、3 文字のモバイル Country Code を入力します。
- b) [CellularIndex] ドロップダウンリストで、1～32 の値を選択します。デフォルトは 1 です。
- c) [Network Code] テキストボックスに、ネットワーク コードを入力します。ネットワーク コードは 2 または 3 文字です。
- d) [Add] をクリックして、このセルラーのネットワーク情報を WLAN に追加します。  
このエントリを削除するには、青いドロップダウン矢印画像の上にカーソルを移動し、[Remove] を選択します。

**ステップ 9** [Apply] をクリックします。

## モバイル コンシェルジュの設定 (802.11u) (CLI)

- WLAN の 802.11u を有効または無効にするには、次のコマンドを入力します。  
**config wlan hotspot dot11u {enable | disable} wlan-id**
- Third Generation Partnership Project のセルラー ネットワークに関する情報を追加または削除するには、次のコマンドを入力します。  
**config wlan hotspot dot11u 3gpp-info {add index mobile-country-code network-code wlan-id | delete index wlan-id}**
- 802.11u ネットワークで動作しているエンティティのドメイン名を設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u domain {{{add | modify} wlan-id domain-index domain-name} | {delete wlan-id domain-index}}**
- WLAN の Homogenous Extended Service Set Identifier (HESSID) 値を設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u hessid hessid wlan-id**  
HESSID は、HESS を識別する 6 オクテットの MAC アドレスです。
- WLAN の IPv4 および IPv6 IP アドレスに使用可能な IP アドレスのタイプを設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u ipaddr-type ipv4-type ipv6-type wlan-id**
- ネットワーク認証タイプを設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u auth-type network-auth wlan-id**

- ローミング コンソーシアムの OI リストを設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u roam-oi** {{{add | modify} wlan-id oi-index oi is-beacon} | {delete wlan-id oi-index}}
- 802.11u ネットワーク タイプとインターネット アクセスを設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u network-type** wlan-id network-type internet-access
- WLAN のレルムを設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u nai-realm** {{{add | modify} realm-name wlan-id realm-index realm-name | {delete realm-name wlan-id realm-index}}
- レルムの認証方式を設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u nai-realm** {add | modify} auth-method wlan-id realm-index eap-index auth-index auth-method auth-parameter
- レルムの認証方式を削除するには、次のコマンドを入力します。  
**config wlan hotspot dot11u nai-realm delete auth-method** wlan-id realm-index eap-index auth-index
- レルムの拡張認証プロトコル (EAP) 方式を設定するには、次のコマンドを入力します。  
**config wlan hotspot dot11u nai-realm** {add | modify} eap-method wlan-id realm-index eap-index eap-method
- レルムの EAP 方式を削除するには、次のコマンドを入力します。  
**config wlan hotspot dot11u nai-realm delete eap-method** wlan-id realm-index eap-index

## 802.11u Mobility Services Advertisement Protocol の設定

### 802.11u MSAP について

MSAP (Mobility Services Advertisement Protocol) は、ネットワーク接続を確立するためのポリシーセットを使用して設定されたモバイルデバイスで主に使用するために設計されています。これらのサービスは、上位層サービスを提供するデバイス、つまりサービスプロバイダー経由で有効にされるネットワーク サービス向けです。

サービスアドバタイズメントは、MSAPを使用して、Wi-Fiアクセスネットワークへのアソシエーションの前にサービスをモバイル デバイスに提供します。この情報はサービスアドバタイズメントで伝送されます。シングルモードまたはデュアルモードモバイル デバイスは、アソシエーションの前にサービス ネットワークをネットワークにクエリーします。デバイスによるネットワークの検出および選択機能では、ネットワークに join する判断においてサービスアドバタイズメントを使用する場合があります。

## 802.11u MSAP の設定 (GUI)

- 
- ステップ 1 [WLAN] を選択して、[WLANs] ページを開きます。
- ステップ 2 MSAP パラメータを設定する目的の WLAN の青いドロップダウンの矢印の上にカーソルを置いて、[Service Advertisements] を選択します。 [Service Advertisement] ページが表示されます。
- ステップ 3 サービス アドバタイズメントを有効にします。
- ステップ 4 この WLAN のサーバインデックスを入力します。サーバのインデックス フィールドによって、BSSID を使用して到達可能である場所を提供する MSAP サーバ インスタンスを一意に識別します。
- ステップ 5 [Apply] をクリックします。
- 

## MSAP の設定 (CLI)

- WLAN の MSAP を有効または無効にするには、次のコマンドを入力します。  
**config wlan hotspot msap {enable | disable} wlan-id**
- サーバ ID を割り当てるには、次のコマンドを入力します。  
**config wlan hotspot msap server-id server-id wlan-id**

## 802.11u HotSpot の設定

### 802.11u HotSpot について

この機能は IEEE 802.11 デバイスを外部ネットワークと相互運用できるようにするものであり、サービスが登録制か無料かに関係なく、ホットスポットまたはその他のパブリック ネットワーク で一般的に使用されています。

インターワーキング サービスはネットワークの検出や選択を支援し、外部ネットワークから情報を転送できるようにします。アソシエーション前にネットワークに関する情報をステーションに提供します。インターワーキングは、家、企業、およびパブリック アクセスのユーザに役立つだけでなく、製造業者やオペレータが IEEE 802.11 カスタマーに共通のコンポーネントおよびサービスを提供するのにも役立ちます。これらのサービスは、コントローラの各 WLAN 単位で設定されます。

## 802.11u Hotspot の設定 (GUI)

- ステップ 1** [WLAN] を選択して、[WLANs] ページを開きます。
- ステップ 2** HotSpot パラメータを設定する対象の WLAN の青いドロップダウンの矢印の上にカーソルを置いて、[HotSpot] を選択します。[WLAN > HotSpot 2.0] ページが表示されます。
- ステップ 3** [WLAN > HotSpot 2.0] ページで、HotSpot2 を有効にします。
- ステップ 4** WAN リンク パラメータを設定するには、次の手順を実行します。
- [WAN Link Status] ドロップダウン リストから、ステータスを選択します。デフォルトのステータスは [Not Configured] です。
  - [WAN Symmetric Link Status] ドロップダウン リストから、ステータスとして [Different] または [Same] を選択します。
  - WAN のダウンリンクおよびアップリンクの速度を入力します。最大値は 4,294,967,295 kbps です。
- ステップ 5** [Operator Name List] 領域で、次の手順を実行します。
- [Operator Name] テキスト ボックスに、802.11 オペレータの名前を入力します。
  - [Operator index] ドロップダウン リストから、オペレータのインデックス値として 1 ~ 32 の値を選択します。
  - [Language Code] テキスト ボックスに、言語を定義する ISO-14962-1997 エンコード文字列を入力します。この文字列は 3 文字の言語コードです。
  - [Add] をクリックして、オペレータの詳細を追加します。オペレータの詳細が表形式で表示されます。オペレータを削除するには、青のドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。
- ステップ 6** [Port Config List] 領域で、次の手順を実行します。
- [IP Protocol] ドロップダウン リストから、有効にする IP プロトコルを選択します。
  - [Port No] ドロップダウン リストから、WLAN で有効にするポート番号を選択します。
  - [Status] ドロップダウン リストから、ポートのステータスを選択します。
  - [Index] ドロップダウン リストから、ポート設定のインデックス値を選択します。
  - [Add] をクリックして、ポート設定パラメータを追加します。ポート コンフィギュレーション リストからポートを削除するには、青いドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。
- ステップ 7** [Apply] をクリックします。

## Hotspot 2.0 の設定 (CLI)

- WLAN の HotSpot2 を有効または無効にするには、次のコマンドを入力します。  
**config wlan hotspot hs2 {enable | disable}**
- WLAN のオペレータ名を設定するには、次のコマンドを入力します。



**config wlan hotspot hs2 operator-name {add | modify} wlan-id index operator-name lang-code**

次のオプションを使用できます。

- *wlan-id* : オペレータ名を設定する WLAN の ID。
- *index* : オペレータのオペレータ インデックス。指定できる範囲は 1 ~ 32 です。
- *operator-name* : 802.11 オペレータの名前。
- *lang-code* : 使用する言語。言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。言語の最初の 3 文字を英語で入力します (たとえば、英語の場合は *eng*) 。



**ヒント** キーワードまたは引数を入力した後、Tab キーを押し、コマンドの有効な値のリストを取得します。

- オペレータ名を削除するには、次のコマンドを入力します。

**config wlan hotspot hs2 operator-name delete wlan-id index**

- ポート設定パラメータを設定するには、次のコマンドを入力します。

**config wlan hotspot hs2 port-config {add | modify} wlan-id index ip-protocol port-number**

- ポート設定を削除するには、次のコマンドを入力します。

**config wlan hotspot hs2 port-config delete wlan-id index**

- WAN メトリックを設定するには、次のコマンドを入力します。

**config wlan hotspot hs2 wan-metrics wlan-id link-status symet-link downlink-speed uplink-speed**

値は次のとおりです。

- *link-status* : リンク ステータス。有効な範囲は 1 ~ 3 です。
- *symet-link* : シンメトリック リンク ステータス。たとえば、アップリンクとダウンリンクに異なる速度または同じ速度を設定できます。
- *downlink-speed* : ダウンリンク速度。最大値は 4,194,304 kbps です。
- *uplink-speed* : アップリンク速度。最大値は 4,194,304 kbps です。

- すべてのホットスポットの設定をクリアするには、次のコマンドを入力します。

**config wlan hotspot clear-all wlan-id**

- Access Network Query Protocol (ANQP) のフォーウェイ メッセージを設定するには、次のコマンドを入力します。

**config advanced hotspot anqp-4way {enable | disable | threshold value}**

- TU で ANQP のカムバック遅延値を設定するには、次のコマンドを入力します。

**config advanced hotspot cmbk-delay value**

- ワイヤレス ネットワークに転送する Gratuitous ARP (GARP) を設定するには、次のコマンドを入力します。

```
config advanced hotspot garp {enable | disable}
```

- 一定期間内に AP によってコントローラに送信される GAS 要求のアクションフレームの数を制限するには、次のコマンドを入力します。

```
config advanced hotspot gas-limit {enable num-of-GAS-required interval | disable}
```

## アクセス ポイントでの HotSpot2 の設定 (GUI)

HotSpot2 を設定する場合は、ネットワークに属するアクセス ポイントを HotSpot2 をサポートするよう設定する必要があります。

**ステップ 1** [Wireless] > [All APs] の順にクリックして、[All APs] ページを開きます。

**ステップ 2** [AP Name] リンクをクリックして、目的のアクセス ポイントの Hotspot パラメータを設定します。[AP Details] ページが表示されます。

**ステップ 3** [General] タブで、次のパラメータを設定します。

- [Venue Group] : このアクセス ポイントが属する場所のカテゴリ。 次のオプションを使用できます。
  - **Unspecified**
  - **Assembly**
  - **Business**
  - **Educational**
  - **Factory and Industrial**
  - **Institutional**
  - **Mercantile**
  - **Residential**
  - **Storage**
  - **Utility and Misc**
  - **Vehicular**
  - **Outdoor**
- [Venue Type] : 上で選択した場所のカテゴリに応じて、[Venue Type] ドロップダウン リストに場所のタイプのオプションが表示されます。
- [Venue Name] : アクセス ポイントに提供できる場所の名前。 この名前は BSS と関連付けられます。これは SSID から場所に関する十分な情報が提供されない場合に使用します。

- [Language] : 使用する言語。言語を定義する ISO-14962-1997 エンコード文字列。これは 3 文字の言語コードです。言語の最初の 3 文字を英語で入力します (たとえば、英語の場合は **eng**) 。

ステップ 4 [Apply] をクリックします。

## アクセス ポイントでの HotSpot2 の設定 (CLI)

- **config ap venue add** *venue-name venue-group venue-type lang-code ap-name* : HotSpot2 をサポートしているアクセス ポイントに、場所の詳細を追加します。

値は次のとおりです。

- *venue-name* : このアクセス ポイントが設置されている場所の名前。
- *venue-group* : 場所のカテゴリ。次の表を参照してください。
- *venue-type* : 場所のタイプ。選択した *venue-group* に応じて、場所のタイプを選択します。次の表を参照してください。
- *lang-code* : 使用する言語。言語を定義する ISO-14962-1997 エンコード文字列。これは 3 文字の言語コードです。言語の最初の 3 文字を英語で入力します (たとえば、英語の場合は **eng**) 。
- *ap-name* : アクセス ポイント名。



**ヒント** キーワードまたは引数を入力した後、Tab キーを押し、コマンドの有効な値のリストを取得します。

- **config ap venue delete** *ap-name* : アクセス ポイントから場所に関連する情報を削除します。

表 21 : 場所グループのマッピング

場所グループの名前	値	グループの場所のタイプ
未指定	0	

場所グループの名前	値	グループの場所のタイプ
アセンブリ	1	<ul style="list-style-type: none"> <li>• 0 : 未指定のアセンブリ</li> <li>• 1 : アリーナ</li> <li>• 2 : スタジアム</li> <li>• 3 : 乗客ターミナル (たとえば、空港、バス、フェリー、電車の駅)</li> <li>• 4 : 円形劇場</li> <li>• 5 : アミューズメントパーク</li> <li>• 6 : 礼拝所</li> <li>• 7 : 会議場</li> <li>• 8 : 図書館</li> <li>• 9 : 博物館</li> <li>• 10 : レストラン</li> <li>• 11 : シアター</li> <li>• 12 : バー</li> <li>• 13 : 喫茶店</li> <li>• 14 : 動物園または水族館</li> <li>• 15 : 緊急対応センター</li> </ul>
ビジネス	2	<ul style="list-style-type: none"> <li>• 0 : 未指定のビジネス</li> <li>• 1 : 医師または歯科医師のオフィス</li> <li>• 2 : 銀行</li> <li>• 3 : 消防署</li> <li>• 4 : 警察署</li> <li>• 6 : 郵便局</li> <li>• 7 : 専門家のオフィス</li> <li>• 8 : 研究および開発施設</li> <li>• 9 : 弁護士のオフィス</li> </ul>

場所グループの名前	値	グループの場所のタイプ
教育機関	3	<ul style="list-style-type: none"> <li>• 0 : 未指定の教育機関</li> <li>• 1 : 小学校</li> <li>• 2 : 中学校</li> <li>• 3 : 大学</li> </ul>
工場および産業	4	<ul style="list-style-type: none"> <li>• 0 : 未指定の工場および産業</li> <li>• 1 : 工場</li> </ul>
機関	5	<ul style="list-style-type: none"> <li>• 0 : 未指定の公共機関</li> <li>• 1 : 病院</li> <li>• 2 : 長期看護施設（療養所、ホスピスなど）</li> <li>• 3 : アルコールおよび薬物のリハビリテーションセンター</li> <li>• 4 : グループホーム</li> <li>• 5 : 刑務所または拘置所</li> </ul>
商業	6	<ul style="list-style-type: none"> <li>• 0 : 未指定の商業施設</li> <li>• 1 : 小売店</li> <li>• 2 : 食料品店</li> <li>• 3 : 自動車サービスステーション</li> <li>• 4 : ショッピングモール</li> <li>• 5 : ガソリンスタンド</li> </ul>
住居	7	<ul style="list-style-type: none"> <li>• 0 : 未指定の居住施設</li> <li>• 1 : 私邸</li> <li>• 2 : ホテルまたはモーテル</li> <li>• 3 : 寄宿舍</li> <li>• 4 : 宿泊施設</li> </ul>
倉庫	8	未指定の倉庫

場所グループの名前	値	グループの場所のタイプ
公共施設、その他	9	0：未指定の公共施設およびその他
乗り物	10	<ul style="list-style-type: none"> <li>• 0：未指定の乗り物</li> <li>• 1：自動車またはトラック</li> <li>• 2：飛行機</li> <li>• 3：バス</li> <li>• 4：フェリー</li> <li>• 5：船またはボート</li> <li>• 6：電車</li> <li>• 7：モーターバイク</li> </ul>
アウトドア	11	<ul style="list-style-type: none"> <li>• 0：未指定のアウトドア</li> <li>• 1：自治体メッシュ ネットワーク</li> <li>• 2：都市公園</li> <li>• 3：休憩施設</li> <li>• 4：交通管制施設</li> <li>• 5：バス停留所</li> <li>• 6：売店</li> </ul>

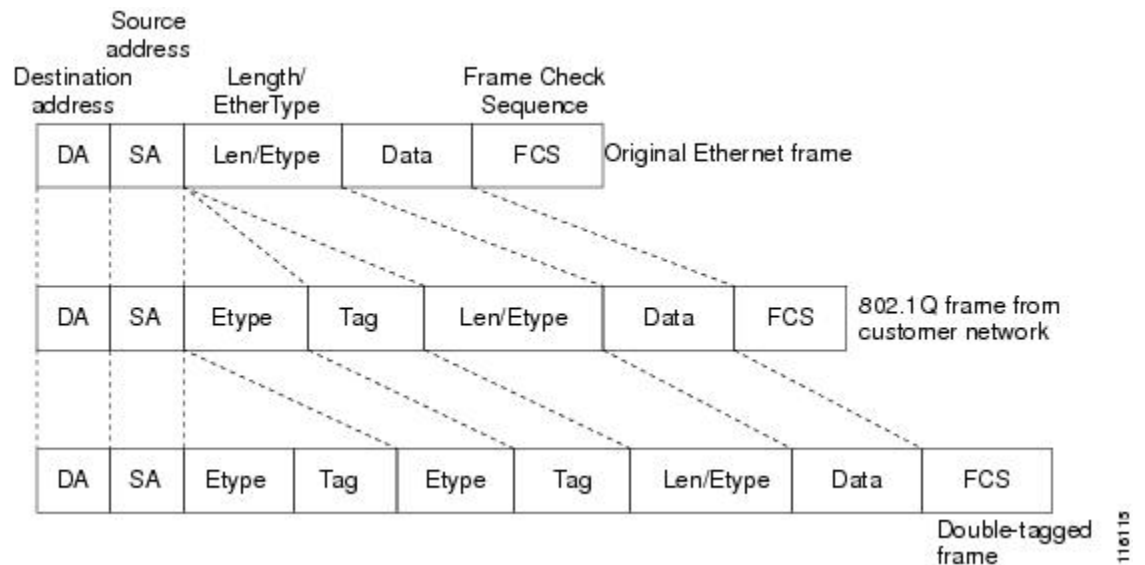
## 802.1Q-in-Q VLAN タギングの情報

クライアントごとに一意の VLAN ID 範囲を割り当てると、4096 VLAN という制限を超える可能性があります。802.1Q-in-Q VLAN タグ機能は、別の 802.1Q VLAN タグ内に 802.1Q VLAN タギングをカプセル化します。外部タグは AP グループに基づいて割り当てられ、内部 VLAN ID は AAA サーバによって動的に割り当てられます。

802.1Q-in-Q 機能を使用すれば、単一の VLAN で複数の VLAN をサポートできます。802.1Q-in-Q 機能では、VLAN ID を保存しながら、複数の VLAN のトラフィックを分離できます。下の図は、

タグなし、802.1Q タグ付き、および 802.1Q-in-Q タグ付きのイーサネット フレームを示しています。

図 50: タグなし、802.1Q タグ付き、および 802.1Q-in-Q タグ付きのイーサネット フレーム



#### 関連トピック

- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)

## 802.1Q-in-Q VLAN タギングの制約事項

- 802.1Q-in-Q VLAN タギングは、Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco 8500 シリーズ ワイヤレス LAN コントローラ、および Cisco WiSM2 でのみサポートされます。
- IGMP スヌーピングを無効にするまで、マルチキャストは有効にできません。
- 802.1Q-in-Q VLAN タギングは、レイヤ2 およびレイヤ3 のコントローラ内ローミング、およびレイヤ2 コントローラ間ローミングでのみサポートされます。レイヤ3 コントローラ間ローミングはサポートされません。
- 0x8100 は、802.1Q-in-Q イーサネットフレームの [Ether Type] フィールドに対してのみサポートされている値です。

- 中央でスイッチされるパケットでのみ、802.1Q-in-Q VLAN タギングを有効にすることができます。
- 802.1Q-in-Q VLAN タギングについては、IPv6 DHCP パケットではなく、IPv4 DHCP パケットのみ有効にすることができます。
- tunnel-type である IETF 属性は、C-VLAN のオーバーライドに必要です。
- C-VLAN は tunnel-private-group-ID /tunnel-type および tunnel-private-group-id で設定できます。

#### 関連トピック

- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)

## 802.1Q-in-Q VLAN タギングの設定 (GUI)

- 
- ステップ 1** [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
  - ステップ 2** [AP Group Name] をクリックして、対応する [AP Groups > Edit] ページを開きます。
  - ステップ 3** [General] タブをクリックして、802.1Q-in-Q VLAN タギングの詳細を設定します。
  - ステップ 4** [Enable Client Traffic QinQ] チェックボックスをオンにして、AP グループの 802.1Q-in-Q VLAN タギングを有効にします。
  - ステップ 5** [Enable DHCPv4 QinQ] チェックボックスをオンにして、AP グループの IPv4 DHCP パケットの 802.1Q-in-Q VLAN タギングを有効にします。
  - ステップ 6** [QinQ Service VLAN ID] テキスト ボックスに、802.1Q-in-Q VLAN タギングの VLAN ID を入力します。
  - ステップ 7** [Apply] をクリックします。
- 

#### 関連トピック

- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)



## 802.1Q-in-Q VLAN タギングの設定 (CLI)

- ステップ 1** 次のコマンドを入力して、AP グループの 802.1Q-in-Q VLAN タギングを有効または無効にします。  
**config wlan apgroup qinq tagging client-traffic***apgroup\_name*{enable| disable}  
 デフォルトでは、AP グループのクライアント トラフィックの 802.1Q-in-Q VLAN タギングは無効です。
- ステップ 2** 次のコマンドを入力して、AP グループのサービス VLAN を設定します。  
**config wlan apgroup qinq service-vlan***apgroup\_name vlan\_id*
- ステップ 3** 次のコマンドを入力して、AP グループのクライアント トラフィックの IPv4 DHCP パケットを有効または無効にします。  
**config wlan apgroup qinq tagging dhcp-v4***apgroup\_name*{enable| disable}  
 (注) DHCPv4 トラフィックの 802.1Q-in-Q タギングを有効にする前に、クライアント トラフィックの 802.1Q-in-Q タギングを有効にする必要があります。  
 デフォルトでは、AP グループの DHCPv4 トラフィックの 802.1Q-in-Q VLAN タギングは無効です。
- ステップ 4** 次のコマンドを入力して、AP グループの EAP for Global System for Mobile Communications (GSM) Subscriber Identity Module (EAP-SIM)、または EAP for Authentication and Key Agreement 認証クライアント トラフィックの 802.1Q-in-Q VLAN タギングを有効または無効にします。  
**config wlan apgroup qinq tagging eap-sim-aka***apgroup\_name*{enable| disable}  
 クライアント トラフィックの 802.1Q-in-Q タギングを有効にすると、EAP for Authentication and Key Agreement (EAP-AKA) および EAP-SIM トラフィックの 802.1Q-in-Q タギングが有効になります。
- ステップ 5** 次のコマンドを入力して、802.1Q-in-Q VLAN タギングが有効かどうかを確認します。  
**show wlan apgroups**
- ```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..... 5

Site Name..... CT_building1
Site Description..... APs for CT Building1
Venue Group Code..... Unspecified
Venue Type Code..... Unspecified

NAS-identifier..... CTB1
Client Traffic QinQ Enable..... TRUE
DHCPv4 QinQ Enable..... TRUE
AP Operating Class..... Not-configured
```

関連トピック

- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)



第 104 章

経路ローミングの設定

- [経路ローミングの制約事項](#), 821 ページ
- [経路ローミングについて](#), 821 ページ
- [経路ローミングの設定 \(CLI\)](#), 823 ページ

経路ローミングの制約事項

- この機能は 1 つのコントローラを使用する場合にだけ実行する必要があります。経路ローミング機能は、複数のコントローラでサポートされません。
- この機能は、802.11n 対応の屋内アクセスポイントでのみサポートされています。1 つの帯域構成の場合、最大 6 のネイバーがネイバーリストに表示されます。デュアルバンド構成の場合、最大 12 のネイバーが表示されます。
- コントローラ CLI をのみを使用して経路ローミングを設定できます。コントローラ GUI を使用する構成はサポートされていません。

経路ローミングについて

802.11k 標準では、クライアントがサービスセットの移行の候補となる既知のネイバーアクセスポイントに関する情報を含むネイバーレポートを要求することができます。802.11k ネイバーリストを使用すると、アクティブおよびパッシブスキャンの必要性を軽減できます。

経路ローミング機能は、インテリジェントでクライアントによって最適化されたネイバーリストに基づいています。

Cisco Client Extension (CCX) ネイバーリストとは異なり、802.11k ネイバーリストは動的かつオンデマンドで生成されます。コントローラ上では維持されません。802.11k ネイバーリストは、クライアントのロケーションに基づくもので、Mobility Services Engine (MSE) を必要としません。同じコントローラ上であっても異なる AP の 2 クライアントが、周囲の AP の個々の関係に応じて提供される異なるネイバーリストを設定できます。

デフォルトでは、ネイバーリストには、クライアントがアソシエートされている同じ帯域のネイバーだけが含まれます。ただし、両方の帯域のネイバーを返すために、802.11k を可能にするスイッチが存在します。

クライアントは、ビーコン内の RRM（無線リソース管理）機能の情報要素（IE）をアドバタイズする AP に関連付けた後でのみ、ネイバーリストの要求を送信します。ネイバーリストには、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

ネイバー リストの作成と最適化

802.11k ネイバー リスト要求をコントローラが受信すると、次の処理が実行されます。

- 1 コントローラは、クライアントが現在関連付けられている AP と同じ帯域で、ネイバーリストについて RRM ネイバー テーブルを検索バンドします。
- 2 コントローラは、帯域ごとにネイバーリストを6つに削減するために、AP間のRSSI（Received Signal Strength Indication）、現在のAPの現在のロケーション、Cisco Prime インフラストラクチャからのネイバーAPのフロア情報、コントローラ上でのローミング履歴情報に従ってネイバーをチェックします。このリストは、同じフロアのAPに対して最適化されています。

非 802.11k クライアントの経路ローミング

非 802.11k クライアントのローミングを最適化することもできます。クライアントが 802.11k ネイバーリスト要求を送信する必要なく、各クライアントの予測ネイバーリストを生成できます。成功した各クライアントアソシエーション/再アソシエーションの後、WLAN でこれが有効である場合、ネイバー リストを生成し、モバイルステーションのソフトウェア データ構造にリストを格納するために、同じネイバー リストの最適化を非 802.11k クライアントに適用する必要があります。クライアントプロブが異なるネイバーによって異なる RSSI 値により認識されるため、異なるロケーションのクライアントが異なるリストを持ちます。クライアントは、通常はアソシエーションまたは再アソシエーションの前にプロブするため、このリストは、更新されたほとんどのプロブデータによって構築され、クライアントがローミングする可能性が高い次の AP を予測します。

AP へのアソシエーション要求が保存された予測ネイバーリストのエントリに一致しない場合に、アソシエーションを拒否することによって、あまり望ましくないネイバーへのクライアントのローミングを抑制します。

アグレッシブ ロード バランシングに加えて、経路ローミング機能を ▪ WLAN ごとおよびグローバルにオンにするスイッチがあります。次のオプションを使用できます。

- Denial count : クライアントでアソシエーションが拒否される最大回数です。
- Prediction threshold : 経路ローミング機能をアクティブにするために、予測リスト内で必要なエントリの最小数です。

ロード バランシングおよび経路ローミングの両方で、クライアントがアソシエートする AP に影響を与えるように設計されているため、WLAN で両オプションを同時にイネーブルにすることはできません。

経路ローミングの設定 (CLI)

- 次のコマンドを入力して、WLAN の 802.11k ネイバー リストを設定します。
config wlan assisted-roaming neighbor-list {enable | disable} wlan-id
- 次のコマンドを入力して、ネイバー フロア ラベル バイアスを設定します。
config assisted-roaming floor-bias dBm
- 次のコマンドを入力して、WLAN のデュアルバンド 802.11k ネイバー リストを設定します。
config wlan assisted-roaming dual-list {enable | disable} wlan-id



(注) デフォルトは、クライアントがアソシエートに使用している帯域です。

- 次のコマンドを入力して、WLAN の経路ローミング予測リスト機能を設定します。
config wlan assisted-roaming prediction {enable | disable} wlan-id



(注) ロード バランシングが WLAN に対してすでにイネーブルである場合、警告メッセージが表示され、ロード バランシングが WLAN に対してディセーブルになります。

- 次のコマンドを入力して、予測リスト機能の実行に必要な予測 AP の最小数を設定します。
config assisted-roaming prediction-minimum count



(注) クライアントに割り当てられた Forecast、AP が指定した数よりもこの値が小さい場合、経路ローミング機能はこのルールに適用されません。

- AP に送信されたアソシエーション要求が予測リストの AP に一致しない場合に、クライアントのアソシエーションを拒否できる最大回数を設定します。
config assisted-roaming denial-maximum count
- 次のコマンドを入力して、経路ローミング用にクライアントをデバッグします。
debug mac addr client-mac-addr
- 次のコマンドを入力して、すべての 802.11k イベントのデバッグを設定します。
debug 11k all {enable | disable}
- 次のコマンドを入力して、ネイバー詳細のデバッグを設定します。
debug 11k detail {enable | disable}
- 次のコマンドを入力して、802.11k エラーのデバッグを設定します。
debug 11k errors {enable | disable}
- 次のコマンドを入力して、ネイバー要求が受信されているかどうかを確認します。
debug 11k events {enable | disable}
- 次のコマンドを入力して、クライアントのローミング履歴のデバッグを設定します。
debug 11k history {enable | disable}

- 次のコマンドを入力して、802.11k 最適化のデバッグを設定します。
debug 11k optimization {enable | disable}
- 次のコマンドを入力して、オフラインシミュレーションで使用するためにインポートされるクライアント ローミング パラメータの詳細を取得します。
debug 11k simulation {enable | disable}



第 105 章

VLAN タギング 802.1Q-in-Q の設定

- [802.1Q-in-Q VLAN タギングの情報, 825 ページ](#)
- [802.1Q-in-Q VLAN タギングの制約事項, 826 ページ](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , 827 ページ](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , 828 ページ](#)

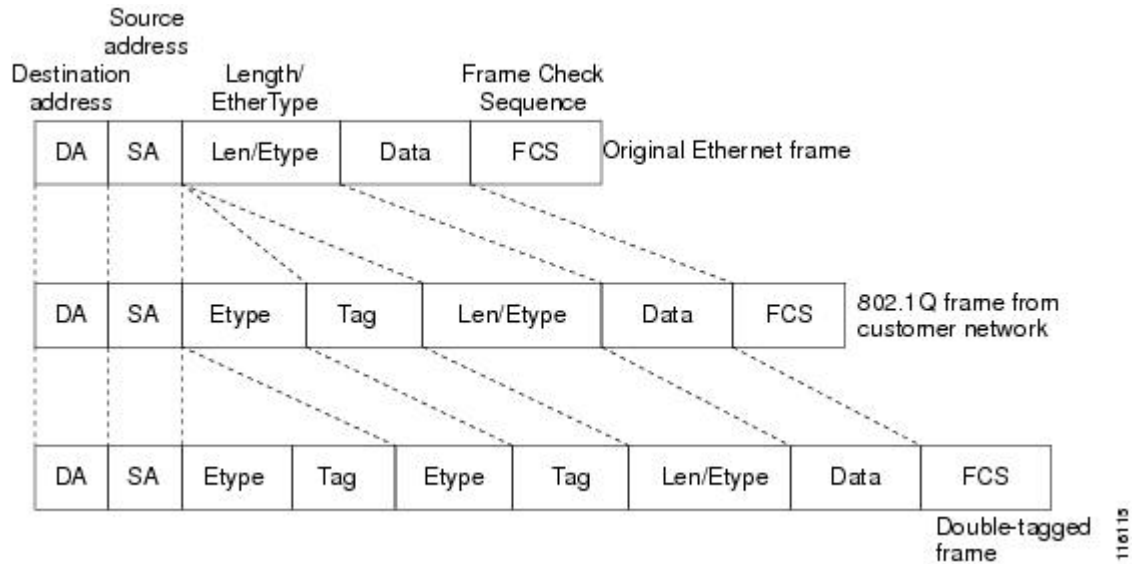
802.1Q-in-Q VLAN タギングの情報

クライアントごとに一意の VLAN ID 範囲を割り当てると、4096 VLAN という制限を超える可能性があります。802.1Q-in-Q VLAN タグ機能は、別の 802.1Q VLAN タグ内に 802.1Q VLAN タギングをカプセル化します。外部タグは AP グループに基づいて割り当てられ、内部 VLAN ID は AAA サーバによって動的に割り当てられます。

802.1Q-in-Q 機能を使用すれば、単一の VLAN で複数の VLAN をサポートできます。802.1Q-in-Q 機能では、VLAN ID を保存しながら、複数の VLAN のトラフィックを分離できます。下の図は、

タグなし、802.1Q タグ付き、および 802.1Q-in-Q タグ付きのイーサネット フレームを示しています。

図 51: タグなし、802.1Q タグ付き、および 802.1Q-in-Q タグ付きのイーサネットフレーム



関連トピック

- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)

802.1Q-in-Q VLAN タギングの制約事項

- 802.1Q-in-Q VLAN タギングは、Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco 8500 シリーズ ワイヤレス LAN コントローラ、および Cisco WiSM2 でのみサポートされます。
- IGMP スヌーピングを無効にするまで、マルチキャストは有効にできません。
- 802.1Q-in-Q VLAN タギングは、レイヤ 2 およびレイヤ 3 のコントローラ内ローミング、およびレイヤ 2 コントローラ間ローミングでのみサポートされます。レイヤ 3 コントローラ間ローミングはサポートされません。
- 0x8100 は、802.1Q-in-Q イーサネットフレームの [Ether Type] フィールドに対してのみサポートされている値です。

- 中央でスイッチされるパケットでのみ、802.1Q-in-Q VLAN タギングを有効にすることができます。
- 802.1Q-in-Q VLAN タギングについては、IPv6 DHCP パケットではなく、IPv4 DHCP パケットのみ有効にすることができます。
- tunnel-type である IETF 属性は、C-VLAN のオーバーライドに必要です。
- C-VLAN は tunnel-private-group-ID /tunnel-type および tunnel-private-group-id で設定できます。

関連トピック

- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(GUI\) , \(818 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの設定 \(CLI\) , \(819 ページ\)](#)

802.1Q-in-Q VLAN タギングの設定 (GUI)

-
- ステップ 1** [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。
 - ステップ 2** [AP Group Name] をクリックして、対応する [AP Groups > Edit] ページを開きます。
 - ステップ 3** [General] タブをクリックして、802.1Q-in-Q VLAN タギングの詳細を設定します。
 - ステップ 4** [Enable Client Traffic QinQ] チェックボックスをオンにして、AP グループの 802.1Q-in-Q VLAN タギングを有効にします。
 - ステップ 5** [Enable DHCPv4 QinQ] チェックボックスをオンにして、AP グループの IPv4 DHCP パケットの 802.1Q-in-Q VLAN タギングを有効にします。
 - ステップ 6** [QinQ Service VLAN ID] テキスト ボックスに、802.1Q-in-Q VLAN タギングの VLAN ID を入力します。
 - ステップ 7** [Apply] をクリックします。
-

関連トピック

- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)
- [802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)

802.1Q-in-Q VLAN タギングの設定 (CLI)

ステップ 1 次のコマンドを入力して、AP グループの 802.1Q-in-Q VLAN タギングを有効または無効にします。

```
config wlan apgroup qinq tagging client-traffic apgroup_name {enable| disable}
```

デフォルトでは、AP グループのクライアントトラフィックの 802.1Q-in-Q VLAN タギングは無効です。

ステップ 2 次のコマンドを入力して、AP グループのサービス VLAN を設定します。

```
config wlan apgroup qinq service-vlan apgroup_name vlan_id
```

ステップ 3 次のコマンドを入力して、AP グループのクライアントトラフィックの IPv4 DHCP パケットを有効または無効にします。

```
config wlan apgroup qinq tagging dhcp-v4 apgroup_name {enable| disable}
```

(注) DHCPv4 トラフィックの 802.1Q-in-Q タギングを有効にする前に、クライアントトラフィックの 802.1Q-in-Q タギングを有効にする必要があります。

デフォルトでは、AP グループの DHCPv4 トラフィックの 802.1Q-in-Q VLAN タギングは無効です。

ステップ 4 次のコマンドを入力して、AP グループの EAP for Global System for Mobile Communications (GSM) Subscriber Identity Module (EAP-SIM)、または EAP for Authentication and Key Agreement 認証クライアントトラフィックの 802.1Q-in-Q VLAN タギングを有効または無効にします。

```
config wlan apgroup qinq tagging eap-sim-aka apgroup_name {enable| disable}
```

クライアントトラフィックの 802.1Q-in-Q タギングを有効にすると、EAP for Authentication and Key Agreement (EAP-AKA) および EAP-SIM トラフィックの 802.1Q-in-Q タギングが有効になります。

ステップ 5 次のコマンドを入力して、802.1Q-in-Q VLAN タギングが有効かどうかを確認します。

```
show wlan apgroups
```

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..... 5

Site Name..... CT_builing1
Site Description..... APs for CT Building1
Venue Group Code..... Unspecified
Venue Type Code..... Unspecified

NAS-identifier..... CTB1
Client Traffic QinQ Enable..... TRUE
DHCPv4 QinQ Enable..... TRUE
AP Operating Class..... Not-configured
```

関連トピック

[802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)

[802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)

[802.1Q-in-Q VLAN タギングの情報, \(816 ページ\)](#)

[802.1Q-in-Q VLAN タギングの制約事項, \(817 ページ\)](#)



第 VI 部

Lightweight アクセス ポイントの制御

- [アクセス ポイント通信プロトコルの使用, 831 ページ](#)
- [CAPWAP の望ましいモード設定, 841 ページ](#)
- [アクセス ポイントの検索, 845 ページ](#)
- [アクセス ポイントのグローバル クレデンシヤルの設定, 853 ページ](#)
- [アクセス ポイントの認証の設定, 857 ページ](#)
- [組み込みアクセス ポイントの設定, 863 ページ](#)
- [自律アクセス ポイントの Lightweight モードへの変換, 867 ページ](#)
- [パケット キャプチャの設定, 893 ページ](#)
- [OfficeExtend アクセス ポイントの設定, 897 ページ](#)
- [設定の Cisco 700 シリーズ アクセス ポイント, 919 ページ](#)
- [Cisco ワークグループ ブリッジの使用, 921 ページ](#)
- [Cisco 以外のワークグループブリッジの使用, 929 ページ](#)
- [バックアップ コントローラの設定, 931 ページ](#)
- [アクセス ポイントのフェールオーバー プライオリティの設定, 937 ページ](#)
- [AP の再送信間隔および再試行回数の設定, 941 ページ](#)
- [Country Code の設定, 945 ページ](#)

- [アクセスポイントでの RFID トラッキングの最適化, 951 ページ](#)
- [プローブ要求フォワーディングの設定, 955 ページ](#)
- [コントローラとアクセスポイント上の一意のデバイス ID の取得, 957 ページ](#)
- [リンクテストの実行, 959 ページ](#)
- [リンク遅延の設定, 963 ページ](#)
- [TCP MSS の設定, 967 ページ](#)
- [Power over Ethernet の設定, 969 ページ](#)
- [クライアントの表示, 975 ページ](#)
- [アクセスポイントの LED 状態の設定, 979 ページ](#)
- [デュアルバンド無線によるアクセスポイントの設定, 983 ページ](#)
- [UDP Lite の設定, 985 ページ](#)
- [Cisco Hyperlocation, 989 ページ](#)
- [Cisco Air Time Fairness, 993 ページ](#)
- [Cisco Universal Small Cell 8x18 デュアルモード モジュール, 1001 ページ](#)



第 106 章

アクセス ポイント通信プロトコルの使用

- [アクセス ポイント通信プロトコルについて, 831 ページ](#)
- [アクセス ポイント通信プロトコルの制約事項, 832 ページ](#)
- [データ暗号化の設定, 832 ページ](#)
- [CAPWAP の最大伝送単位情報の表示, 836 ページ](#)
- [CAPWAP のデバッグ, 836 ページ](#)
- [コントローラ ディスカバリ プロセス, 837 ページ](#)
- [アクセス ポイントのコントローラへの join の確認, 838 ページ](#)

アクセス ポイント通信プロトコルについて

Cisco Lightweight アクセス ポイントは、IETF 標準 Control and Provisioning of Wireless Access Points Protocol (CAPWAP) を使用してネットワーク上のコントローラおよび他の Lightweight アクセス ポイントと通信します。

CAPWAP は LWAPP に基づく標準の互換プロトコルであり、コントローラによる無線アクセス ポイントの集合の管理を可能にします。CAPWAP は、次の理由でコントローラに実装されます。

- LWAPP を使用するシスコ製品に、CAPWAP を使用する次世代シスコ製品へのアップグレードパスを提供するため。
- RFID リーダーおよび類似のデバイスを管理するため。
- コントローラにサードパーティのアクセス ポイントとの将来的な互換性を持たせるため。

LWAPP を使用可能なアクセス ポイントは CAPWAP コントローラを検出して join することができ、CAPWAP コントローラへの変換はシームレスです。たとえば、CAPWAP 使用時のコントローラ ディスカバリ プロセスおよびファームウェア ダウンロードプロセスは、LWAPP 使用時のものと同じです。例外として、レイヤ 2 の展開は CAPWAP ではサポートされません。

CAPWAP コントローラおよび LWAPP コントローラは、同じネットワークで展開が可能です。CAPWAP を使用可能なソフトウェアでは、アクセス ポイントは CAPWAP を実行するコントローラでも LWAPP を実行するコントローラでも join できます。Cisco Aironet 1040、1140、1260、3500、および 3600 シリーズ アクセス ポイントは唯一の例外であり、これらは CAPWAP のみをサポートし、CAPWAP を実行するコントローラにのみ join します。たとえば、1130 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにも LWAPP を実行するコントローラにも join できますが、1140 シリーズ アクセス ポイントは CAPWAP を実行するコントローラにのみ join できます。

次に、アクセス ポイント通信プロトコルについて従う必要がある注意事項を示します。

- LWAPP を使用するアクセス ポイントからのトラフィックのみ許可するようファイアウォールが設定されている場合は、ファイアウォールのルールを変更して CAPWAP を使用するアクセス ポイントからのトラフィックを許可する必要があります。
- CAPWAP UDP ポート 5246 および 5247 (LWAPP UDP ポート 12222 および 12223 と同等のポート) が有効になっており、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- アクセス コントロール リスト (ACL) がコントローラとアクセス ポイントの間の制御パスにある場合は、新しいプロトコル ポートを開いてアクセス ポイントが孤立しないようにする必要があります。

アクセス ポイント通信プロトコルの制約事項

- 仮想コントローラ プラットフォームでは、クライアントごとのダウンストリーム レート制限は FlexConnect 中央スイッチングでサポートされません。
- レート制限は、どの方向からでも CPU 宛てのすべてのトラフィックに適用されます (無線または有線)。コントローラにトラフィックをレート制限するデフォルトの **config advanced rate enable** コマンドでコントローラが常に実行し、サービス拒絶 (DoS) 攻撃から保護することを推奨します。Internet Control Message Protocol (ICMP) エコー応答のレート制限をテスト目的で停止する **config advanced rate disable** コマンドを使用できます。ただしテスト完了後、**config advanced rate enable** コマンドを再適用することを推奨します。
- コントローラが適切な日時で設定されていることを確認してください。コントローラに設定されている日時がアクセス ポイントの証明書の作成日とインストール日に先行すると、アクセス ポイントはコントローラに join しません。

データ暗号化の設定

Cisco 5500 シリーズ コントローラにより、データグラム トランスポート層セキュリティ (DTLS) を使用してアクセス ポイントとコントローラの間で送信される CAPWAP コントロール パケット (および、オプションとして CAPWAP データ パケット) の暗号化が可能です。DTLS は、標準化過程にある TLS に基づくインターネット技術特別調査委員会 (IETF) プロトコルです。CAPWAP コントロール パケットとはコントローラとアクセス ポイントの間で交換される管理パケットであ

り、CAPWAP データ パケットは転送された無線フレームをカプセル化します。CAPWAP コントロールおよびデータ パケットはそれぞれ異なる UDP ポートである 5246 (コントロール) および 5247 (データ) で送信されます。アクセス ポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロールプレーンにのみ有効となり、データ プレーンの DTLS セッションは確立されません。

データ暗号化のためのガイドライン

- Cisco 1130 および 1240 シリーズのアクセス ポイントはソフトウェアベースの暗号化で DTLS データ暗号化をサポートしています。
- Cisco 1040、1140、1250、1260、1530、1550、1600、2600、3500、および 3600 シリーズのアクセス ポイントはハードウェアベースの暗号化で DTLS データ暗号化をサポートしています。
- Cisco Aironet 1552 および 1522 屋外アクセス ポイントはデータ DTLS をサポートしています。
- DTLS データ暗号化は、Cisco Aironet 700 シリーズ アクセス ポイントではサポートされていません。
- DTLS データ暗号化は OfficeExtend アクセス ポイントに対しては自動的に有効になりますが、他のすべてのアクセス ポイントに対してはデフォルトで無効になります。ほとんどのアクセス ポイントは会社のビルディング内の安全なネットワークにおいて展開されるため、データの暗号化は必要ありません。反対に、OfficeExtend アクセス ポイントとコントローラの間トラフィックは安全でないパブリック ネットワークを経由するため、これらのアクセス ポイントではデータの暗号化はより重要です。データの暗号化が有効な場合、トラフィックはアクセス ポイントで暗号化されてからコントローラに送信され、また、コントローラで暗号化されてからクライアントに送信されます。
- 暗号化はコントローラおよびアクセス ポイントの両方においてスループットを制限するため、多くのエンタープライズ ネットワークにおいて最大スループットが必要です。
- シスコのユニファイド ローカル ワイヤレス ネットワーク 環境では、Cisco 1130 および 1240 アクセス ポイントで DTLS を有効にしないでください。有効にすると、重大なスループットの低下が発生し、AP が使用できなくなるおそれがあります。

OfficeExtend アクセス ポイントの詳細は、『OfficeExtend Access Points』を参照してください。

- コントローラを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効化または無効化できます。
- データ DTLS のアベイラビリティは次のとおりです。
 - Cisco 5500 シリーズ コントローラは、2 個のライセンスのオプションで使用可能です。ライセンスおよびデータ DTLS を使用するのにライセンスを必要とする他のイメージなしでデータ DTLS を使用可能にします。「[Cisco 5500 シリーズ コントローラ用 DTLS イメージのアップグレードまたはダウングレード](#)」の項を参照してください。DTLS のイメージとライセンス付き DTLS のイメージは、次のとおりです。

ライセンス付きの DTLS : AS_5500_LDPE_x_x_x_x.aes

ライセンスなしの DTLS—AS_5500_x_x_x_x.aes

- ° Cisco 2500、Cisco WiSM2、Cisco 仮想ワイヤレス コントローラ：デフォルトでは、これらのプラットフォームに DTLS は含まれていません。データ DTLS をオンにするには、ライセンスをインストールする必要があります。これらのプラットフォームには、データ DTLS を無効にした 1 つのイメージがあります。データ DTLS を使用するには、ライセンスが必要です。

データ DTLS が含まれていない Cisco 仮想ワイヤレス コントローラの場合、コントローラの平均スループットは約 200 Mbps です。データ DTLS を使用するすべての AP を使用すると、コントローラの平均スループットは約 100 Mbps になります。

- コントローラにデータ DTLS のライセンスがなく、コントローラに関連付けられているアクセス ポイントで DTLS が有効になっている場合、データ パスは暗号化されません。
- Cisco 5508 シリーズ コントローラを使用しているロシア以外のお客様はデータ DTLS ライセンスを必要としません。ただし、Cisco 2500 シリーズ コントローラ、Cisco 8500 シリーズ コントローラ、WiSM2 および Cisco 仮想ワイヤレス コントローラを使用しているすべてのお客様は、データ DTLS 機能をオンにするためにデータ DTLS ライセンスが必要です。

Cisco 5500 シリーズ コントローラ用 DTLS イメージのアップグレードまたはダウングレード

ステップ 1 アップグレード操作は、最初の試みで失敗し、警告はライセンス付きの DTLS イメージへのアップグレードを行うと元に戻せないことを示します。

(注) ステップ 1 の後にコントローラをリブートしないでください。

ステップ 2 次のアップデートでは、ライセンスが適用され、イメージが正常に更新します。

DTLS イメージへまたは DTLS イメージからのアップグレード時のガイドライン

- ライセンス付きのデータ DTLS イメージがインストールされると、通常のイメージ（ライセンスなしのデータ DTLS）をインストールできません。
- ライセンス付き DTLS イメージから別のライセンス付き DTLS イメージにアップグレードできます。
- 通常のイメージ（DTLS）からライセンス付きの DTLS イメージへのアップグレードは、2 ステップ プロセスで行います。
- **show sysinfo** コマンドを使用して、イメージのアップグレードの前後に LDPE イメージを確認できます。

データ暗号化の設定（GUI）

Cisco 5500 シリーズコントローラに基本ライセンスがインストールされていることを確認します。ライセンスがインストールされると、アクセスポイントのデータ暗号化を有効化できます。

-
- ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
 - ステップ 2 暗号化を有効にするアクセスポイントの名前をクリックします。
 - ステップ 3 [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。
 - ステップ 4 このアクセスポイントでデータ暗号化を有効にする場合は [Data Encryption] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。デフォルト値はオフです。
(注) データ暗号化モードに変更するには、アクセスポイントをコントローラに再 join する必要があります。
 - ステップ 5 [Apply] をクリックします。
 - ステップ 6 [Save Configuration] をクリックします。
-

データ暗号化の設定（CLI）



(注) DTLS ライセンスのないイメージでは、**config** または **show** コマンドは使用できません。

コントローラの CLI を使用してコントローラ上のアクセスポイントの DTLS データ暗号化を有効にする手順は、次のとおりです。

-
- ステップ 1 次のコマンドを入力して、すべてのアクセスポイントまたは特定のアクセスポイントのデータ暗号化を有効または無効にします。
config ap link-encryption {enable | disable} {all | Cisco_AP}
デフォルト値はディセーブルです。
(注) データ暗号化モードに変更するには、アクセスポイントをコントローラに再 join する必要があります。
 - ステップ 2 アクセスポイントおよび接続しているクライアントの切断を確認するよう求めるプロンプトが表示されたら、**Y** と入力します。
 - ステップ 3 **save config** コマンドを入力して、設定を保存します。
 - ステップ 4 次のコマンドを入力して、すべてのアクセスポイントまたは特定のアクセスポイントの暗号化状態を表示します。
show ap link-encryption {all | Cisco_AP}

このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセスポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。

ステップ 5 すべてのアクティブな DTLS 接続の概要を表示するには、次のコマンドを入力します。

show dtls connections

(注) DTLS データ暗号化に問題が生じた場合は、**debug dtls {all|event|trace|packet} {enable|disable}** コマンドを入力して、すべての DTLS メッセージ、イベント、トレース、またはパケットをデバッグします。

CAPWAP の最大伝送単位情報の表示

コントローラ上の CAPWAP パスの最大伝送単位 (MTU) を表示するには、次のコマンドを入力します。

show ap config general Cisco_AP

MTU は、送信されるパケットの最大サイズ (バイト) を指定します。

以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 9
Cisco AP Name..... Maria-1250
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A      802.11a:-A
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A      802.11a:-A
Switch Port Number ..... 1
MAC Address..... 00:1f:ca:bd:bc:7c
IP Address Configuration..... DHCP
IP Address..... 1.100.163.193
IP NetMask..... 255.255.255.0
CAPWAP Path MTU..... 1485
```

CAPWAP のデバッグ

次のコマンドを使用して、CAPWAP デバッグ情報を取得します。

- **debug capwap events {enable|disable}** : CAPWAP イベントのデバッグを有効または無効にします。
- **debug capwap errors {enable|disable}** : CAPWAP エラーのデバッグを有効または無効にします。
- **debug capwap detail {enable|disable}** : CAPWAP の詳細のデバッグを有効または無効にします。
- **debug capwap info {enable|disable}** : CAPWAP 情報のデバッグを有効または無効にします。
- **debug capwap packet {enable|disable}** : CAPWAP パケットのデバッグを有効または無効にします。

- **debug capwap payload {enable | disable}** : CAPWAP ペイロードのデバッグを有効または無効にします。
- **debug capwap hexdump {enable | disable}** : CAPWAP 16 進数ダンプのデバッグを有効または無効にします。
- **debug capwap dtls-keepalive {enable | disable}** : CAPWAP DTLS データ キープアライブ パケットのデバッグを有効または無効にします。

コントローラ ディスカバリ プロセス

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してコントローラを検知してから、コントローラに CAPWAP join request を送信します。これに対し、コントローラはアクセス ポイントに CAPWAP join response を返し、アクセス ポイントはコントローラに join できるようになります。アクセス ポイントがコントローラに join すると、コントローラによってアクセス ポイントの構成、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

次に、コントローラ ディスカバリ プロセスの注意事項を示します。

- LWAPP から CAPWAP へのアップグレードパスおよび CAPWAP から LWAPP へのダウングレードパスがサポートされます。LWAPP イメージを持つアクセス ポイントは、LWAPP で ディスカバリ プロセスを開始します。LWAPP コントローラを検出すると、LWAPP ディスカバリ プロセスを開始してコントローラに join します。LWAPP コントローラが見つからない場合は、CAPWAP で ディスカバリ を開始します。1 つの ディスカバリ タイプ (CAPWAP または LWAPP) で ディスカバリ プロセスを開始した回数が最大 ディスカバリ カウントを超えてもアクセス ポイントが discovery response を受信しない場合は、ディスカバリ タイプはもう一方のタイプに変更されます。たとえば、アクセス ポイントが LWAPP でコントローラを検出できない場合、CAPWAP で ディスカバリ プロセスを開始します。
- アクセス ポイントが UP 状態であり、IP アドレスが変更される場合は、既存の CAPWAP トンネルを解除してコントローラに再 join します。
- コントローラが CAPWAP discovery response で送信する IP アドレスを設定するには、**config network ap-discovery nat-ip-only {enable | disable}** コマンドを使用します。
- アクセス ポイントをネットワークでアクティブにするには、コントローラがそのアクセス ポイントを検出する必要があります。Lightweight アクセス ポイントでは、次のコントローラ ディスカバリのプロセスがサポートされています。
 - Layer 3 CAPWAP または LWAPP ディスカバリ : この機能は、アクセス ポイントとは異なるサブネット上で有効化され、レイヤ 2 ディスカバリで使用される MAC アドレスではなく IP アドレスと UDP パケットが使用されます。
 - ローカルに保存されているコントローラの IP アドレス ディスカバリ : アクセス ポイントがすでにコントローラにアソシエートされている場合、プライマリ、セカンダリ、およびターシャリ コントローラの IP アドレスはアクセス ポイントの不揮発性メモリに保存されます。今後の展開用にアクセス ポイントにコントローラの IP アドレスを保存するこのプロセスは、「アクセス ポイントのプライミング」と呼ばれます。

- DHCP サーバの検出：この機能では、DHCP オプション 43 を使用してアクセスポイントにコントローラの IP アドレスを割り当てます。Cisco スイッチでは、通常この機能に使用される DHCP サーバ オプションをサポートしています。DHCP オプション 43 の詳細については、「[DHCP オプション 43 および DHCP オプション 60 の使用](#)」の項を参照してください。
- DNS の検出：アクセスポイントでは、ドメインネームサーバ (DNS) を介してコントローラを検出できます。CISCO-LWAPP-CONTROLLER.localdomain または CISCO-CAPWAP-CONTROLLER.localdomain への応答としてコントローラの IP アドレスを返すよう、DNS を設定する必要があります。ここで、localdomain はアクセスポイントドメイン名です。アクセスポイントは、DHCP サーバから IP アドレスと DNS の情報を受信すると、DNS に接続して CISCO-LWAPP-CONTROLLER.localdomain または CISCO-CAPWAP-CONTROLLER.localdomain を解決します。DNS からコントローラの IP アドレスのリストを受信すると、アクセスポイントはコントローラに discovery request を送信します。

コントローラ ディスカバリ プロセスの制約事項

- ディスカバリ プロセスでは、1040、1140、1260、3500、および 3600 シリーズ アクセスポイントはシスコの CAPWAP コントローラのみをクエリーします。LWAPP コントローラに関するクエリーは送信されません。これらのアクセスポイントで LWAPP と CAPWAP コントローラの両方に対するクエリーを送信する場合は、DNS を更新する必要があります。
- コントローラが現在の時刻に設定されていることを確認してください。コントローラをすでに経過した時刻に設定すると、その時刻には証明書が無効である可能性があり、アクセスポイントがコントローラに join できない場合があります。

アクセスポイントのコントローラへの join の確認

コントローラを交換する場合、アクセスポイントが新しいコントローラに join していることを確認する必要があります。

アクセスポイントのコントローラへの join の確認 (GUI)

ステップ 1 次の手順で、新しいコントローラをマスター コントローラとして設定します。

- a) [Controller] > [Advanced] > [Master Controller Mode] の順に選択し、[Master Controller Configuration] ページを開きます。
- b) [Master Controller Mode] チェックボックスをオンにします。
- c) [Apply] をクリックして、変更を確定します。

d) [Save Configuration] をクリックして、変更を保存します。

- ステップ 2** (任意) ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。
- ステップ 3** アクセス ポイントを再起動します。
- ステップ 4** すべてのアクセス ポイントが新しいコントローラに join した後で、そのコントローラがマスター コントローラとして機能しないように設定するには、[Master Controller Configuration] ページで [Master Controller Mode] チェックボックスをオフにします。
-

アクセス ポイントのコントローラへの join の確認 (CLI)

- ステップ 1** 次のコマンドを入力して、新しいコントローラをマスター コントローラとして設定します。
config network master-base enable
- ステップ 2** (任意) ネットワーク インフラストラクチャ内の ARP アドレス テーブルおよび MAC アドレス テーブルを消去します。
- ステップ 3** アクセス ポイントを再起動します。
- ステップ 4** 次のコマンドを入力して、すべてのアクセス ポイントが新しいコントローラに join した後で、そのコントローラがマスター コントローラとして機能しないように設定します。
config network master-base disable
-



第 107 章

CAPWAP の望ましいモード設定

- [優先モードについて](#), 841 ページ
- [優先モードの設定のガイドライン](#), 841 ページ
- [CAPWAP 設定の望ましいモード \(GUI\)](#), 842 ページ
- [CAPWAP 設定の望ましいモード \(CLI\)](#), 843 ページ

優先モードについて

優先モードでは、アクセスポイントが WLC に join するときに使用する CAPWAP L3 トランスポート (IPv4 と IPv6) を (プライマリ/セカンダリ/ターシャリ設定に基づいて) 管理者が設定できます。

優先モードには次の 2 つのレベルがあります。

- AP グループ別
- グローバル設定

AP PnP

PnP ソリューションは AP が WLC に参加する前にステージングパラメータを提供します。このステージング設定を使用して、AP は WLC に参加するときにランタイム設定を取得します。PnP は AP のリカバリイメージのみがサポートしており、ゼロデイ展開だけのためにアクティブ化されます。PnP は AP が WLC に初めて接続した後では初期化されません。

以下の AP シナリオをサポートしています。

- オンプレミスリダイレクション: ネットワークで PnP サーバをホストしている顧客。

優先モードの設定のガイドライン

次の優先モードの設定を使用できます。

- AP グループ特有の有線モードは、AP グループの有線モードが設定されており、AP がそのグループに属している場合のみ、AP に適用されます。
- グローバル優先モードは、デフォルトグループの AP、および優先モードが設定されていない AP グループに適用されます。
- デフォルトでは、AP グループの優先モードの値は設定されず、グローバルの優先モードの値は IPv4 に設定されます。
- 優先モードが設定されている AP がコントローラに join しようとして失敗すると、他のトランスポートの AP マネージャの選択に戻り、同じコントローラに join します。両方のトランスポートが失敗すると、AP は次のディスカバリ応答に移動します。
- このようなシナリオでは、スタティック IP の設定は、優先モードよりも優先されます。次に例を示します。
 - コントローラでは、優先モードは IPv4 アドレスで設定されます。
 - AP では、スタティック IPv6 は CLI または GUI を使用して設定されます。
 - AP は、IPv6 トランスポートモードを使用してコントローラに join します。
- コントローラ CLI は、優先モードの XML サポートを提供します。

CAPWAP 設定の望ましいモード (GUI)

- ステップ 1** [Controller] > [General] を選択して、[Global Configuration] ページを開きます。[CAPWAP Preferred Mode] リストボックスを選択し、グローバルな CAPWAP 優先モードとして、IPv4 または IPv6 のどちらかを選択します。
- (注) デフォルトでは、コントローラは CAPWAP 優先モード IPv4 アドレスで設定されます。
- ステップ 2** [WLAN] > [Advanced] > [APGroup] > [General] タブの順に選択し、[CAPWAP Preferred Mode] チェックボックスをオンにして、IPv4 または IPv6 CAPWAP 優先モードで AP グループを設定します。
- ステップ 3** [Wireless] > [ALL APs] > [General] タブの順に選択して、APs CAPWAP の設定をチェックします。AP の CAPWAP 優先モードが全体的にまたは AP グループに適用されているかどうかを確認するには、[IP Config] セクションを参照してください。
- ステップ 4** [Monitor] > [Statistics] > [Preferred Mode] の順に選択して、ユーザが、優先モードコマンドが正常に AP にプッシュされたかどうかをチェックできるようにします。
- [Prefer Mode of Global/AP Groups] : IPv4、IPv6、またはグローバルで設定した AP の名前。
 - [Total] : 優先モードで設定された AP の総数。
 - [Success] : AP が優先モードで正常に設定された回数をカウントします。
 - [Unsupporte] : IPv6 CAPWAP で join できない AP。
 - [Already Configured] : すでに設定済みの AP を設定しようとした試行回数をカウントします。

- [Per AP Group Configured] : AP グループごとに設定された優先モード。
- [Failure] : AP が優先モード設定に失敗した回数をカウントします。

CAPWAP 設定の望ましいモード (CLI)

ステップ 1 次のコマンドを使用して、AP グループおよびすべての AP の優先モードを設定します。グローバルな優先モードは、AP グループの優先モードがすでに設定されている AP には適用されません。設定が正常終了すると、AP は CAPWAP を再起動して、プライマリ/セカンダリ/ターシャリ設定に基づいてコントローラを選択した後、設定された優先モードで join します。

```
config ap preferred-mode{IPv4|IPv6}{<apgroup>|<all>}
```

ステップ 2 (設定解除する) AP の優先モードをディセーブルにするには、このコマンドを使用します。

```
config ap preferred-mode disable<apgroup>
```

(注) <apgroup> に属する AP は CAPWAP を再起動し、グローバルな優先モードでコントローラに再 join します。

ステップ 3 次のコマンドを使用して、優先モード設定の統計情報を表示します。統計情報は累積されませんが、最後に実行された優先モードの設定 CLI に対して更新されます。

```
show ap prefer-mode stats
```

ステップ 4 次のコマンドを使用して、すべての AP グループ用に設定された優先モードを表示します。

```
show wlan apgroups
```

ステップ 5 次のコマンドを使用して、設定されているグローバルな優先モードを表示します。

```
show network summary
```

ステップ 6 次のコマンドを使用して、AP にプッシュされる優先モードコマンドがグローバルコンフィギュレーションからなのか、AP グループ固有の設定からなのかを表示して確認します。

```
show ap config general <Cisco AP>
```

```
(Cisco Controller) >show ap config general AP-3702E
```

```
Cisco AP Identifier..... 2
Cisco AP Name..... AP-3702E
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-A 802.11a:-A
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-A
Switch Port Number ..... 1
MAC Address..... bc:16:65:09:4e:fc
IPv6 Address Configuration..... SLAAC
IPv6 Address..... 2001:9:2:35:be16:65ff:fe09:4efc
IPv6 Prefix Length..... 64
Gateway IPv6 Addr..... fe80::a2cf:5bff:fe51:c4ce
NAT External IP Address..... None
CAPWAP Path MTU..... 1473
Telnet State..... Globally Enabled
```

```
Ssh State..... Globally Enabled
Cisco AP Location..... default location
Cisco AP Floor Label..... 0
Cisco AP Group Name..... default-group
Primary Cisco Switch Name..... amb
Primary Cisco Switch IP Address..... 9.2.35.25
.....
.....
.....
.....
.....
Ethernet Port Speed..... Auto
AP Link Latency..... Disabled
Rogue Detection..... Enabled
AP TCP MSS Adjust..... Disabled
IPv6 Capwap UDP Lite..... Enabled
Capwap Prefer Mode..... Ipv6 (Global Config)
Hotspot Venue Group..... Unspecified
Hotspot Venue Type..... Unspecified
DNS server IP ..... Not Available
```

(注) コマンド出力の **Capwap Prefer Mode** をチェックします。



第 108 章

アクセスポイントの検索

- [アクセスポイントの検索について, 845 ページ](#)
- [APフィルタの検索 \(GUI\) , 845 ページ](#)
- [インターフェイスの詳細の監視, 848 ページ](#)
- [アクセスポイント無線の検索, 850 ページ](#)

アクセスポイントの検索について

[All APs] ページのアクセスポイントのリストで、特定のアクセスポイントを検索できます。検索を実行するには、特定の基準（MACアドレス、ステータス、アクセスポイントモード、および証明書タイプなど）を満たすアクセスポイントのみを表示するフィルタを作成します。この機能は、アクセスポイントのリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。

AP フィルタの検索 (GUI)

ステップ 1 [Monitor] > [Access Point Summary] > [All APs] > [Details] の順に選択して、[All APs] ページを開きます。このページには、コントローラに join しているすべてのアクセスポイントが表示されます。アクセスポイントそれぞれについて、名前、MACアドレス、稼働時間、ステータス、動作モード、証明書、OfficeExtend アクセスポイントステータス、およびアクセスポイントサブモードを確認できます。

ページの右上部には、アクセスポイントの合計数が表示されます。アクセスポイントのリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページにアクセスできます。各ページには最大 20 台のアクセスポイントを表示できます。

ステップ 2 [Change Filter] をクリックして、[Search AP] ダイアログボックスを開きます。

ステップ 3 次のチェックボックスの1つまたは複数をおんにして、アクセスポイントを表示する際に使用する基準を指定します。

- [MAC Address] : アクセス ポイントの MAC アドレス。
 - (注) [MAC Address] フィルタを有効にすると、その他のフィルタは自動的に無効になります。その他のフィルタのいずれかを有効にすると、[MAC Address] フィルタは自動的に無効になります。
 - [AP Name] : アクセス ポイントの名前を入力します。
 - [AP Model] : アクセス ポイントのモデル名を入力します。
 - [Operating Status] : 次のチェックボックスの 1 つまたは複数をおんにして、アクセス ポイントの動作ステータスを指定します。
 - [UP] : アクセス ポイントは稼働中です。
 - [DOWN] : アクセス ポイントは動作していません。
 - [REG] : アクセス ポイントはコントローラに登録されています。
 - [DEREG] : アクセス ポイントはコントローラに登録されていません。
 - [DOWNLOAD] : コントローラはそのソフトウェア イメージをアクセス ポイントにダウンロードしています。
 - [Port Number] : アクセス ポイントを接続するコントローラのポート番号を入力します。
 - [Admin Status] : [Enabled] または [Disabled] を選択して、コントローラ上でアクセス ポイントを有効にするか無効にするかを指定します。
 - [AP Mode] : 次のオプションの 1 つまたは複数をおんにして、アクセス ポイントの動作モードを指定します。
 - [Local] : デフォルト オプション。
 - (注) 600 OEAP シリーズ アクセス ポイントでは、ローカル モードのみ使用します。
 - ローカル モードのアクセス ポイントが Cisco Flex 7500 シリーズ コントローラに接続している場合、そのアクセス ポイントはクライアントにサービスを提供しません。アクセス ポイントの詳細はコントローラで使用できます。アクセス ポイントが Cisco Flex 7500 シリーズ コントローラに接続しているときに、クライアントにサービスを提供できる、またはモニタ関連のタスクを実行できるようにするには、アクセス ポイントのモードを FlexConnect モードまたは監視モードにします。コントローラの `join` でアクセス ポイントを Join FlexConnect モードまたはモニタ モードに自動的に変換するには、次のコマンドを使用します。
- ```
config ap autoconvert {flexconnect | monitor | disable}
```
- コントローラに接続するすべてのアクセス ポイントは、指定した設定によって FlexConnect モードまたは監視モードに変換されます。
- [FlexConnect] : このモードは、1040、1130、1140、1240、1250、1260、1600、2600、3500、3600、および 800 アクセス ポイントで使用されます。
  - [REAP] : このモードは、リモート エッジ Lightweight アクセス ポイントです。

- [Monitor] : このモードは、モニタリング専用モードです。
- [Rogue Detector] : このモードは、有線の不正 AP をモニタします。無線ではフレームを送受信せず、不正 AP は含まれません。
  - (注) 検出された不正に関する情報は、コントローラ間で共有されません。したがって、Rogue Detector AP を使用する場合は、それぞれのコントローラで独自に接続した Rogue Detector AP を使用することをお勧めします。
- [Sniffer] : アクセスポイントは、所定のチャンネルで無線のスニファを開始します。アクセスポイントは、そのチャンネル上のクライアントからのすべてのパケットを取得し、AiroPeek または Wireshark (IEEE 802.11 無線 LAN のパケットアナライザ) を実行するリモートマシンに転送します。これには、タイムスタンプ、信号強度、パケットサイズなどの情報が含まれます。
  - (注) このブリッジオプションは、AP がブリッジ対応の場合のみ表示されます。
  - (注) AP モードが「ブリッジ」に設定され、AP が REAP 対応でない場合、エラーが表示されます。
- [Bridge] : このモードでは、Root AP を接続している場合、AP モードを「ブリッジ」に設定します。
- [SE-Connect] : このモードでは、Spectrum Expert への接続を可能にして、アクセスポイントがスペクトラムインテリジェンスを実行できるようにします。
  - (注) AP3500 および AP3600 はスペクトルインテリジェンスをサポートしますが、AP1260 はスペクトルインテリジェンスをサポートしません。
  - (注) アクセスポイントは、SE-Connect モードに設定されると、リブートしてコントローラに再joinします。このモードに設定されたアクセスポイントは、クライアントにサービスを提供しません。
- **Flex+Bridge** : スタンドアロンモードのサポートは、AP がこのモードである場合に適用されません。
- [Certificate Type] : 次のチェックボックスの 1 つまたは複数をおんにして、アクセスポイントにインストールされる証明書のタイプを指定します。
  - [MIC] : Manufactured-Installed Certificate (製造元でインストールされる証明書)
  - [SSC] : Self-Signed Certificate (自己署名証明書)
  - [LSC] : Local Significant Certificate (ローカルで有効な証明書)
    - (注) 証明書のタイプの詳細については、「[アクセスポイントの許可](#)」の項を参照してください。
- [Primary S/W Version] : このチェックボックスをおんにして、プライマリソフトウェアバージョン番号を入力します。
- [Backup S/W Version] : このチェックボックスをおんにして、セカンダリソフトウェアバージョン番号を入力します。

ステップ 4 [Apply] をクリックします。

検索基準に一致するアクセスポイントのみが [All APs] ページに表示され、ページ上部の [Current Filter] パラメータはリストを生成するのに使用したフィルタを示します（たとえば、MAC Address:00:1d:e5:54:0e:e6、AP Name:pmsk-ap、Operational Status: UP、Status: Enabled など）

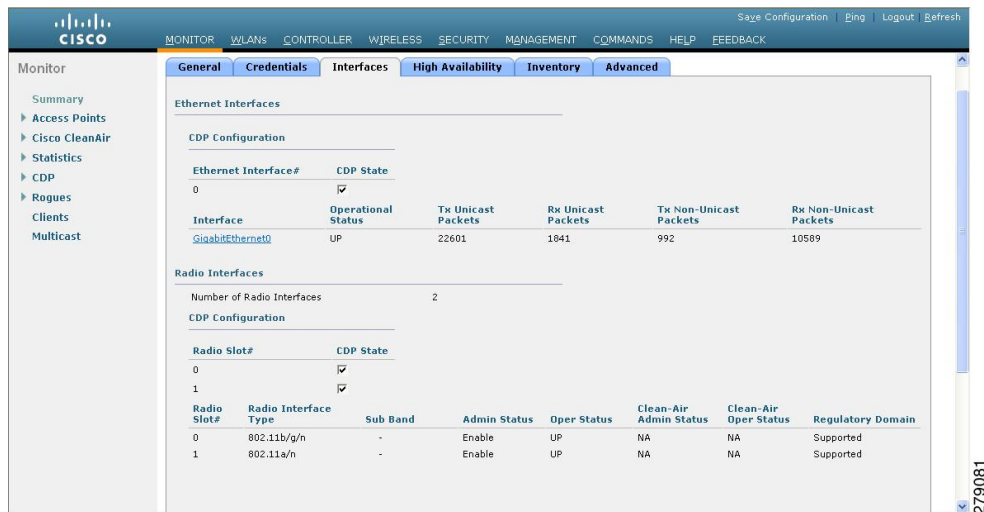
(注) フィルタを削除してアクセスポイントリスト全体を表示するには、[Clear Filter] をクリックします。

## インターフェイスの詳細の監視

ステップ 1 [Monitor] > [Summary] > [All APs] の順に選択します。 [All APs > Details] ページが表示されます。

ステップ 2 [Interfaces] タブをクリックします。

図 52 : [Interfaces] タブ



ステップ 3 使用可能なインターフェイス名をクリックします。 [Interface Details] ページが表示されます。

ステップ 4 [Interface Details] ページには、次のパラメータの詳細が表示されます。

表 22 : インターフェイス パラメータの詳細

ボタン	説明
AP Name	アクセスポイントの名前。
Link Speed	干渉の速度（Mbps 単位）。

ボタン	説明
RX Bytes	インターフェイス上で受信したエラーのないパケットの総バイト数。
RX Unicast Packets	インターフェイスで受信されたユニキャストパケットの合計数。
RX Non-Unicast Packets	インターフェイスで受信された非ユニキャストまたはマルチキャストパケットの総数。
Input CRC	インターフェイス上で受信したパケット内のCRCエラーの総数。
Input Errors	インターフェイスでの受信中に発生した、パケットのすべてのエラーの合計。
Input Overrun	入力レートが、受信者側のデータ処理能力を超えていたため、受信者側のハードウェアでハードウェアバッファに受信したデータを処理できなかった回数。
Input Resource	インターフェイス上で受信したパケット内のリソースエラーの総数。
Runts	メディアの最小パケットサイズと同様であるために、破棄されたパケットの数。
Throttle	インターフェイスが、送信中のパケットが多すぎるため、配信速度を落とすように、送信NICにアドバイスを送信した合計回数。
Output Collision	イーサネットコリジョンにより再送信したパケットの総数。
Output Resource	インターフェイスで送信されたパケットのリソースエラー。
Output Errors	最終的にインターフェイスからのパケットの送信ができなかった原因となるエラー。
Operational Status	AP上の物理イーサネットインターフェイスの動作ステート。
Duplex	インターフェイスのデュプレックスモード。
TX Bytes	インターフェイスで送信されたエラーのないパケットのバイト数。
TX Unicast Packets	インターフェイスで送信されたユニキャストパケットの合計数。
TX Non-Unicast Packets	インターフェイスで送信された非ユニキャストまたはマルチキャストパケットの総数。
Input Aborts	インターフェイス上で受信中に中断されたパケットの総数。
Input Frames	CRCエラーがあり、オクテット数が整数でなかったため、インターフェイスで正常に受信されなかったパケットの合計数。

ボタン	説明
Input Drops	インターフェイス上での受信中に、キューが一杯だったためにドロップされたパケットの総数。
Unknown Protocol	不明なプロトコルによってインターフェイスで破棄されたパケットの合計数。
Giants	メディアの最大パケットサイズを超えたために、破棄されたパケットの数。
Interface Resets	インターフェイスが完全にリセットされた回数。
Output No Buffer	バッファ容量がないために破棄されたパケットの合計数。
Output Underrun	ルータの処理能力を超えた速度でトランスミッタが動作した回数。
Output Total Drops	インターフェイスからの送信中に、キューが一杯だったためにドロップされたパケットの総数。

## アクセスポイント無線の検索

### アクセスポイント無線の検索について

[802.11a/n/ac Radios] ページまたは [802.11b/g/n Radios] ページの無線のリストで、特定のアクセスポイント無線を検索できます。アクセスポイント無線を表示するときは、メニューバーの [Monitor] タブから、またはアクセスポイント無線を設定するときはメニューバーの [Wireless] タブからこれらのページにアクセスできます。特定のアクセスポイント無線を検索するには、特定の基準（無線 MAC アドレス、アクセスポイント名、CleanAir ステータスなど）を満たす無線だけを表示するためのフィルタを作成します。この機能は、アクセスポイント無線のリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。

### アクセスポイント無線の検索（GUI）

**ステップ 1** 次のいずれかを実行します。

- [Monitor] > [Access Points Summary] > [802.11a/n/ac（または 802.11b/g/n）> Radios] > [Details] を選択して、[802.11a/n/ac（または 802.11b/g/n）Radios] ページを開きます。



- [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac (または 802.11b/g/n)] と選択して、[802.11a/n/ac (または 802.11b/g/n) Radios] ページを開きます。

このページには、コントローラに join しているすべての 802.11a/n/ac または 802.11b/g/n アクセスポイント無線とその現在の設定が表示されます。

ページの右上部には、アクセスポイント無線の合計数が表示されます。無線のリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページにアクセスできます。各ページには最大 25 台のアクセスポイント無線を表示できます。

- (注) Cisco Unified Wireless Network 環境では、802.11a/n/ac および 802.11b/g/n 無線は、同じアドレスを持つ可能性があるため、Base Radio MAC アドレスに基づいて区別するべきではありません。代わりに、物理アドレスに基づいて区別してください。

**ステップ 2** [Change Filter] をクリックして、[Search AP] ダイアログボックスを開きます。

**ステップ 3** 次のチェックボックスのいずれかをオンにして、アクセスポイント無線を表示する際に使用する基準を指定します。

- [MAC Address] : アクセスポイント無線の基本無線 MAC アドレスを入力します。
- [AP Name] : アクセスポイント名。
 

(注) [MAC Address] フィルタを有効にすると、その他のフィルタは自動的に無効になります。その他のフィルタのいずれかを有効にすると、[MAC Address] フィルタは自動的に無効になります。
- [CleanAir Status] : 次のチェックボックスの 1 つまたは複数をおんにして、アクセスポイントの動作ステータスを指定します。
  - [UP] : アクセスポイント無線に対するスペクトラムセンサーが現在正常に動作中です。
  - [DOWN] : アクセスポイント無線に対するスペクトラムセンサーは、エラーが発生したために現在動作していません。最も可能性の高いエラーの原因は、アクセスポイント無線が無効になっていることです。
  - [ERROR] : アクセスポイント無線に対するスペクトラムセンサーがクラッシュしており、この無線に対する CleanAir のモニタリングが機能していません。アクセスポイントをリポート、または無線の CleanAir 機能を無効にすることを推奨します。
  - [N/A] : このアクセスポイント無線は CleanAir の機能に対応していません。現在、Cisco Aironet 3500 シリーズ アクセスポイント無線のみがシスコ CleanAir 用に設定できます。

**ステップ 4** [Find] をクリックして、変更を適用します。検索基準に一致するアクセスポイント無線のみが [802.11a/n/ac Radios] ページまたは [802.11b/g/n Radios] ページに表示され、ページ上部の [Current Filter] パラメータには、リストを生成するのに使用したフィルタが表示されます (たとえば、MAC Address:00:1e:f7:75:0a:a0 または AP Name:pmsk-ap)。

- (注) フィルタを削除してアクセスポイント無線リスト全体を表示するには、[Clear Filter] をクリックします。





# 第 109 章

## アクセスポイントのグローバルクレデンシャルの設定

- [アクセスポイントのグローバルクレデンシャルの設定について](#), 853 ページ
- [アクセスポイントのグローバルクレデンシャルに関する制約事項](#), 854 ページ
- [アクセスポイントのグローバル資格情報の設定 \(GUI\)](#), 855 ページ
- [アクセスポイントのグローバル資格情報の設定 \(CLI\)](#), 856 ページ

### アクセスポイントのグローバルクレデンシャルの設定について

Cisco IOS アクセスポイントには、工場出荷時にデフォルトの `enable` パスワード `Cisco` が設定されています。ユーザはこのパスワードを使用して、非特権モードにログインし、`show` コマンドおよび `debug` コマンドを入力することができますが、これはセキュリティに対する脅威となります。不正アクセスを防止し、ユーザがアクセスポイントのコンソールポートからコンフィギュレーションコマンドを入力できるようにするには、デフォルトのイネーブルパスワードを変更する必要があります。

次に、アクセスポイントのグローバルクレデンシャルの設定に関する注意事項を示します。

- コントローラに現在 `join` している、また、今後 `join` するすべてのアクセスポイントがコントローラに `join` するときに継承するグローバルユーザ名、パスワード、およびイネーブルパスワードを設定することができます。必要に応じて、このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、およびイネーブルパスワードを特定のアクセスポイントに割り当てることができます。
- アクセスポイントをコントローラに `join` すると、そのアクセスポイントのコンソールポートセキュリティが有効になり、コンソールポートへログインするたびにユーザ名とパスワードの入力を要求されます。ログインした時点では非特権モードのため、特権モードを使用するには、イネーブルパスワードを入力する必要があります。
- コントローラで設定したグローバル資格情報はコントローラやアクセスポイントをリブートした後も保持されます。この情報が上書きされるのは、アクセスポイントを、グローバル

ユーザ名およびパスワードが設定された新しいコントローラに **join** した場合のみです。グローバル資格情報を使って新しいコントローラを設定しなかった場合、このアクセスポイントは最初のコントローラに設定されているグローバルユーザ名とパスワードをそのまま保持します。

- アクセスポイントにより使用される資格情報は常に把握している必要があります。そうではない場合、アクセスポイントのコンソールポートにログインできない可能性があります。アクセスポイントをデフォルトのユーザ名およびパスワード *Cisco/Cisco* に戻す必要がある場合は、コントローラの設定をクリアする必要があります。これにより、アクセスポイントの設定は工場出荷時のデフォルト設定に戻ります。コントローラの設定をクリアするには、コントローラ GUI で [Commands] > [Reset to Factory Default] > [Reset] を選択するか、またはコントローラ CLI で **clear config** コマンドを入力します。アクセスポイントの設定をクリアするには、[Wireless] > [Access Points] > [All APs] を選択して AP 名をクリックし、コントローラの GUI で [Clear All Config] をクリックするか、コントローラの CLI で **clear ap config Cisco\_AP** コマンドを入力します。スタティック IP アドレス以外のアクセスポイントの設定をクリアするには、[Wireless] > [Access Points] > [All APs] を選択して AP 名をクリックし、[Clear Config Except Static IP] をクリックするか、コントローラの CLI で **clear ap config ap-name keep-ip-config** コマンドを入力します。アクセスポイントがコントローラに再 **join** した後、デフォルトの *Cisco/Cisco* のユーザ名およびパスワードを適用します。



(注) メッシュモードにするために屋内 Cisco AP を設定したとします。ローカルモードに Cisco AP をリセットする場合は、**test mesh mode local** コマンドを使用します。

- AP ハードウェアをリセットするには、[Wireless] > [Access Points] > [All APs] を選択し、AP 名をクリックして [Reset AP Now] をクリックします。

## アクセスポイントのグローバルクレデンシャルに関する制約事項

- コントローラソフトウェア機能は、1100 シリーズを除いて、Lightweight モードに変換されたすべてのアクセスポイントでサポートされています。VxWorks アクセスポイントはサポートされていません。

## アクセスポイントのグローバル資格情報の設定 (GUI)

- ステップ 1** [Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます。
- ステップ 2** [Username] テキストボックスに、そのコントローラに join するすべてのアクセスポイントが継承するユーザ名を入力します。
- ステップ 3** [Password] テキストボックスに、そのコントローラに join するすべてのアクセスポイントが継承するパスワードを入力します。
- 現在コントローラに join している、また、今後 join するアクセスポイントを含む、すべてのアクセスポイントがコントローラに join するときに継承するグローバルユーザ名、パスワード、および enable パスワードを設定することができます。このグローバル資格情報よりも優先される、独自のユーザ名、パスワード、および enable パスワードを特定のアクセスポイントに割り当てることができます。次に、パスワードに適用される要件を示します。
- パスワードには、小文字、大文字、数字、特殊文字のうち、3つ以上の文字クラスが含まれる必要があります。
  - パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
  - パスワードには、管理ユーザ名やユーザ名を逆にした文字列を含めることはできません。
  - パスワードには、Cisco、ocsic、admin、nimda などの単語や、大文字と小文字の変更、1、|、または ! の代用、または o を 0、s を \$ などで代用したバリエーションを含めることはできません。
- ステップ 4** [Enable Password] テキストボックスに、コントローラに join するすべてのアクセスポイントに継承される enable パスワードを入力します。
- ステップ 5** [Apply] をクリックして、グローバルユーザ名、パスワード、および enable パスワードを、コントローラに現在 join しているアクセスポイント、および今後 join するすべてのアクセスポイントに送信します。
- ステップ 6** [Save Configuration] をクリックして、変更を保存します。
- ステップ 7** (任意) 次の手順で、特定のアクセスポイントに対するグローバル資格情報を無効にし、このアクセスポイントに独自のユーザ名、パスワード、および enable パスワードを割り当てます。
- a) [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
  - b) グローバル資格情報を無効にするアクセスポイントの名前をクリックします。
  - c) [Credentials] タブを選択します。[All APs > Details for] ([Credentials]) ページが表示されます。
  - d) [Override Global Credentials] チェックボックスをオンにし、このアクセスポイントがコントローラからグローバルユーザ名、パスワード、enable パスワードを継承しないようにします。デフォルト値はオフです。
  - e) [Username]、[Password]、および [Enable Password] テキストボックスに、このアクセスポイントに割り当てる独自のユーザ名、パスワード、および enable パスワードを入力します。
 

(注) 入力した情報は、コントローラやアクセスポイントをリブートした後や、アクセスポイントが新しいコントローラに join された場合でも保持されます。
  - f) [Apply] をクリックして、変更を確定します。

g) [Save Configuration] をクリックして、変更を保存します。

(注) このアクセスポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

## アクセスポイントのグローバル資格情報の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、コントローラに現在 join しているアクセスポイント、および今後 join するすべてのアクセスポイントについて、グローバルユーザ名、パスワード、および enable パスワードを設定します。

**config ap mgmtuser add username user password password enablesecret enable\_password all**

**ステップ 2** (任意) 次のコマンドを入力して、特定のアクセスポイントに対するグローバル資格情報を無効にし、このアクセスポイントに独自のユーザ名、パスワード、および enable パスワードを割り当てます。

**config ap mgmtuser add username user password password enablesecret enable\_password Cisco\_AP**

このコマンドに入力した資格情報は、コントローラやアクセスポイントをリブートした後や、アクセスポイントが新しいコントローラに join された場合でも保持されます。

(注) このアクセスポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、**config ap mgmtuser delete Cisco\_AP** コマンドを入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

**ステップ 3** **save config** コマンドを入力して、変更を保存します。

**ステップ 4** 次のコマンドを入力して、コントローラに join するすべてのアクセスポイントに対して、グローバル資格情報が設定されていることを確認します。

**show ap summary**

(注) グローバル資格情報が設定されていない場合、[Global AP User Name] テキストボックスには「Not Configured」と表示されます。

特定のアクセスポイントの概要を表示するには、アクセスポイント名を指定します。また、アクセスポイントのフィルタリングを行うときは、ワイルドカード検索を使用できます。

**ステップ 5** 次のコマンドを入力して、特定のアクセスポイントのグローバル資格情報の設定を表示します。

**show ap config general Cisco\_AP**

(注) アクセスポイントの名前では、大文字と小文字が区別されません。

(注) [AP User Mode] テキストボックスには、グローバル資格情報を使用するようにこのアクセスポイントが設定されている場合は「Automatic」と表示され、このアクセスポイントに対してグローバル資格情報が無効にされている場合は「Customized」と表示されます。



# 第 110 章

## アクセスポイントの認証の設定

---

- [アクセスポイントに対する認証の設定について, 857 ページ](#)
- [アクセスポイントの認証を設定するための前提条件, 857 ページ](#)
- [アクセスポイントの認証に関する制約事項, 858 ページ](#)
- [アクセスポイントの認証の設定 \(GUI\) , 858 ページ](#)
- [アクセスポイントの認証の設定 \(CLI\) , 859 ページ](#)
- [スイッチの認証の設定, 860 ページ](#)

### アクセスポイントに対する認証の設定について

Lightweight アクセスポイントとシスコのスイッチの間で 802.1X 認証を設定できます。アクセスポイントは 802.1X サプリカントとして動作し、EAP-FAST と匿名 PAC プロビジョニングを使用してスイッチにより認証されます。

コントローラに現在関連付けられている、または今後関連付けられるすべてのアクセスポイントにグローバル認証を設定できます。グローバル認証設定を上書きし、特定のアクセスポイントに一意的な認証設定を割り当てることもできます。

### アクセスポイントの認証を設定するための前提条件

---

**ステップ 1** アクセスポイントが新しい場合は、次を実行します。

- a) アクセスポイントを、インストールされたリカバリイメージでブートします。
- b) この提案フローに従わず、アクセスポイントがコントローラに join する前にアクセスポイントに接続されたスイッチポートで 802.1X 認証を有効化するには、次のコマンドを入力します。

**lwapp ap dot1x username username password password**

(注) この提案フローに従って、アクセスポイントがコントローラに join されて設定済みの 802.1X 資格情報を受信してからスイッチポートで 802.1X 認証を有効化する場合は、このコマンドを入力する必要はありません。

(注) このコマンドは、5.1、5.2、6.0、または 7.0 リカバリ イメージを実行しているアクセスポイントでのみ使用できます。

アクセスポイントをスイッチポートに接続します。

**ステップ 2** 5.1、5.2、6.0、または 7.0 イメージをコントローラにインストールし、コントローラをリブートします。

**ステップ 3** すべてのアクセスポイントによるコントローラへの join を許可します。

**ステップ 4** コントローラ上で認証を設定します。コントローラの認証の設定に関する情報については、「[アクセスポイントの認証の設定 \(GUI\)](#)」の項、または「[アクセスポイントの認証の設定 \(CLI\)](#)」の項を参照してください。

**ステップ 5** スイッチを設定して認証を許可します。スイッチの認証の設定については、「[スイッチの認証の設定](#)」の項を参照してください。

## アクセスポイントの認証に関する制約事項

- OEAP 600 シリーズ アクセスポイントでは、LEAP はサポートされません。

## アクセスポイントの認証の設定 (GUI)

**ステップ 1** [Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます。

**ステップ 2** [802.1x Supplicant Credentials] で、[802.1x Authentication] チェックボックスをオンにします。

**ステップ 3** [Username] テキストボックスに、そのコントローラに join するすべてのアクセスポイントが継承するユーザ名を入力します。

**ステップ 4** [Password] ボックスと [Confirm Password] ボックスに、コントローラに join するすべてのアクセスポイントによって継承されるパスワードを入力します。

(注) これらのテキストボックスには、強力なパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。



- ステップ 5** [Apply] をクリックして、グローバル認証ユーザ名およびパスワードを、コントローラに現在 join しているアクセスポイント、および今後 join するすべてのアクセスポイントに送信します。
- ステップ 6** [Save Configuration] をクリックして、変更を保存します。
- ステップ 7** 必要に応じて、次の手順に従って、グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセスポイントに割り当てることができます。
- [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
  - 認証設定を無効にするアクセスポイントの名前をクリックします。
  - [Credentials] タブをクリックして [All APs > Details for] (Credentials) ページを開きます。
  - [802.1x Supplicant Credentials] で [Over-ride Global Credentials] チェックボックスをオンにして、このアクセスポイントがグローバル認証のユーザ名およびパスワードをコントローラから継承しないようにします。デフォルト値はオフです。
  - [Username]、[Password]、および [Confirm Password] テキストボックスに、このアクセスポイントに割り当てて一意のユーザ名およびパスワードを入力します。  
(注) 入力した情報は、コントローラやアクセスポイントをリブートした後や、アクセスポイントが新しいコントローラに join された場合でも保持されます。
  - [Apply] をクリックして、変更を確定します。
  - [Save Configuration] をクリックして、変更を保存します。  
(注) このアクセスポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

## アクセスポイントの認証の設定 (CLI)

- ステップ 1** 次のコマンドを入力して、コントローラに現在 join しているアクセスポイント、および今後 join するすべてのアクセスポイントについて、グローバル認証のユーザ名とパスワードを設定します。
- ```
config ap 802.1Xuser add username ap-username password ap-password all
```
- (注) *ap-password* パラメータには強力なパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。
- 少なくとも 8 文字の長さである。
 - 小文字と大文字、数字、および記号の組み合わせ。
 - どの言語の単語でもない。
- ステップ 2** (任意) グローバル認証設定を無効にし、独自のユーザ名およびパスワードを特定のアクセスポイントに割り当てることができます。そのためには、次のコマンドを入力します。

```
config ap 802.1Xuser add username ap-username password ap-password Cisco_AP
```

(注) *ap-password* パラメータには強力なパスワードを入力する必要があります。強力なパスワードの特徴については、[ステップ 1](#) の注記を参照してください。

このコマンドに入力した認証設定は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。

- (注) このアクセス ポイントで、コントローラのグローバル認証設定を強制的に使用する必要がある場合は、**config ap 802.1Xuser delete Cisco_AP** コマンドを入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

ステップ 3 **save config** コマンドを入力して、変更を保存します。

ステップ 4 (任意) 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントに対して 802.1X 認証を無効にします。

config ap 802.1Xuser disable {all | Cisco_AP}

- (注) 特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

ステップ 5 次のコマンドを入力して、コントローラに join するすべてのアクセス ポイントの認証設定を表示します。
show ap summary

以下に類似した情報が表示されます。

```
Number of APs..... 1
Global AP User Name..... globalap
Global AP Dot1x User Name..... globalDot1x
```

ステップ 6 次のコマンドを入力して、特定のアクセス ポイントの認証設定を表示します。

show ap config general Cisco_AP

- (注) アクセス ポイントの名前では、大文字と小文字が区別されません。
- (注) このアクセス ポイントがグローバル認証を使用するよう設定されている場合は、[APDot1xUser Mode] テキストボックスに「Automatic」と表示されます。このアクセス ポイントでグローバル認証設定が無効にされている場合は、[AP Dot1x User Mode] テキストボックスに「Customized」と表示されます。

スイッチの認証の設定

スイッチ ポートで 802.1X 認証を有効にするには、スイッチ CLI で次のコマンドを入力します。

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**

- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**



第 111 章

組み込みアクセス ポイントの設定

- [組み込みアクセス ポイントについて, 863 ページ](#)

組み込みアクセス ポイントについて

コントローラ ソフトウェア 7.0.116.0 以降のリリースでは、組み込みアクセス ポイント AP802 および AP801 をサポートしています。これらは、Cisco 880 シリーズ サービス統合型ルータ (ISR) の統合されたアクセス ポイントです。このアクセス ポイントはルータの Cisco IOS イメージとは別の Cisco IOS ソフトウェア イメージを使用します。これらのアクセス ポイントは、ローカルに設定および管理される自律アクセス ポイントとして動作することも、CAPWAP または LWAPP プロトコルを使用する、中央管理型のアクセス ポイントとして動作することもできます。AP801 および AP802 アクセス ポイントは、自律 Cisco IOS リリースと、統合モードのリカバリ イメージの両方にプリロードされます。

次に、組み込みアクセス ポイントの注意事項を示します。

- コントローラ ソフトウェア リリース 7.0.116.0 以降のリリースで AP801 または AP802 シリーズ Lightweight アクセス ポイントを使用する前に、Cisco IOS 151-4.M 以降は、次世代 Cisco 880 シリーズ サービス統合型ルータ (ISR) のソフトウェアをアップグレードする必要があります。



(注) リリース 7.4 では、ブリッジング (メッシュに必要) を除くすべての AP モードが AP801 および AP802 の両方でサポートされます。リリース 7.5 以降では、すべての AP モードは AP802 でサポートされます。ただし、ブリッジングは AP801 ではサポートされません。

- コントローラで AP801 または AP802 を使用する場合、ルータ上の特権 EXEC モードで **service-module wlan-ap 0 bootimage unified** コマンドを入力して、アクセス ポイント上の統合モードのリカバリ イメージを有効にする必要があります。
- **service-module wlan-ap 0 bootimage unified** コマンドが動作しない場合は、ソフトウェア ライセンスが有効かどうかを確認してください。

- リカバリ イメージを有効にした後、ルータ上で **service-module wlan-ap 0 reload** コマンドを入力し、アクセス ポイントのシャットダウンとリブートを行います。アクセス ポイントはリブート後にコントローラを検知し、完全な CAPWAP または LWAPP ソフトウェア リリースをコントローラからダウンロードして **Lightweight** アクセス ポイントとして動作します。



(注) 前述の CLI コマンドを使用するには、ルータが Cisco IOS Release 12.4(20)T 以降のリリースを実行している必要があります。

- CAPWAP または LWAPP をサポートするには、ルータがアクティブ化されており、Cisco Advanced IP Services IOS のライセンス グレード イメージを保持している必要があります。ルータ上の Cisco IOS イメージをアップグレードするには、ライセンスが必要です。ライセンス情報については、http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html を参照してください。
- AP801 または AP802 が統合モードのリカバリ イメージと共にブートすると、コントローラと通信し、統合イメージと設定をコントローラからダウンロードするため、IP アドレスが必要です。ルータは DHCP サーバ機能、コントローラにアクセスするための DHCP プール、および DHCP プール設定におけるコントローラ IP アドレスのためのセットアップ オプション 43 を提供できます。このタスクを実行するには、次の設定を使用します。

```
ip dhcp pool pool_name
network ip_address subnet_mask
dns-server ip_address
default-router ip_address
option 43 hex controller_ip_address_in_hex
```

例 :

```
ip dhcp pool embedded-ap-pool
network 60.0.0.0 255.255.255.0
dns-server 171.70.168.183
default-router 60.0.0.1
option 43 hex f104.0a0a.0a0f /* single WLC IP address(10.10.10.15) in hex format
*/
```

- AP801 および AP802 802.11n 無線は、Cisco Aironet 1250 シリーズ アクセス ポイントの 802.11n 無線よりも低い電力レベルをサポートします。AP801 および AP802 アクセス ポイントは、無線電力レベルを保存し、アクセス ポイントがコントローラに join したときにそれらの電力レベルをコントローラに渡します。コントローラは与えられた値を使用してユーザ設定を制限します。
- AP801 と AP802 アクセス ポイントは FlexConnect モードで使用できます。

AP801 の詳細は、次の URL にある Cisco 800 シリーズ ISR についてのマニュアルを参照してください。http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html

AP802 の詳細は、次の URL にある次世代 Cisco 880 シリーズ ISR についてのマニュアルを参照してください。 http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/SCG_880_series.pdf



第 112 章

自律アクセスポイントの Lightweight モード への変換

- [自律アクセスポイントの Lightweight モードへの変換について](#), 868 ページ
- [自律アクセスポイントの Lightweight モードへの変換に関する制約事項](#), 868 ページ
- [Lightweight モードから Autonomous モードへの復帰](#), 868 ページ
- [アクセスポイントの許可](#), 870 ページ
- [アクセスポイントからの CAPWAP フレームの VLAN タギングの設定](#), 876 ページ
- [DHCP オプション 43 および DHCP オプション 60 の使用](#), 877 ページ
- [アクセスポイント join プロセスのトラブルシューティング](#), 879 ページ
- [Lightweight モードに変換されるアクセスポイントへのデバッグコマンドの送信](#), 883 ページ
- [変換したアクセスポイントがクラッシュ情報をコントローラに送信する方法について](#), 884 ページ
- [変換したアクセスポイントが無線コアダンプをコントローラに送信する方法について](#), 884 ページ
- [変換したアクセスポイントからのメモリコアダンプのアップロード](#), 886 ページ
- [AP クラッシュログ情報の表示](#), 888 ページ
- [変換されたアクセスポイントの MAC アドレスの表示](#), 888 ページ
- [Lightweight モードに変換したアクセスポイントの Reset ボタンの無効化](#), 889 ページ
- [Lightweight アクセスポイントでの固定 IP アドレスの設定](#), 889 ページ
- [サイズの大きなアクセスポイントのイメージのサポート](#), 891 ページ

自律アクセス ポイントの Lightweight モードへの変換について

アップグレード変換ツールを使用して、Cisco Aironet 1100、1130AG、1200、1240AG、1260、および 1300 シリーズの Autonomous アクセス ポイントを Lightweight モードに変換できます。これらのいずれかのアクセス ポイントを Lightweight モードに変換した場合、アクセス ポイントはコントローラと通信し、コントローラから設定とソフトウェア イメージを受信します。

自律アクセス ポイントを Lightweight モードにアップグレードする手順については、『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* (自律アクセス ポイントの Lightweight モードへのアップグレード)』を参照してください。

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

次に、自律 AP を Lightweight モードに変換する際の注意事項を示します。

- すべての Cisco Lightweight アクセス ポイントは、無線ごとに 16 個の BSSID、アクセス ポイントごとに総計 16 個の無線 LAN をサポートします。変換したアクセス ポイントがコントローラにアソシエートすると、1～16 の ID を持つ無線 LAN のみがアクセス ポイントにプッシュされます。
- Lightweight モードに変換したアクセス ポイントは、DHCP、DNS、または IP サブネットブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。
- 1130AG アクセス ポイントと 1240AG アクセス ポイントは、FlexConnect モードをサポートします。

自律アクセス ポイントの Lightweight モードへの変換に関する制約事項

- Lightweight モードに変換したアクセス 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。変換したアクセス ポイントは、Cisco 無線 LAN コントローラとのみ通信し、WDS デバイスとは通信できません。ただし、アクセス ポイントがコントローラにアソシエートする際、コントローラが WDS に相当する機能を提供します。
- アクセス ポイントを Lightweight モードに変換した後、コンソール ポートは、そのアクセス ポイントへの読み取り専用アクセスを提供します。

Lightweight モードから Autonomous モードへの復帰

アップグレード ツールで Autonomous アクセス ポイントを Lightweight モードに変換した後、Autonomous モードをサポートする Cisco IOS Release (Cisco IOS Release 12.3(7)JA 以前のリリース) をロードして、そのアクセス ポイントを Lightweight 装置から Autonomous 装置に戻すことができます。アクセス ポイントがコントローラにアソシエートされている場合、コントローラを使用して Cisco IOS Release をロードできます。アクセス ポイントがコントローラにアソシエートされて

いない場合、TFTP を使用して Cisco IOS Release をロードできます。いずれの方法でも、ロードする Cisco IOS Release を含む TFTP サーバにアクセスポイントがアクセスできる必要があります。

以前のリリース (CLI) への復帰

-
- ステップ 1** アクセスポイントがアソシエートしているコントローラで CLI にログインします。
- ステップ 2** 次のコマンドを入力して、lightweight モードから復帰します。
config ap tftp-downgrade tftp-server-ip-address filename access-point-name
- ステップ 3** アクセスポイントがリポートするまで待ち、CLI または GUI を使用してアクセスポイントを再設定します。
-

MODE ボタンと TFTP サーバを使用して前のリリースへの復帰

-
- ステップ 1** TFTP サーバソフトウェアを実行している PC に、10.0.0.2 ~ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定します。
- 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 (1200 シリーズアクセスポイントの場合は、*c1200-k9w7-tar.123-7.JA.tar* など) があり、TFTP サーバがアクティブ化されていることを確認します。
- ステップ 3** 1200 シリーズアクセスポイントの場合は、TFTP サーバフォルダにあるアクセスポイントのイメージファイル名を **c1200-k9w7-tar.default** に変更します。
- 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。
 (注) アクセスポイントの **MODE** ボタンを有効にしておく必要があります。アクセスポイントの **MODE** ボタンのステータスを選択するには、[Lightweight モードに変換したアクセスポイントの Reset ボタンの無効化](#)の手順を実行します。
- ステップ 7** **MODE** ボタンを押し続けて、ステータス LED が赤色に変わった後 (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ポートしてすべての 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** アクセスポイントがリポートしたら、GUI または CLI を使用してアクセスポイントを再設定します。
-

アクセスポイントの許可

5.2よりも前のコントローラソフトウェアリリースでは、コントローラでは自己署名証明書（SSC）を使用してアクセスポイントが認証されるか、RADIUSサーバに許可情報が送信されるかのいずれかとなります（アクセスポイントに製造元がインストールした証明書（MIC）がある場合）。コントローラソフトウェアリリース 5.2以降では、コントローラを設定してローカルで有効な証明書（LSC）を使用できます。

SSCを使用したアクセスポイントの許可

無線アクセスポイントのコントロールおよびプロビジョニング（CAPWAP）プロトコルは、アクセスポイントおよびコントローラの両方で X.509 証明書を必要とするセキュアなキーを配布することにより、アクセスポイントとコントローラの間での制御通信を保護します。CAPWAPは、X.509 証明書のプロビジョニングに依存します。2005年7月18日より前に出荷された Cisco Aironet アクセスポイントにはMICがありません。このため、これらのアクセスポイントでは Lightweight モードで動作するようにアップグレードされた場合、SSCが作成されます。コントローラは特定のアクセスポイントの認証についてローカルSSCを許可するようにプログラムされており、これらの認証要求をRADIUSサーバに転送しません。これは、許容できるセキュアな動作です。

SSCを使用する仮想コントローラのアクセスポイントの許可

物理コントローラによって使用される、製造元がインストールした証明書（MIC）の代わりにSSC証明書を使用する仮想コントローラ。コントローラをAPが仮想コントローラのSSCを検証するように設定できます。APがSSCを検証する場合、APは仮想コントローラハッシュキーがフラッシュに保存されるハッシュキーと一致するかどうかを確認します。一致が見つかった場合、APはコントローラに関連付けます。一致がない場合、検証は失敗し、APはコントローラから切断され、ディスカバリプロセスを再起動します。デフォルトでは、ハッシュ検証は有効です。APは仮想コントローラに関連付ける前に、フラッシュの仮想コントローラのハッシュキーが必要です。SSCのハッシュ検証を無効にすると、APはハッシュ検証をバイパスし、Run状態に直接移動します。APは物理コントローラに関連付けることが可能で、ハッシュキーをダウンロードし、次に仮想コントローラに関連付けます。APが物理コントローラに関連付けられ、ハッシュ検証が無効にされている場合、APはハッシュ検証なしで任意の仮想コントローラに関連付けます。仮想コントローラのハッシュキーをモビリティグループメンバに設定することができます。このハッシュキーは、APがコントローラのハッシュキーを検証できるように、APにプッシュされます。

SSC（GUI）の設定

- ステップ 1** [Security] > [Certificate] > [SSC] の順に選択して、[Self Significant Certificates (SSC)] ページを開きます。SSCのデバイス認証の詳細が表示されます。

ステップ 2 ハッシュ キー検証を有効にするには、[Enable SSC Hash Validation] チェックボックスを選択します。

ステップ 3 [Apply] をクリックして、変更を確定します。

SSC の設定 (CLI)

ステップ 1 SSC のハッシュ検証を設定するには、次のコマンドを入力します。
config certificate ssc hash validation {enable | disable}

ステップ 2 ハッシュ キーの詳細を表示するには、次のコマンドを入力します。
show certificate ssc

MIC を使用したアクセスポイントの許可

RADIUS サーバによって、MIC を使用してアクセスポイントを許可するようにコントローラを設定できます。コントローラでは、情報を RADIUS サーバに送信する際、アクセスポイントの MAC アドレスがユーザ名とパスワードの両方に使用されます。たとえば、アクセスポイントの MAC アドレスが 000b85229a70 の場合、コントローラでアクセスポイントを許可する際に使用されるユーザ名もパスワードも 000b85229a70 になります。



(注) アクセスポイントの MAC アドレスでは、パスワードが強力ではないことは問題にはなりません。コントローラでは RADIUS サーバを介したアクセスポイントの許可の前に、MIC を使用してアクセスポイントが認証されるためです。MIC の使用により、強力で認証されます。



(注) MAC アドレスを RADIUS AAA サーバのアクセスポイントの認証に対するユーザ名とパスワードに使用する場合には、同じ AAA サーバをクライアント認証に使用しないでください。

LSC を使用したアクセスポイントの許可

独自の公開キーインフラストラクチャ (PKI) でセキュリティを向上させ、認証局 (CA) を管理し、生成された証明書上の方針、制限、および使用方法を定義する場合、LSC を使用できます。

LSC CA 証明書は、アクセスポイントおよびコントローラにインストールされています。アクセスポイント上のデバイス証明書はプロビジョニングが必要です。アクセスポイントは、コントローラに certRequest を送信して署名された X.509 証明書を取得します。コントローラは CA プロキシとして動作し、このアクセスポイントのために CA が署名した certRequest を受信します。



(注) CA サーバが手動モードにあり、保留中の登録である LSC SCEP テーブルに AP エントリがある場合、コントローラは保留中の応答を返すように、CA サーバを待ちます。CA サーバからの応答がない場合、コントローラは応答の取得を3回まで試みます。その後、フォールバックモードに入り、AP プロビジョニングはタイムアウトとなり、AP はリブートして、MIC を提示します。



(注) コントローラの LSC ではパスワードの確認は行われません。このため、LSC を機能させるには、CA サーバでパスワードの確認を無効にする必要があります。Microsoft Windows Server 2008 ではパスワードの確認を無効に設定できないため、それを CA サーバとして使用することはできません。

ローカルで有効な証明書 (GUI) の設定

- ステップ 1** [Security] > [Certificate] > [LSC] を選択して、[Local Significant Certificates (LSC)] ([General]) ページを開きます。
- ステップ 2** [Enable LSC on Controller] チェックボックスをオンにして、システムの LSC を有効にします。
- ステップ 3** [CA Server URL] テキストボックスで、CA サーバへの URL を入力します。ドメイン名を入力することも IP アドレスを入力することもできます。
- ステップ 4** [Params] テキストボックスに、デバイス証明書のパラメータを入力します。キーのサイズは 384 ~ 2048 (ビット) の範囲であり、デフォルト値は 2048 です。
- ステップ 5** [Apply] をクリックして、変更を確定します。
- ステップ 6** コントローラの CA 証明書データベースに CA 証明書を追加するには、証明書タイプの青いドロップダウンの矢印の上にカーソルを置いて、[Add] を選択します。
- ステップ 7** [AP Provisioning] タブを選択して、[Local Significant Certificates (LSC)] ([AP Provisioning]) ページを開きます。
- ステップ 8** [Enable] チェックボックスをオンにして [Update] をクリックし、アクセスポイントに LSC をプロビジョニングします。
- ステップ 9** アクセスポイントがリブートされることを示すメッセージが表示されたら、[OK] をクリックします。
- ステップ 10** [Number of Attempts to LSC] テキストボックスに、アクセスポイントが、証明書をデフォルト (MIC または SSC) に戻す前に、LSC を使用してコントローラに join を試みる回数を入力します。範囲は 0 ~ 255 (両端の値を含む) で、デフォルト値は 3 です。
- (注) 再試行回数を 0 以外の値に設定した場合に、アクセスポイントが設定された再試行回数後に LSC を使用してコントローラに join できなかった場合、アクセスポイントは証明書をデフォルトに戻します。再試行回数を 0 に設定した場合、アクセスポイントが LSC 使用によるコントローラへの join に失敗すると、このアクセスポイントはデフォルトの証明書を使用したコントローラへの join を試みません。

(注) 初めて LSC を設定する場合は、ゼロ以外の値を設定することが推奨されます。

ステップ 11 [AP Ethernet MAC Addresses] テキストボックスにアクセスポイントの MAC アドレスを入力し、[Add] をクリックしてアクセスポイントのプロビジョンリストに追加します。

(注) アクセスポイントのプロビジョンリストから削除するには、そのアクセスポイントの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。

(注) アクセスポイントプロビジョンリストを設定すると、AP プロビジョニングを有効にした場合に、プロビジョンリスト内のアクセスポイントのみがプロビジョニングされます。アクセスポイントプロビジョンリストを設定しない場合、コントローラに join する MIC または SSC 証明書を持つすべてのアクセスポイントが LSC でプロビジョニングされます。

ステップ 12 [Apply] をクリックして、変更を確定します。

ステップ 13 [Save Configuration] をクリックして、変更を保存します。

ローカルで有効な証明書 (CLI) の設定

ステップ 1 次のコマンドを入力して、システム上で LSC を有効にします。
config certificate lsc {enable | disable}

ステップ 2 次のコマンドを入力して、URL を CA サーバに設定します。
config certificate lsc ca-server http://url:port/path

ここで、*url* にはドメイン名を入力することも IP アドレスを入力することもできます。

(注) 1 つの CA サーバだけを設定できます。異なる CA サーバを設定するには、**config certificate lsc ca-server delete** コマンドを使用して設定された CA サーバを削除し、異なる CA サーバを設定します。

ステップ 3 次のコマンドを入力して、LSC CA 証明書をコントローラの CA 証明書データベースに追加します。
config certificate lsc ca-cert {add | delete}

ステップ 4 次のコマンドを入力して、デバイス証明書のパラメータを設定します。
config certificate lsc subject-params country state city orgn dept e-mail

(注) Common Name (CN) は、現在の MIC/SSC 形式である *Cxxxx-MacAddr* を使用して、アクセスポイント上で自動的に生成されます。ここで、*xxxx* は製品番号です。

ステップ 5 次のコマンドを入力して、キーサイズを設定します。
config certificate lsc other-params keysize

keysize は 384 ~ 2048 (ビット) の値を指定します。デフォルト値は 2048 です。

ステップ 6 次のコマンドを入力して、アクセスポイントをプロビジョンリストに追加します。
config certificate lsc ap-provision auth-list add AP_mac_addr

- (注) プロビジョンリストからアクセスポイントを削除するには、**config certificate lsc ap-provision auth-list delete AP_mac_addr** コマンドを入力します。
- (注) アクセスポイントプロビジョニングリストを設定する場合は、APプロビジョニングを有効にしたときに(手順8)プロビジョニングリストのアクセスポイントだけがプロビジョニングされます。アクセスポイントプロビジョンリストを設定しない場合、コントローラにjoinするMICまたはSSC証明書を持つすべてのアクセスポイントがLSCでプロビジョニングされます。

ステップ7 次のコマンドを入力して、アクセスポイントがデフォルトの証明書(MICまたはSSC)に復帰する前に、LSCを使用してコントローラにjoinを試みる回数を設定します。

config certificate lsc ap-provision revert-cert retries

ここで、*retries* の値は 0 ~ 255、デフォルト値は 3 です。

- (注) 再試行回数を 0 以外の値に設定した場合に、アクセスポイントが設定された再試行回数後にLSCを使用してコントローラにjoinできなかった場合、アクセスポイントは証明書をデフォルトに戻します。再試行回数を 0 に設定した場合、アクセスポイントがLSC使用によるコントローラへのjoinに失敗すると、このアクセスポイントはデフォルトの証明書を使用したコントローラへのjoinを試みません。
- (注) 初めてLSCを設定する場合は、ゼロ以外の値を設定することが推奨されます。

ステップ8 次のコマンドを入力して、アクセスポイントのLSCをプロビジョニングします。

config certificate lsc ap-provision {enable | disable}

ステップ9 次のコマンドを入力して、LSCの概要を表示します。

show certificate lsc summary

以下に類似した情報が表示されます。

```
LSC Enabled..... Yes
LSC CA-Server..... http://10.0.0.1:8080/caserver

LSC AP-Provisioning..... Yes
Provision-List..... Not Configured
LSC Revert Count in AP reboots..... 3

LSC Params:
Country..... 4
State..... ca
City..... ss
Orgn..... org
Dept..... dep
Email..... dep@co.com
KeySize..... 390

LSC Certs:
CA Cert..... Not Configured
RA Cert..... Not Configured
```

ステップ10 次のコマンドを入力して、LSCを使用してプロビジョニングされたアクセスポイントについての詳細を表示します。

show certificate lsc ap-provision

以下に類似した情報が表示されます。

```
LSC AP-Provisioning..... Yes
Provision-List..... Present

Idx  Mac Address
---  -
1    00:18:74:c7:c0:90
```

アクセスポイントの許可 (GUI)

- ステップ 1** [Security] > [AAA] > [AP Policies] の順に選択して、[AP Policies] ページを開きます。
- ステップ 2** アクセスポイントに自己署名証明書 (SSC)、製造元でインストールされる証明書 (MIC)、またはローカルで有効な証明書 (LSC) を受け入れさせる場合は、該当するチェックボックスをオンにします。
- ステップ 3** アクセスポイントを許可する際に AAA RADIUS サーバを使用する場合は、[Authorize MIC APs against auth-list or AAA] チェックボックスをオンにします。
- ステップ 4** アクセスポイントを許可する際に LSC を使用する場合は、[Authorize LSC APs against auth-list] チェックボックスをオンにします。
- ステップ 5** [Apply] をクリックして、変更を確定します。
- ステップ 6** アクセスポイントをコントローラの許可リストに追加する手順は、次のとおりです。
- [Add] をクリックして、[Add AP to Authorization List] 領域にアクセスします。
 - [MAC Address] テキストボックスに、アクセスポイントの MAC アドレスを入力します。
 - [Certificate Type] ドロップダウンリストから、[MIC]、[SSC]、または [LSC] を選択します。
 - [Add] をクリックします。アクセスポイントが許可リストに表示されます。
 - (注) アクセスポイントを許可リストから削除するには、そのアクセスポイントの青いドロップダウン矢印にカーソルを置いて [Remove] を選択します。
 - (注) 特定のアクセスポイントを許可リストで検索するには、[Search by MAC] テキストボックスにアクセスポイントの MAC アドレスを入力して [Search] をクリックします。

アクセスポイントの許可 (CLI)

- 次のコマンドを入力して、アクセスポイントの許可ポリシーを設定します。
config auth-list ap-policy {authorize-ap {enable | disable} | authorize-lsc-ap {enable | disable}}

- 次のコマンドを入力して、アクセスポイントが製造元でインストールされる証明書（MIC）、自己署名証明書（SSC）、またはローカルで有効な証明書（LSC）を受け入れるよう設定します。

```
config auth-list ap-policy {mic | ssc | lsc {enable | disable}}
```

- ユーザ名がアクセスポイント認証要求で使用されるように設定します。

```
config auth-list ap-policy {authorize-ap username {ap_name | ap_mac | both}}
```

- 次のコマンドを入力して、許可リストにアクセスポイントを追加します。

```
config auth-list add {mic | ssc | lsc} ap_mac [ap_key]
```

ap_key は 20 バイト、つまり 40 桁のオプションキーハッシュ値です。



(注) アクセスポイントを許可リストから削除するには、次のコマンドを入力します。 **config auth-list delete ap_mac**

- 次のコマンドを入力して、アクセスポイントの許可リストを表示します。

```
show auth-list
```

アクセスポイントからの CAPWAP フレームの VLAN タギングの設定

アクセスポイントからの CAPWAP フレームの VLAN タギングについて

AP コンソールのまたはコントローラから直接イーサネットインターフェイスで VLAN タギングを設定できます。設定はフラッシュメモリに保存され、ローカルにスイッチングされるすべてのトラフィックとともに、すべての CAPWAP フレームは設定されるように VLAN タグを使用し、VLAN にはマッピングされていません。

この機能は、ブリッジモードのメッシュアクセスポイントではサポートされません。

アクセスポイントからの CAPWAP フレームの VLAN タギングの設定 (GUI)

ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

ステップ 2 AP の [Details] ページを開くには、AP 名のリストから AP 名をクリックします。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 VLAN タギングの領域で、[VLAN Tagging] チェックボックスを選択します。

ステップ 5 [Trunk VLAN ID] テキストボックスに、ID を入力します。

約 10 分後に、アクセスポイントが指定したトランク VLAN を経由してトラフィックをルーティングできない場合、リポートおよびタグなしモードで CAPWAP フレームの送信により、アクセスポイントは回復手順を実行し、コントローラに再アソシエートします。コントローラは Cisco Prime Infrastructure などトラップサーバにトランク VLAN の失敗を示すトラップを送信します。

アクセス ポイントが指定トランク VLAN を経由してトラフィックをルーティングできない場合、パケットのタグ付けが解除され、コントローラに再アソシエートされます。コントローラは Cisco Prime Infrastructure などトラップ サーバにトランク VLAN の失敗を示すトラップを送信します。

トランク VLAN ID が 0 の場合、アクセス ポイントは CAPWAP フレームのタグ付けを解除します。

AP が CAPWAP フレームにタグ付けするかタグ付けを解除するかを示す VLAN タグのステータスが表示されます。

ステップ 6 [Apply] をクリックします。

ステップ 7 設定がアクセス ポイントのリポートを発生させることを伝える警告メッセージが表示されます。[OK] をクリックして作業を続行します。

ステップ 8 [Save Configuration] をクリックします。

次の作業

設定後にタグ付きイーサネット フレームをサポートするには、AP のイーサネット インターフェイスに接続されているスイッチまたは他の機器も設定する必要があります。

アクセス ポイントからの CAPWAP フレームの VLAN タギングの設定 (CLI)

ステップ 1 次のコマンドを入力して、アクセス ポイントからの CAPWAP フレームの VLAN タギングを設定します。
config ap ethernet tag {disable | id vlan-id} {ap-name | all}

ステップ 2 次のコマンドを入力して、AP またはすべての AP についての VLAN タギング情報を表示できます。
show ap ethernet tag {summary | ap-name}

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセス ポイントは、DHCP オプション 43 に Type-Length-Value (TLV) 形式を使用します。DHCP サーバは、アクセス ポイントの DHCP ベンダー クラス ID (VCI) 文字列に基づいてオプションを返すようにプログラムする必要があります (DHCP オプション 60)。

次の表に、Lightweight モードで動作可能な Cisco アクセス ポイントの VCI 文字列を示します。

表 23: Lightweight アクセス ポイントの VCI 文字列

| アクセス ポイント | VCI 文字列 |
|-------------------------|----------------|
| Cisco Aironet 1040 シリーズ | Cisco AP c1040 |

| アクセス ポイント | VCI 文字列 |
|---------------------------|----------------|
| Cisco Aironet 1130 シリーズ | Cisco AP c1130 |
| Cisco Aironet 1140 シリーズ | Cisco AP c1140 |
| Cisco Aironet 1240 シリーズ | Cisco AP c1240 |
| Cisco Aironet 1250 シリーズ | Cisco AP c1250 |
| Cisco Aironet 1260 シリーズ | Cisco AP c1260 |
| Cisco Aironet 1520 シリーズ | Cisco AP c1520 |
| Cisco Aironet 1550 シリーズ | Cisco AP c1550 |
| Cisco Aironet 3600 シリーズ | Cisco AP c3600 |
| Cisco Aironet 3500 シリーズ | Cisco AP c3500 |
| Cisco AP801 組み込みアクセス ポイント | Cisco AP801 |
| Cisco AP802 組み込みアクセス ポイント | Cisco AP802 |

TLV ブロックの形式は、次のとおりです。

- 型：0xf1（十進数では 241）
- 長さ：コントローラの IP アドレス数 * 4
- 値：コントローラの管理インターフェイスの IP アドレス リスト

DHCP オプション 43 の設定方法については、ご使用の DHCP サーバの製品ドキュメンテーションを参照してください。『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセス ポイントが、サービス プロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセス ポイントの VCI ストリングは上記の VCI ストリングと異なります。VCI ストリングには、「ServiceProvider」が含まれます。たとえば、このオプション付きの 1260 は、VCI ストリング「Cisco AP c1260-ServiceProvider」を返します。



- (注) DHCP サーバから取得するコントローラの IP アドレスは、ユニキャスト IP アドレスになります。DHCP オプション 43 を設定する場合は、マルチキャストアドレスとしてコントローラの IP アドレスを設定しないでください。

アクセス ポイント join プロセスのトラブルシューティング

アクセス ポイントがコントローラへの join を失敗する理由として、RADIUS の許可が保留の場合、コントローラで自己署名証明書が有効になっていない場合、アクセス ポイントとコントローラ間の規制ドメインが一致しない場合など、多くの原因が考えられます。

コントローラ ソフトウェア リリース 5.2 以降のリリースでは、すべての CAPWAP 関連エラーを syslog サーバに送信するようアクセス ポイントを設定できます。すべての CAPWAP エラーメッセージは syslog サーバ自体から表示できるので、コントローラでデバッグ コマンドを有効にする必要はありません。

アクセス ポイントの状態は、アクセス ポイントからの CAPWAP join request を受信するまでコントローラで維持されません。そのため、特定のアクセス ポイントからの CAPWAP discovery request が拒否された理由を判断することは難しい場合があります。そのような join の問題をコントローラで CAPWAP デバッグ コマンドを有効にせずトラブルシューティングするために、コントローラは discovery メッセージを送信してきたすべてのアクセス ポイントの情報を収集し、このコントローラに正常に join したアクセス ポイントの情報を保持します。

コントローラは、CAPWAP discovery request を送信してきた各アクセス ポイントについて、join 関連のすべての情報を収集します。収集は、アクセス ポイントから最初に受信した discovery メッセージから始まり、コントローラからアクセス ポイントに送信された最後の設定ペイロードで終わります。

join 関連の情報を表示できるアクセス ポイントの数は、次のとおりです。

コントローラが最大数のアクセス ポイントの join 関連情報を維持している場合、それ以上のアクセス ポイントの情報は収集されません。

以上のいずれかの条件と一致しているのにアクセス ポイントがコントローラに join しない場合には、DHCP サーバを設定し、サーバ上のオプション 7 を使用して syslog サーバの IP アドレスをアクセス ポイントに戻すこともできます。それにより、アクセス ポイントではすべての syslog メッセージがこの IP アドレスへ送信されるようになります。

lwapp ap log-server syslog_server IP_address コマンドを入力することにより、アクセス ポイントが現在コントローラに接続していない場合、アクセス ポイントの CLI を介して syslog サーバの IP アドレスを設定することもできます。

アクセス ポイントが最初にコントローラに join する際に、コントローラはグローバルな syslog サーバの IP アドレス（デフォルトは 255.255.255.255）をアクセス ポイントにコピーします。その後、IP アドレスが次のいずれかのシナリオで上書きされるまで、アクセス ポイントはすべての syslog メッセージをこの IP アドレスに送信します。

- アクセス ポイントは同じコントローラに接続されたままで、コントローラ上のグローバル syslog サーバの IP アドレスの設定が **config ap syslog host global syslog_server IP_address** コマンドを使用して変更された。この場合、コントローラは新しいグローバル syslog サーバの IP アドレスをアクセス ポイントへコピーします。
- アクセス ポイントは同じコントローラに接続されたままで、特定の syslog サーバの IP アドレスが **config ap syslog host specific Cisco_AP syslog_server IP_address** コマンドを使用してコ

ントローラ上のアクセスポイントに対して設定された。この場合、コントローラは新しい特定の syslog サーバの IP アドレスをアクセスポイントへコピーします。

- アクセスポイントはコントローラから接続を切断されており、syslog サーバの IP アドレスが **lwapp ap log-server syslog_server IP_address** コマンドを使用して、アクセスポイントの CLI から設定された。このコマンドは、アクセスポイントが他のコントローラに接続されていない場合に限り機能します。
- アクセスポイントがコントローラから join を切断され、別のコントローラに join している。この場合、新しいコントローラはそのグローバル syslog サーバの IP アドレスをアクセスポイントへコピーします。

新しい syslog サーバの IP アドレスが既存の syslog サーバの IP アドレスを上書きするたびに、古いアドレスは固定記憶域から消去され、新しいアドレスがそこに保存される。アクセスポイントはその syslog サーバの IP アドレスに到達できれば、すべての syslog メッセージを新しい IP アドレスに送信するようになります。

コントローラ GUI を使用してアクセスポイントの syslog サーバを設定したり、コントローラ GUI または CLI を使用してアクセスポイントの接続情報を表示したりできます。

アクセスポイントの Syslog サーバの設定 (CLI)

ステップ 1 次のいずれかの操作を行います。

- このコントローラに join するすべてのアクセスポイントに対して、グローバルな syslog サーバを設定するには、次のコマンドを入力します。

config ap syslog host global syslog_server IP_address

(注) デフォルトでは、すべてのアクセスポイントのグローバル syslog サーバ IP アドレスは 255.255.255.255 です。コントローラ上の syslog サーバを設定する前に、アクセスポイントがこのサーバが常駐するサブネットにアクセスできることを確認します。このサブネットにアクセスできない場合、アクセスポイントは syslog メッセージを送信できません。

- 特定のアクセスポイントの syslog サーバを設定するには、次のコマンドを入力します。

config ap syslog host specific Cisco_AP syslog_server IP_address

(注) デフォルトでは、各アクセスポイントの syslog サーバ IP アドレスは 0.0.0.0 で、これはまだアクセスポイントが設定されていないことを示しています。このデフォルト値を使用すると、グローバルアクセスポイント syslog サーバの IP アドレスがアクセスポイントにプッシュされます。

ステップ 2 **save config** コマンドを入力して、変更を保存します。

ステップ 3 次のコマンドを入力して、コントローラに join するすべてのアクセスポイントに対して、グローバルな syslog サーバの設定を表示します。

show ap config global

以下に類似した情報が表示されます。

```
AP global system logging host..... 255.255.255.255
```

- ステップ 4** 次のコマンドを入力して、特定のアクセスポイントの syslog サーバの設定を表示します。
show ap config general Cisco_AP

アクセスポイントの join 情報の表示

CAPWAP discovery request をコントローラに少なくとも 1 回送信するアクセスポイントの join に関する統計情報は、アクセスポイントがリブートまたは切断されても、コントローラ上に維持されます。これらの統計情報は、コントローラがリブートされた場合、または統計情報のクリアを選択した場合のみ削除されます。

アクセスポイントの join 情報の表示 (GUI)

- ステップ 1** [Monitor] > [Statistics] > [AP Join] の順に選択して、[AP Join Stats] ページを開きます。このページには、コントローラに join している、または join を試みたことのあるすべてのアクセスポイントが表示されます。無線 MAC アドレス、アクセスポイント名、現在の join ステータス、イーサネット MAC アドレス、IP アドレス、および各アクセスポイントの最後の join 時刻を示します。
- ページの右上部には、アクセスポイントの合計数が表示されます。アクセスポイントのリストが複数ページに渡る場合、ページ番号のリンクをクリックしてこれらのページを表示できます。各ページには最大 25 台のアクセスポイントの join 統計情報を表示できます。
- (注) アクセスポイントをリストから削除する必要がある場合は、そのアクセスポイントの青いドロップダウン矢印にカーソルを置いて [Remove] をクリックします。
 - (注) すべてのアクセスポイントの統計情報をクリアして統計を再開したい場合は、[Clear Stats on All APs] をクリックします。
- ステップ 2** [AP Join Stats] ページのアクセスポイントリストで特定のアクセスポイントを検索する場合は、次の手順に従って、特定の基準 (MAC アドレスやアクセスポイント名など) を満たすアクセスポイントのみを表示するフィルタを作成します。
- (注) この機能は、アクセスポイントのリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。
- a) [Change Filter] をクリックして、[Search AP] ダイアログボックスを開きます。
 - b) 次のチェックボックスのいずれかをオンにして、アクセスポイントを表示する際に使用する基準を指定します。
 - [MAC Address] : アクセスポイントのベース無線 MAC アドレスを入力します。
 - [AP Name] : アクセスポイントの名前を入力します。

(注) これらのフィルタのいずれかを有効にすると、もう1つのフィルタは自動的に無効になります。

- c) [Find] をクリックして、変更を適用します。検索基準と一致するアクセスポイントのみが [AP Join Stats] ページに表示され、ページ上部の [Current Filter] はリストを生成するのに使用したフィルタ (MAC Address:00:1e:f7:75:0a:a0、または AP Name:pmsk-ap など) を示します。

(注) フィルタを削除してアクセスポイントリスト全体を表示するには、[Clear Filter] をクリックします。

ステップ 3 特定のアクセスポイントの詳細な join 統計情報を表示するには、アクセスポイントの無線 MAC アドレスをクリックします。[AP Join Stats Detail] ページが表示されます。このページには、コントローラ側からの join プロセスの各段階に関する情報と発生したエラーが表示されます。

アクセスポイントの join 情報の表示 (CLI)

次の CLI コマンドを使用して、アクセスポイントの join 情報を表示します。

- 次のコマンドを入力して、コントローラに join している、または join を試行した、すべてのアクセスポイントの MAC アドレスを表示します。

show ap join stats summary all

- 次のコマンドを入力して、特定のアクセスポイントの最新 join エラーの詳細を表示します。

show ap join stats summary ap_mac

ap_mac は、802.11 無線インターフェースの MAC アドレスです。



(注) 802.11 無線インターフェースの MAC アドレスを取得するには、目的のアクセスポイントで **show interfaces Dot11Radio 0** コマンドを入力します。

以下に類似した情報が表示されます。

```
Is the AP currently connected to controller..... Yes
Time at which the AP joined this controller last time..... Aug 21
12:50:36.061
Type of error that occurred last..... AP got or has
been disconnected
Reason for error that occurred last..... The AP has
been reset by the controller
Time at which the last join error occurred..... Aug 21
12:50:34.374
```

- 次のコマンドを入力して、特定アクセスポイントで収集されたすべての join 関連の統計情報を表示します。

show ap join stats detailed ap_mac

以下に類似した情報が表示されます。

```
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt..... RADIUS authorization
  is pending for the AP
- Time at last successful join attempt..... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt..... Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable

Last AP disconnect details
- Reason for last AP connection failure..... The AP has been reset by
  the controller

Last join error summary
- Type of error that occurred last..... AP got or has been
  disconnected
- Reason for error that occurred last..... The AP has been reset by
  the controller
- Time at which the last join error occurred..... Aug 21 12:50:34.374
```

- 次のコマンドを入力して、すべてのアクセスポイントまたは特定のアクセスポイントのjoin統計情報をクリアします。

```
clear ap join stats {all | ap_mac}
```

Lightweight モードに変換されるアクセスポイントへのデバッグコマンドの送信

次のコマンドを入力して、コントローラが、Lightweight モードに変換されるアクセスポイントにデバッグコマンドを送信できるようにします。

```
debug ap {enable | disable | command cmd} Cisco_AP
```

この機能を有効にした場合、コントローラは変換したアクセスポイントに文字列としてデバッグコマンドを送信します。Cisco IOS ソフトウェアを Lightweight モードで実行する Cisco Aironet アクセスポイントがサポートしている任意のデバッグコマンドを送信することができます。

変換したアクセスポイントがクラッシュ情報をコントローラに送信する方法について

変換したアクセスポイントが予期せずリブートした場合、アクセスポイントではクラッシュ発生時にローカルフラッシュメモリ上にクラッシュファイルが保存されます。リブート後、アクセスポイントはリブートの理由をコントローラに送信します。クラッシュにより装置がリブートした場合、コントローラは既存の CAPWAP メッセージを使用してクラッシュファイルを取得し、コントローラのフラッシュメモリにそれを保存します。クラッシュ情報コピーは、コントローラがアクセスポイントからこれを取得した時点でアクセスポイントのフラッシュメモリから削除されます。

変換したアクセスポイントが無線コア ダンプをコントローラに送信する方法について

変換したアクセスポイントの無線モジュールがコア ダンプを生成した場合、アクセスポイントは無線クラッシュ発生時にローカルフラッシュメモリ上に無線のコア ダンプ ファイルを保存します。また、無線がコア ダンプ ファイルを生成したことを知らせる通知メッセージをコントローラに送信します。アクセスポイントから無線コア ファイルを受信できるように通知するトラップが、コントローラから送られてきます。

取得したコア ファイルはコントローラのフラッシュに保存されます。このファイルを TFTP または FTP 経由で外部サーバにアップロードし、分析に使用することができます。コア ファイルは、コントローラがアクセスポイントからそれを取得した時点でアクセスポイントのフラッシュメモリから削除されます。

無線コア ダンプの取得 (CLI)

-
- ステップ 1** 次のコマンドを入力して、アクセスポイントからコントローラに無線コア ダンプ ファイルを転送します。
config ap crash-file get-radio-core-dump slot Cisco_AP
- slot* パラメータには、クラッシュした無線のスロット ID を入力します。
- ステップ 2** 次のコマンドを入力して、ファイルがコントローラにダウンロードされたことを確認します。
show ap crash-file
-

無線コア ダンプのアップロード (GUI)

-
- ステップ 1 [Commands] > [Upload File] の順に選択して、[Upload File from Controller] ページを開きます。
- ステップ 2 [File Type] ドロップダウン リストから、[Radio Core Dump] を選択します。
- ステップ 3 [Transfer Mode] ドロップダウン リストで、次のオプションから選択します。
- TFTP
 - FTP
 - SFTP (7.4 以降のリリースで利用可能)
- ステップ 4 [IP Address] テキスト ボックスに、サーバの IP アドレスを入力します。
- ステップ 5 [File Path] テキスト ボックスに、ファイルのディレクトリ パスを入力します。
- ステップ 6 [File Name] テキスト ボックスに、無線コア ダンプ ファイルの名前を入力します。
(注) 入力するファイル名は、コントローラで生成されるファイル名と一致する必要があります。コントローラ上のファイル名を確認するには、**show ap crash-file** コマンドを入力します。
- ステップ 7 [Transfer Mode] として [FTP] を選択した場合は、次の手順を実行します。
- a) [Server Login Username] テキスト ボックスに、FTP サーバのログイン名を入力します。
 - b) [Server Login Password] テキスト ボックスに、FTP サーバのログインパスワードを入力します。
 - c) [Server Port Number] テキスト ボックスに、FTP サーバのポート番号を入力します。サーバポートのデフォルト値は 21 です。
- ステップ 8 [Upload] をクリックして、コントローラから無線コア ダンプ ファイルをアップロードします。アップロードのステータスを示すメッセージが表示されます。
-

無線コア ダンプのアップロード (CLI)

-
- ステップ 1 次のコマンドを入力して、コントローラからサーバにファイルを転送します。
- **transfer upload mode {tftp | ftp | sftp}**
 - **transfer upload datatype radio-core-dump**
 - **transfer upload serverip *server_ip_address***
 - **transfer upload path *server_path_to_file***
 - **transfer upload filename *filename***
- (注) 入力するファイル名は、コントローラで生成されるファイル名と一致する必要があります。コントローラ上のファイル名を確認するには、**show ap crash-file** コマンドを入力します。

- (注) *filename* および *server_path_to_file* に特殊文字 \、:、*、?、"、<、>、および | が含まれていないことを確認してください。パス区切り文字として使用できるのは、/ (フォワードスラッシュ) のみです。許可されていない特殊文字を *filename* に使用すると、その特殊文字は _ (アンダースコア) に置き換えられます。また、許可されていない特殊文字を *server_path_to_file* に使用すると、パスがルートパスに設定されます。

ステップ 2 FTP サーバを使用している場合は、次のコマンドも入力します。

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

- (注) *port* パラメータのデフォルト値は 21 です。

ステップ 3 次のコマンドを入力して、更新された設定を表示します。

transfer upload start

ステップ 4 現在の設定を確認してソフトウェアアップロードを開始するよう求めるプロンプトが表示されたら、**y** と入力します。

変換したアクセスポイントからのメモリコアダンプのアップロード

デフォルトでは、Lightweight モードに変換したアクセスポイントは、コントローラにメモリコアダンプを送信しません。この項では、コントローラ GUI または CLI を使用してアクセスポイントコアダンプをアップロードする手順について説明します。

アクセスポイントのコアダンプのアップロード (GUI)

-
- ステップ 1** [Wireless] > [Access Points] > [All APs] > [access point name] > [Advanced] タブを順に選択して、[All APs > Details for] ([Advanced]) ページを開きます。
- ステップ 2** [APCoreDump] チェックボックスをオンにして、アクセスポイントのコアダンプをアップロードします。
- ステップ 3** [TFTP Server IP] テキストボックスに、TFTP サーバの IP アドレスを入力します。
- ステップ 4** [File Name] テキストボックスに、アクセスポイントコアダンプファイルの名前 (*dump.log* など) を入力します。
- ステップ 5** [File Compression] チェックボックスをオンにして、アクセスポイントのコアダンプファイルを圧縮します。このオプションを有効にすると、ファイルは .gz 拡張子を付けて保存されます (*dump.log.gz* など)。このファイルは、WinZip で開くことができます。
- ステップ 6** [Apply] をクリックして、変更を確定します。
- ステップ 7** [Save Configuration] をクリックして、変更を保存します。
-

アクセスポイントのコアダンプのアップロード (CLI)

-
- ステップ 1** アクセスポイントのコアダンプをアップロードするには、コントローラで次のコマンドを入力します。
- ```
config ap core-dump enable tftp_server_ip_address filename {compress | uncompress} {ap_name | all}
```
- 値は次のとおりです。
- *tftp\_server\_ip\_address* は、アクセスポイントがコアダンプファイルを送信する送信先 TFTP サーバの IP アドレスです。
    - (注) アクセスポイントは TFTP サーバに到達できる必要があります。
  - *filename* は、アクセスポイントがコアファイルのラベル付けに使用する名前です。
  - **compress** はアクセスポイントが圧縮されたコアファイルを送信するよう設定し、**uncompress** はアクセスポイントが非圧縮のコアファイルを送信するよう設定します。
    - (注) **compress** を選択すると、ファイルは .gz 拡張子を付けて保存されます (たとえば、*dump.log.gz*)。このファイルは、WinZip で開くことができます。
  - *ap\_name* はコアダンプがアップロードされる特定のアクセスポイントの名前であり、**all** は Lightweight モードに変換されたすべてのアクセスポイントです。
- ステップ 2** **save config** コマンドを入力して、変更を保存します。
-

## AP クラッシュ ログ情報の表示

コントローラがリブートまたはアップグレードすると常に、APクラッシュ ログ情報がコントローラから削除されます。コントローラをリブートまたはアップグレードする前に、APクラッシュ ログ情報のバックアップを作成することをお勧めします。

### AP クラッシュ ログ情報の表示 (GUI)

- [Management] > [Tech Support] > [AP Crash Log] を選択して、[AP Crash Logs] ページを開きます。

### AP クラッシュ ログ情報の表示 (CLI)

---

**ステップ 1** 次のコマンドを入力して、クラッシュファイルがコントローラにダウンロードされたことを確認します。  
**show ap crash-file**

以下に類似した情報が表示されます。

```
Local Core Files:
lrad_AP1130.rdump0 (156)
The number in parentheses indicates the size of the file. The size should be greater than zero if
a core dump file is available.
```

**ステップ 2** 次のコマンドを入力して、AP クラッシュ ログ ファイルのコンテンツを表示します。  
**show ap crash-file *Cisoc\_AP***

---

## 変換されたアクセス ポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ページには、コントローラにより変換されたアクセス ポイントのイーサネット MAC アドレスのリストが表示されます。
- [AP Detail] ページには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセス ポイントのリストが、コントローラにより無線 MAC アドレス順に表示されます。

## Lightweight モードに変換したアクセス ポイントの Reset ボタンの無効化

Lightweight モードに変換したアクセス ポイントの Reset ボタンを無効化できます。Reset ボタンは、アクセス ポイントの外面に MODE と書かれたラベルが付けられています。

次のコマンドを使用すると、あるコントローラにアソシエートしている変換されたアクセス ポイントの 1 つまたはすべての Reset ボタンを無効または有効にできます。

```
config ap rst-button {enable | disable} {ap-name}
```

変換されたアクセス ポイントの Reset ボタンは、デフォルトでは有効です。

## Lightweight アクセス ポイントでの固定 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。固定 IP アドレスは通常、ユーザ数の限られた導入でのみ使用されます。

固定 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバとアクセス ポイントが属するドメインを指定しない限り、アクセス ポイントはドメイン ネーム システム (DNS) 解決を使用してコントローラを検出できません。以前は、これらのパラメータは CLI を使用してのみ設定可能でしたが、コントローラ ソフトウェア リリース 6.0 以降のリリースではこの機能を GUI にも拡張しています。



- (注) アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォールバックします。アクセス ポイントが DHCP アドレスにフォールバックした場合は、**show ap config general Cisco\_AP** CLI コマンドを入力すると、アクセス ポイントがフォールバック IP アドレスを使用していることが表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバックアドレスであるとは識別しません。

## 固定 IP アドレスの設定 (GUI)

- 
- ステップ 1** [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2** 固定 IP アドレスを有効にするアクセス ポイントの名前をクリックします。[All APs>Details for] ([General]) ページが表示されます。
- ステップ 3** このアクセス ポイントに固定 IP アドレスを割り当てる場合は、[IP Config] で [Static IP] チェックボックスをオンにします。デフォルト値はオフです。
- ステップ 4** 対応するテキスト ボックスに固定 IP アドレス、ネットマスク、およびデフォルト ゲートウェイを入力します。
- ステップ 5** [Apply] をクリックして、変更を確定します。アクセス ポイントがリブートしてコントローラを再 join し、**ステップ 4** で指定した固定 IP アドレスがアクセス ポイントに送信されます。
- ステップ 6** 固定 IP アドレスがアクセス ポイントに送信された後は、次の手順で DNS サーバの IP アドレスおよびドメイン名を設定できます。
- [DNS IP Address] テキスト ボックスに、DNS サーバの IP アドレスを入力します。
  - [Domain Name] テキスト ボックスに、アクセス ポイントが属するドメイン名を入力します。
  - [Apply] をクリックして、変更を確定します。
  - [Save Configuration] をクリックして、変更を保存します。
- 

## 固定 IP アドレスの設定 (CLI)

- 
- ステップ 1** 次のコマンドを入力して、アクセス ポイントで固定 IP アドレスを設定します。
- ```
config ap static-ip enable Cisco_AP ip_address mask gateway
```
- (注) アクセス ポイントの固定 IP を無効にするには、**config ap static-ip disable Cisco_AP** コマンドを入力します。
- ステップ 2** **save config** コマンドを入力して、変更を保存します。
アクセス ポイントがリブートしてコントローラを再 join し、**ステップ 1** で指定した固定 IP アドレスがアクセス ポイントにプッシュされます。
- ステップ 3** 固定 IP アドレスがアクセス ポイントに送信された後は、次の手順で DNS サーバの IP アドレスおよびドメイン名を設定できます。
- DNS サーバを指定して特定のアクセス ポイントが DNS 解決を使用してコントローラをディスカバーできるようにするには、次のコマンドを入力します。
- ```
config ap static-ip add nameserver {Cisco_AP | all} ip_address
```
- (注) 特定のアクセス ポイントまたはすべてのアクセス ポイントの DNS サーバを削除するには、**config ap static-ip delete nameserver {Cisco\_AP | all}** コマンドを入力します。



- b) 特定のアクセスポイント、またはすべてのアクセスポイントが属するドメインを指定するには、次のコマンドを入力します。

```
config ap static-ip add domain {Cisco_AP|all} domain_name
```

(注) 特定のアクセスポイント、またはすべてのアクセスポイントのドメインを削除するには、**config ap static-ip delete domain** {Cisco\_AP|all} コマンドを入力します。

- c) **save config** コマンドを入力して、変更を保存します。

**ステップ 4** 次のコマンドを入力して、アクセスポイントの IP アドレス設定を表示します。

```
show ap config general Cisco_AP
```

以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 4
Cisco AP Name..... AP6
...
IP Address Configuration..... Static IP assigned
IP Address..... 10.10.10.118
IP NetMask..... 255.255.255.0
Gateway IP Addr..... 10.10.10.1

Domain..... Domain1
Name Server..... 10.10.10.205
...
```

## サイズの大きなアクセスポイントのイメージのサポート

コントローラソフトウェアリリース 5.0 以降のリリースでは、リカバリイメージを自動的に削除して十分なスペースをすることで、サイズの大きなアクセスポイントのイメージにアップグレードできます。

リカバリイメージによって、イメージのアップグレード時にアクセスポイントのパワーサイクリングを行っても使用できる、バックアップイメージが提供されます。アクセスポイントでリカバリの必要を避ける最善の方法は、システムのアップグレード時にアクセスポイントのパワーサイクリングを避けることです。サイズの大きなアクセスポイントイメージへのアップグレードの際にパワーサイクリングが発生した場合、TFTP リカバリの手順を使用してアクセスポイントを回復できます。

## アクセス ポイントの回復 : TFTP リカバリ手順の使用

- 
- ステップ 1** 必要なリカバリ イメージを Cisco.com (c1100-rcvk9w8-mx、c1200-rcvk9w8-mx、または c1310-rcvk9w8-mx) からダウンロードし、お使いの TFTP サーバのルート ディレクトリにインストールします。
- ステップ 2** TFTPサーバをターゲットのアクセス ポイントと同じサブネットに接続して、アクセス ポイントをパワー サイクリングします。アクセス ポイントは TFTP イメージから起動し、次にコントローラに join してサイズの大きなアクセス ポイントのイメージをダウンロードし、アップグレード手順を完了します。
- ステップ 3** アクセス ポイントが回復したら、TFTP サーバを削除できます。
-



# 第 113 章

## パケット キャプチャの設定

---

- [パケット キャプチャについて](#), 893 ページ
- [パケット キャプチャの制約事項](#), 894 ページ
- [パケット キャプチャの設定 \(CLI\)](#), 894 ページ

### パケット キャプチャについて

AP が正常に動作中に、ワイヤレス ネットワークにおける音声およびセキュリティなどの問題を解決するには、分析の AP からのパケットをダンプする必要がある場合があります。パケットが FTP サーバにダンプできます。分析用のパケットのダンプするこのプロセスは、パケット キャプチャと呼ばれます。クライアントのパケット キャプチャを開始または終了するためにコントローラを使用します。次のタイプのコントローラ CLI を使用して、キャプチャする必要のあるパケットのタイプを選択できます。

- 管理パケット
- 制御パケット
- データ パケット
  - Dot1X
  - ARP
  - IAPP
  - All IP
  - 一致するポート番号を持つ UDP
  - DHCP
  - 一致するポート番号を持つ TCP
  - マルチキャスト フレーム
  - ブロードキャスト フレーム

パケットは、ビーコンとプローブ応答を除き、パケットの到着順または送信順にキャプチャおよびダンプされます。パケットキャプチャには、チャンネル、RSSI、データレート、SNR およびタイムスタンプなどの情報が含まれています。各パケットは、APからの追加情報に付加されます。パケットヘッダーだけをダンプまたはパケットをフルダンプのいずれかを選択できます。

次に、パケットキャプチャの注意事項を示します。

- FTP転送時間がパケットレートより遅い場合、一部のパケットはキャプチャファイルに表示されません。
- バッファにパケットが含まれていない場合、接続を維持するために、既知のダミーパケットがダンプされます。
- ファイルは、一意のAPとコントローラ名とタイムスタンプに基づいて、各APのFTPサーバに作成されます。FTPサーバがAPによって到達可能であることを確認します。
- FTP転送が失敗した場合、またはFTP接続がパケットキャプチャ中に失われた場合、APは、パケットのキャプチャを止め、エラーメッセージおよびSNMPトラップによって通知し、新しいFTP接続が確立されます。

## パケットキャプチャの制約事項

- パケットキャプチャは、1つのクライアントに対してのみ有効にできます。
- コントローラ間ローミングには、この機能はサポートされていません。クライアントがローミングするAPまたはコントローラがわかる場合は、CLIを使用して、新しいコントローラのクライアント用のパケットキャプチャまたはAPを設定できます。
- 無線配信中にすべてのパケットがキャプチャされるわけではなく、無線ドライバに到達するものだけがキャプチャされます。
- デフォルトでは、パケットキャプチャの処理は10分後に停止します。ただし、パケットキャプチャを1～60分の範囲でいつでも停止するように設定できます。

## パケットキャプチャの設定 (CLI)

- 
- ステップ 1** 次のコマンドを入力して、パケットキャプチャ用にFTPパラメータを設定します。  
**config ap packet-dump ftp serverip ip-address path path username user\_ID password password**
- ステップ 2** 次のコマンドを入力して、パケットキャプチャを開始または停止します。  
**config ap packet-dump {start client-mac-address ap-name | stop}**
- ステップ 3** 次のコマンドを入力して、パケットキャプチャのバッファサイズを設定します。  
**config ap packet-dump buffer-size size-in-kb**
- ステップ 4** 次のコマンドを入力して、パケットキャプチャ時間を設定します。

```
config ap packet-dump capture-time time-in-minutes
```

有効な範囲は 1 ~ 60 分です。

**ステップ 5** 次のコマンドを入力して、キャプチャされるパケットのタイプを設定します。

```
config ap packet-dump classifier {arp | broadcast | control | data | dot1x | iapp | ip | management | multicast |
{tcp port port-number} | {udp port port-number}} {enable | disable}
```

**ステップ 6** 次のコマンドを入力して、切り捨て後のパケット長を設定します。

```
config ap packet-dump truncate length-in-bytes
```

**ステップ 7** 次のコマンドを入力して、パケットキャプチャの状態を確認します。

```
show ap packet-dump status
```

**ステップ 8** 次のコマンドを入力して、パケットキャプチャのデバッグを設定します。

```
debug ap packet-dump {enable | disable}
```

---





# 第 114 章

## OfficeExtend アクセス ポイントの設定

---

- [OfficeExtend アクセス ポイントについて, 897 ページ](#)
- [OEAP 600 シリーズ アクセス ポイント, 898 ページ](#)
- [セキュリティの実装, 908 ページ](#)
- [OfficeExtend アクセス ポイントのライセンスング, 908 ページ](#)
- [OfficeExtend アクセス ポイントの設定, 909 ページ](#)
- [OfficeExtend アクセス ポイントでの個人 SSID の設定, 915 ページ](#)
- [OfficeExtend アクセス ポイント統計情報の表示, 917 ページ](#)

### OfficeExtend アクセス ポイントについて

Cisco 600 シリーズ OfficeExtend アクセス ポイント (Cisco OEAP) はコントローラからリモートロケーションのアクセス ポイントへのセキュア通信を提供して、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホーム オフィスにおけるユーザの使用感は、会社のオフィスとまったく同じです。アクセス ポイントとコントローラの間での Datagram Transport Layer Security (DTLS; データグラム トランスポート層セキュリティ) による暗号化は、すべての通信のセキュリティを最高レベルにします。



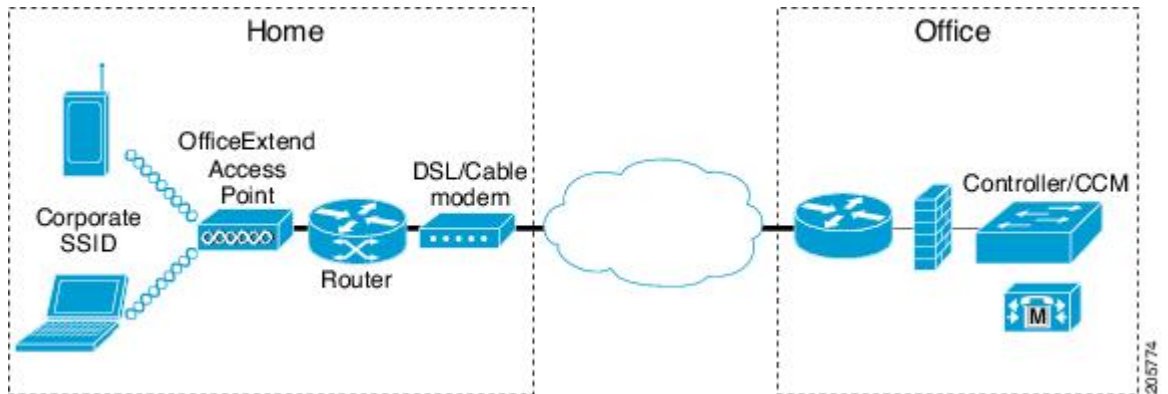
---

(注) DTLS は Cisco OEAP で永続的に有効です。このアクセス ポイントで、DTLS を無効にすることはできません。

---

次に、一般的な OfficeExtend アクセス ポイント セットアップを示します。

図 53: 一般的な OfficeExtend アクセス ポイント セットアップ



- (注) Cisco OEAP は、ルータまたはネットワーク アドレス変換 (NAT) を使用するその他のゲートウェイ デバイスの背後で動作するように設計されています。NAT により、ルータなどのデバイスはインターネット (パブリック) と個人ネットワーク (プライベート) 間のエージェントとして動作でき、コンピュータのグループ全体を単一の IP アドレスで表すことができます。NAT デバイスの背後に配置できる Cisco OEAP の数に制限はありません。ローミングは Cisco 600 OEAP モデルではサポートされていません。

現在、コントローラにアソシエートされている Cisco 1040、1130、1140、2602I、3502I、および 3600 シリーズ アクセス ポイントを、Cisco OEAP として動作するように設定できます。統合アンテナ対応のすべてのサポートされる AP モデルは OEAP として設定できます。

## OEAP 600 シリーズ アクセス ポイント

ここでは、Cisco 600 シリーズ OfficeExtend アクセス ポイントと一緒に使用するように、Cisco 無線 LAN コントローラを設定するための要件について詳しく説明します。600 シリーズ OfficeExtend アクセス ポイントは、スプリット モード動作をサポートしており、ローカル モードでの WLAN コントローラを介した設定を必要とします。ここでは、適切に接続するために必要な設定と、サポートされている機能セットについて説明します。



- (注) WLAN コントローラと 600 シリーズ OfficeExtend アクセス ポイントの間にあるファイアウォールで、CAPWAP UDP 5246 および 5247 が開いている必要があります。



- (注) マルチキャストは、Cisco 600 シリーズ OfficeExtend アクセス ポイントではサポートされません。



## ローカルモードの OEAP

600 シリーズ OfficeExtend アクセス ポイントは、ローカルモードでコントローラに接続します。これらの設定は変更できません。



(注) Monitor モード、FlexConnect モード、Sniffer モード、Rogue Detector、Bridge、および SE-Connect は、600 シリーズ OfficeExtend アクセス ポイントではサポートされておらず、設定することはできません。

図 54 : OEAP モード

General	Interfaces	High Availability	Inventory
<b>General</b>			
AP Name	Evora-OEAP		
Location	default location		
AP MAC Address	98:fc:11:8b:66:e0		
Base Radio MAC	00:22:bd:d9:fc:80		
Admin Status	Enable		
AP Mode	local		
AP Sub Mode	None		
Operational Status	REG		
Port Number	13		

## 600 シリーズ OfficeExtend アクセス ポイントに対してサポートされる WLAN の設定

600 シリーズ OfficeExtend アクセス ポイントでは、最大で 3 つの WLAN と 1 つのリモート LAN がサポートされます。ネットワーク導入に 4 つ以上の WLAN が存在する場合は、600 シリーズ OfficeExtend アクセス ポイントを AP グループに入れる必要があります。600 シリーズ OfficeExtend アクセス ポイントが AP グループに追加されると、3 つの WLAN と 1 つのリモート LAN に対する同一の制限が AP グループの設定に適用されます。

600 シリーズ OfficeExtend アクセス ポイントがデフォルトグループにある場合、つまり、定義された AP グループにない場合、WLAN/リモート LAN ID を ID 7 以下に設定する必要があります。

600 シリーズ OfficeExtend アクセス ポイントにより使用されている WLAN またはリモート LAN を変更する目的で、追加の WLAN またはリモート LAN を作成する場合は、新しい WLAN またはリモート LAN を 600 シリーズ OfficeExtend アクセス ポイントで有効にする前に、削除する現在の WLAN またはリモート LAN を無効にする必要があります。AP グループで複数のリモート LAN が有効にされている場合は、すべてのリモート LAN を無効にしてから 1 つのリモート LAN のみを有効にしてください。

AP グループで4つ以上の WLAN が有効にされている場合は、すべての WLAN を無効にしてから3つの WLAN のみを有効にしてください。

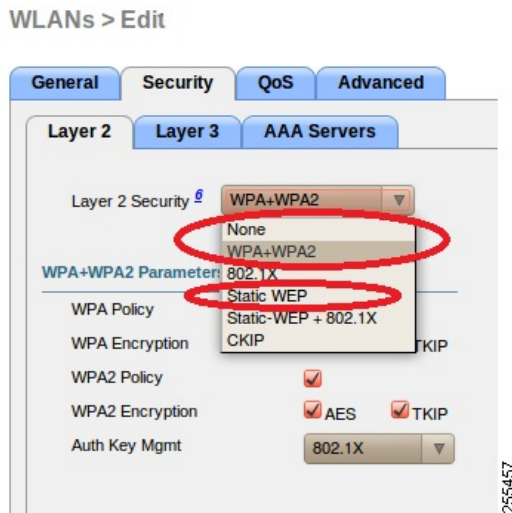
## 600 シリーズ OfficeExtend アクセス ポイントに対する WLAN のセキュリティ設定

WLAN でセキュリティを設定（次の図を参照）する際は、600 シリーズ OfficeExtend アクセス ポイントでサポートされていない特定の要素があることに注意してください。CCX は、600 シリーズ OfficeExtend アクセス ポイントではサポートされず、CCX に関連する要素もサポートされません。

レイヤ2セキュリティの場合、600 シリーズ OfficeExtend アクセス ポイントに対して次のオプションがサポートされます。

- None
- WPA+WPA2
- Static WEP
- 802.1X（リモート LAN の場合のみ）

図 55: WLAN レイヤ2セキュリティ設定



[Security] タブ (次の図を参照) では、WPA+WPA2 設定の [CCKM] を選択しないでください。802.1X または PSK のみを設定します。

図 56: WLAN のセキュリティ設定 - 認証キー管理

WLANs > Edit

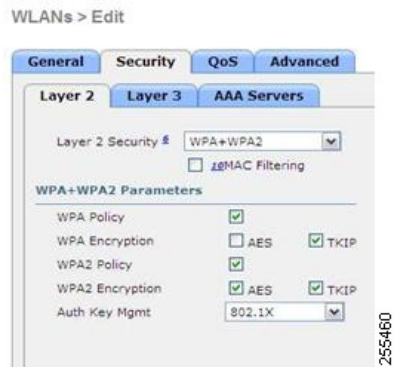
The screenshot shows the configuration page for a WLAN, specifically the Security tab. The 'Layer 2 Security' is set to 'WPA+WPA2'. Under 'WPA+WPA2 Parameters', the following options are checked: WPA Policy, WPA Encryption (AES and TKIP), WPA2 Policy, WPA2 Encryption (AES and TKIP), and Auth Key Mgmt. The 'Auth Key Mgmt' dropdown menu is open, showing the following options: 802.1X, 802.1X, CCKM, PSK, and 802.1X+CCKM. The first three options (802.1X, 802.1X, and CCKM) are circled in red.

TKIP および AES に対するセキュリティの暗号化設定は、WPA と WPA2 で同一であることが必要です。次に、TKIP と AES に対する非互換の設定例を示します。

図 57 : OEAP 600 シリーズに対する非互換の WPA および WPA2 セキュリティ暗号化設定



図 58 : OEAP 600 シリーズに対する非互換の WPA および WPA2 セキュリティ暗号化設定



次に、互換性のある設定例を示します。

図 59 : OEAP シリーズに対する互換性のあるセキュリティ設定



図 60 : OEAP シリーズに対する互換性のあるセキュリティ設定



QoS 設定はサポートされています（次の図を参照）が、CAC 設定はサポートされていないため、有効にしないでください。



(注) カバレッジ ホールの検出は有効にしないでください。



(注) Aironet IE は有効にしないでください。このオプションはサポートされていません。

図 61 : OEAP 600 に対する QoS の設定

WLANs > Edit

DTIM Period (in beacon interval)	Value
802.11a/n (1 - 255)	1
802.11b/g/n (1 - 255)	1

MFP もサポートされていないので、無効にするか、[Optional] に設定してください。

図 62 : OEAP シリーズ アクセス ポイントに対する MFP の設定

WLANs > Edit

DTIM Period (in beacon interval)	Value
802.11a/n (1 - 255)	1
802.11b/g/n (1 - 255)	1

クライアント ロード バランシング および クライアント 帯域の選択はサポートされていません。

## 認証の設定

600 シリーズ OfficeExtend アクセス ポイントの認証の場合、LEAP はサポートされません。この設定については、EAP-Fast、EAP-TTLS、EAP-TLS、または PEAP に移行するように、クライアント および RADIUS サーバで対処する必要があります。

コントローラでローカル EAP が使用されている場合も、LEAP が使用されないように設定を変更する必要があります。

## 600 シリーズ OfficeExtend アクセス ポイントでサポートされるユーザ カウント

一度に 15 のユーザだけが Cisco 600 シリーズ OEAP で提供される WLAN に接続できます。クライアントのいずれかが認証を解除されるか、コントローラのタイムアウトが発生するまで、16 番目のユーザは認証できません。この数は、600 シリーズ OfficeExtend アクセス ポイントでのコントローラ WLAN における累積数です。

たとえば、2 つのコントローラ WLAN が設定されており、1 つの WLAN に 15 ユーザが接続している場合、600 シリーズ OfficeExtend アクセス ポイントでは同時にもう 1 つの WLAN に別のユーザが join することができません。

この制限は、エンドユーザが 600 シリーズ OfficeExtend アクセス ポイントで個人用に設定するローカルプライベート WLAN には適用されません。これらのプライベート WLAN または有線ポートで接続されるクライアントは、これらの制限に影響しません。



(注) この制限は、OfficeExtend モードで動作する他の AP モデルには適用されません。

## リモート LAN の設定

600 シリーズ OfficeExtend アクセス ポイントでは、リモート LAN ポートを介して 4 つのクライアントのみ接続できます。この接続クライアントの数は、コントローラ WLAN でのユーザ制限数 (15) には影響しません。リモート LAN のクライアント制限では、リモート LAN ポートにスイッチまたはハブを接続して複数のデバイスを接続することや、このポートに接続している Cisco IP 電話に直接接続することは可能です。接続できるデバイスは 4 つまでです。これは、この 4 つのデバイスの 1 つのアイドル時間が 1 分を超えるまで適用されます。

リモート LAN は、コントローラでの WLAN またはゲスト LAN の設定と同様に設定されます。

図 63: OEAP 600 シリーズ AP に対するリモート LAN の設定

### WLANs > New

Type	WLAN
Profile Name	WLAN
SSID	Remote LAN
ID	4

255468

[Security] 設定を開いたままにし、MAC フィルタリングまたは Web 認証を設定することができます。デフォルトでは MAC フィルタリングが使用されます。さらに、802.1X レイヤ 2 セキュリティ設定を指定することもできます。

図 64: リモート LAN の OEAP 600 シリーズ AP に対するレイヤ 2 セキュリティ設定



図 65: リモート LAN の OEAP 600 シリーズ AP に対するレイヤ 3 セキュリティ設定



## チャネルの管理と設定

600 シリーズ OfficeExtend アクセス ポイントの無線は、無線 LAN コントローラではなく、そのアクセス ポイントのローカル GUI で管理されます。スペクトラム チャネルまたは電力の管理や、無線の無効化をコントローラから実行しても、600 シリーズ OfficeExtend アクセス ポイントには反映されません。RRM は、600 シリーズ OfficeExtend アクセス ポイントではサポートされません。

ローカル GUI で 2.4 GHz および 5.0 GHz の両方のデフォルト設定を変更していない限り、600 シリーズは起動時にチャネルをスキャンし、2.4 GHz および 5 GHz のチャネルを選択します。

図 66: OEAP 600 シリーズ AP のチャネル選択





20 MHz または 40 MHz のワイドチャネルについても、600 シリーズ OfficeExtend アクセス ポイントのローカル GUI で 5.0 GHz 用のチャネル帯域幅が設定されます。2.4 GHz のチャネル幅を 40 MHz に設定することはできず、20 MHz に固定されます。

図 67: OEAP 600 AP のチャネル幅



## その他の注意事項

- Cisco 600 シリーズ OfficeExtend アクセス ポイント (OEAP) は、単一の AP 導入向けに設計されているので、Cisco 600 シリーズ OEAP 間のクライアント ローミングはサポートされません。  
コントローラで 802.11a/n/ac または 802.11b/g/n を無効にしても、ローカル SSID がまだ有効であるために、Cisco 600 シリーズ OEAP ではこれらのスペクトラムが無効にならない場合があります。
- ファイアウォールは、アクセス ポイントからの CAPWAP を使用するトラフィックを許可するよう設定されている必要があります。UDP ポート 5246 および 5247 が有効であり、アクセス ポイントがコントローラに join できないようにする可能性のある中間デバイスによりブロックされていないことを確認してください。
- OEAP モードに変換され、ローカルでスイッチされる WLAN にマッピングされる 3500、3600、1260、2600、1040 など AP は、AP 接続スイッチのローカルサブネット上に DHCP 要求を転送します。この状態を回避するには、ローカルスイッチングとローカル認証を無効にする必要があります。
- Cisco 仮想ワイヤレス LAN コントローラに関連付ける Cisco 600 シリーズ OEAP の場合は、次の手順を実行します。
  - 1 7.5 以降のリリースを使用する物理コントローラに関連付ける OEAP を設定して、対応する AP イメージをダウンロードします。
  - 2 OEAP が物理コントローラに再び関連付けないように OEAP を設定します。たとえば、ネットワークに ACL を実装して、OEAP と物理コントローラ間の CAPWAP をブロックできます。
  - 3 Cisco 仮想ワイヤレス LAN コントローラに関連付ける OEAP を設定します。

## セキュリティの実装



(注) LSC の設定は要件ではなく、オプションです。OfficeExtend 600 アクセス ポイントは、LSC をサポートしません。

- 1 「LSC を使用したアクセス ポイントの許可」の手順に従って、Local Significant Certificates (LSC) を使用して OfficeExtend アクセス ポイントを許可します。
- 2 次のコマンドを入力して、アクセス ポイントの MAC アドレス、名前、または両方を許可要求のユーザ名で使用して AAA サーバ検証を実装します。

```
config auth-list ap-policy authorize-ap username {ap_mac | Cisco_AP | both}
```

検証にアクセス ポイント名を使用すると、有効な従業員の OfficeExtend アクセス ポイントのみをコントローラに関連付けることができます。このセキュリティポリシーを実装するには、各 OfficeExtend アクセス ポイントに、従業員の ID または番号で名前を付けます。従業員が離職した場合は、AAA サーバデータベースからこのユーザを削除するスクリプトを実行して、その従業員の OfficeExtend アクセス ポイントがネットワークに join できないようにします。

- 3 次のコマンドを入力して、変更を保存します。

```
save config
```



(注) CCX は、600 OEAP ではサポートされません。CCX に関連する要素はサポートされません。また、802.1X または PSK のみがサポートされます。TKIP および AES セキュリティ暗号化の設定は、WPA と WPA2 で同一であることが必要です。

## OfficeExtend アクセス ポイントのライセンスング

OfficeExtend アクセス ポイントを使用するには、コントローラに基本ライセンスがインストールされ、使用されている必要があります。ライセンスのインストール後、次の AP モデルの OfficeExtend モードを有効にすることができます。

- 1130
- 1240
- 1040
- 1140
- 1250
- 1260
- 1600

- 2600
- 3500 (統合アンテナ) シリーズ
- 3600 (統合アンテナ) シリーズ

## OfficeExtend アクセスポイントの設定

1130 シリーズ、1140 シリーズ、1040 シリーズ、3500 (統合アンテナ) シリーズ、または 3600 (統合アンテナ) シリーズ アクセスポイントがコントローラに join した後は、OfficeExtend アクセスポイントとして設定できます。

### OfficeExtend アクセスポイントの設定 (GUI)

- 
- ステップ 1** [Wireless] を選択して、[All APs] ページを開きます。
- ステップ 2** 目的のアクセスポイントの名前をクリックして、[All APs > Details] ページを開きます。
- ステップ 3** 次の手順で、アクセスポイントに対して FlexConnect を有効にします。
- a) [General] タブで、[AP Mode] ドロップダウンリストから [FlexConnect] を選択し、このアクセスポイントに対して FlexConnect を有効にします。
- ステップ 4** 次の手順で、アクセスポイントに 1 つまたは複数のコントローラを設定します。
- a) [High Availability] タブをクリックします
  - b) このアクセスポイントのプライマリ コントローラの名前と IP アドレスを [Primary Controller Name] テキストボックスおよび [Management IP Address] テキストボックスに入力します。  
(注) コントローラの名前および IP アドレスの両方を入力する必要があります。入力しないと、アクセスポイントはコントローラに join できません。
  - c) 必要に応じて、セカンダリまたはターシャリ コントローラ (または両方) の名前および IP アドレスを、対応する [Controller Name] テキストボックスおよび [Management IP Address] テキストボックスに入力します。
  - d) [Apply] をクリックします。アクセスポイントはリブートしてからコントローラに再 join します。  
(注) プライマリ、セカンダリ、およびターシャリ コントローラの名前および IP アドレスは一意である必要があります。
- ステップ 5** 次の手順で、OfficeExtend アクセスポイントの設定を有効にします。
- a) [FlexConnect] タブをクリックします。
  - b) [Enable OfficeExtend AP] チェックボックスをオンにして、このアクセスポイントの OfficeExtend モードを有効にします。デフォルト値はオンです。  
このチェックボックスをオフにすると、このアクセスポイントの OfficeExtend モードが無効になります。アクセスポイントの設定すべてが取り消されることはありません。アクセスポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、コントローラ CLI で **clear ap config Cisco\_AP** と入力します。アクセスポイントの個人の SSID のみをクリアする場合は、[Reset Personal SSID] をクリックします。

- (注) アクセスポイントに対して OfficeExtend モードを有効にした場合は、不正なアクセスポイントの検出が自動的に無効になります。ただし、[All APs > Details for] ([Advanced]) ページで [Rogue Detection] チェックボックスをオンまたはオフにして、特定のアクセスポイントの不正検出を有効または無効にできます。家庭の環境で展開されるアクセスポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセスポイントでは不正検出はデフォルトでは無効です。
- (注) アクセスポイントに対して OfficeExtend モードを有効にした場合は、DTLS データ暗号化が自動的に有効になります。ただし、[All APs > Details for] ([Advanced]) ページで [Data Encryption] チェックボックスをオンまたはオフにして、特定のアクセスポイントの DTLS データ暗号化を有効または無効にできます。
- (注) アクセスポイントに対して OfficeExtend モードを有効にした場合は、Telnet および SSH アクセスが自動的に無効になります。ただし、[All APs > Details for] ([Advanced]) ページで [Telnet] チェックボックスまたは [SSH] チェックボックスをオンまたはオフにして、特定のアクセスポイントの Telnet アクセスまたは SSH アクセスを有効または無効にできます。
- (注) アクセスポイントに対して OfficeExtend モードを有効にした場合は、リンク遅延が自動的に有効になります。ただし、[All APs > Details for] ([Advanced]) ページで [Enable Link Latency] チェックボックスをオンまたはオフにして、特定のアクセスポイントのリンク遅延を有効または無効にできます。

- c) join 時にアクセスポイントに遅延の最も少ないコントローラを選択させたい場合は、[Enable Least Latency Controller Join] チェックボックスをオンにします。有効にしない場合は、このチェックボックスをオフのままにします (デフォルト値)。この機能を有効にすると、アクセスポイントは discovery request と discovery response の間の時間を計算し、最初に応答した Cisco 5500 シリーズコントローラに join します。
- d) [Apply] をクリックします。  
[All APs] ページの [OfficeExtend AP] テキストボックスには、どのアクセスポイントが OfficeExtend アクセスポイントとして設定されているかが表示されます。

**ステップ 6** OfficeExtend アクセスポイントに特定のユーザ名とパスワードを設定して、ホームユーザが OfficeExtend アクセスポイントの GUI にログインできるようにします。

- a) [Credentials] タブをクリックします。
- b) [Override Global Credentials] チェックボックスをオンにし、このアクセスポイントがコントローラからグローバルユーザ名、パスワード、enable パスワードを継承しないようにします。デフォルト値はオフです。
- c) [Username]、[Password]、および [Enable Password] テキストボックスに、このアクセスポイントに割り当てる独自のユーザ名、パスワード、およびイネーブルパスワードを入力します。
  - (注) 入力した情報は、コントローラやアクセスポイントをリブートした後や、アクセスポイントが新しいコントローラに join された場合でも保持されます。
- d) [Apply] をクリックします。
  - (注) このアクセスポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、[Over-ride Global Credentials] チェックボックスをオフにします。

**ステップ 7** OfficeExtend アクセスポイントのローカル GUI、LAN ポート、およびローカル SSID へのアクセスを設定します。

- a) [WIRELESS] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。
- b) [OEAP Config Parameters] の下の [Disable Local Access] チェックボックスをオンまたはオフにして、OfficeExtend アクセスポイントのローカルアクセスを有効または無効にします。  
 (注) デフォルトでは、[Disable Local Access] チェックボックスはオフになるので、イーサネットポートおよび個人の SSID が有効になります。この設定は、リモート LAN に影響しません。ポートは、リモート LAN を設定する場合のみ有効になります。

**ステップ 8** 次のように、OfficeExtend アクセスポイントのスプリット トンネリングを設定します。

- a) [Wireless] > [Access Points] > [Global Configuration] を選択します。
- b) [OEAP Config Parameters] 領域で、[Disable Split Tunnel] チェックボックスをオンまたはオフにします。ここでスプリット トンネリングを無効にすると、すべての WLAN およびリモート LAN のスプリット トンネリングが無効になります。特定の WLAN またはリモート LAN のスプリット トンネリングを無効にすることもできます。
- c) [Apply] をクリックします。

**ステップ 9** [Save Configuration] をクリックします。

**ステップ 10** コントローラが OfficeExtend アクセスポイントのみをサポートする場合は、「RRM の設定」の項で、DCA 間隔、チャンネル スキャン間隔、およびネイバー パケット間隔に推奨される値を設定する手順を参照してください。

## OfficeExtend アクセスポイントの設定 (CLI)

- 次のコマンドを入力して、アクセスポイントで FlexConnect を有効にします。  
**config ap mode flexconnect Cisco\_AP**
- アクセスポイントに 1 つまたは複数のコントローラを設定するには、次のいずれか、またはすべてのコマンドを入力します。  
**config ap primary-base controller\_name Cisco\_AP controller\_ip\_address**  
**config ap secondary-base controller\_name Cisco\_AP controller\_ip\_address**  
**config ap tertiary-base controller\_name Cisco\_AP controller\_ip\_address**



- (注) コントローラの名前および IP アドレスの両方を入力する必要があります。入力しないと、アクセスポイントはコントローラに join できません。



(注) プライマリ、セカンダリ、およびターシャリ コントローラの名前および IP アドレスは一意である必要があります。

- 次のコマンドを入力して、このアクセス ポイントで OfficeExtend モードを有効にします。  
**config flexconnect office-extend {enable | disable} Cisco\_AP**

デフォルト値はイネーブルです。 **disable** パラメータは、このアクセス ポイントの OfficeExtend モードを無効にします。アクセス ポイントの設定すべてが取り消されることはありません。アクセス ポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、次のコマンドを入力します。

**clear ap config cisco-ap**

アクセス ポイントの個人の SSID のみをクリアする場合は、次のコマンドを入力します。

**config flexconnect office-extend clear-personalssid-config Cisco\_AP**



(注) アクセス ポイントに対して OfficeExtend モードを有効にした場合は、不正なアクセス ポイントの検出が自動的に無効になります。ただし、 **config rogue detection {enable | disable} {Cisco\_AP | all}** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの不正検出を有効または無効にできます。家庭の環境で展開されるアクセス ポイントは大量の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出はデフォルトでは無効です。



(注) アクセス ポイントに対して OfficeExtend モードを有効にした場合は、DTLS データ暗号化が自動的に有効になります。ただし、 **config ap link-encryption {enable | disable} {Cisco\_AP | all}** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効または無効にできます。



(注) アクセス ポイントに対して OfficeExtend モードを有効にした場合は、Telnet および SSH アクセスが自動的に無効になります。ただし、 **config ap {telnet | ssh} {enable | disable} Cisco\_AP** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの Telnet または SSH アクセスを有効または無効にできます。



(注) アクセス ポイントに対して OfficeExtend モードを有効にした場合は、リンク遅延が自動的に有効になります。ただし、 **config ap link-latency {enable | disable} {Cisco\_AP | all}** コマンドを使用して、コントローラに現在アソシエートされている特定のアクセス ポイントまたはすべてのアクセス ポイントのリンク遅延を有効または無効にできます。

- 次のコマンドを入力して、join 時にアクセス ポイントが遅延の最も少ないコントローラを選択できるようにします。

**config flexconnect join min-latency {enable | disable} Cisco\_AP**

デフォルト値はディセーブルです。この機能を有効にすると、アクセス ポイントは discovery request と discovery response の間の時間を計算し、最初に応答した Cisco 5500 シリーズ コントローラに join します。

- 次のコマンドを入力して、ホーム ユーザが OfficeExtend アクセス ポイントの GUI にログインするために入力できる特定のユーザ名とパスワードを設定します。

**config ap mgmtuser add username user password password enablesecret enable\_password Cisco\_AP**

このコマンドに入力した資格情報は、コントローラやアクセス ポイントをリブートした後や、アクセス ポイントが新しいコントローラに join された場合でも保持されます。



(注) このアクセス ポイントで、コントローラのグローバル資格情報を強制的に使用する必要がある場合は、**config ap mgmtuser delete Cisco\_AP** コマンドを入力します。このコマンドの実行後、「AP reverted to global username configuration」というメッセージが表示されます。

- Cisco 600 シリーズ OfficeExtend アクセス ポイントにローカル ネットワークへのアクセスを設定するには、次のコマンドを入力します。

**config network ocap-600 local-network {enable | disable}**

無効の場合は、ローカル SSID、ローカル ポートが機能せず、コンソールにアクセスできません。リセットすると、デフォルトによってローカル アクセスが復元されます。アクセス ポイントに設定する場合、この設定はリモート LAN 設定に影響しません。

- 次のコマンドを入力して、Cisco 600 シリーズ OfficeExtend アクセス ポイントのイーサネット ポート 3 がリモート LAN として動作できるようにする、デュアル R-LAN ポート機能を設定します。

**config network ocap-600 dual-rlan-ports {enable | disable}**

この設定は、コントローラに対してグローバルであり、AP および NVRAM 変数によって保存されます。この変数が設定されていると、リモート LAN の動作が変わります。この機能は、リモート LAN ポートごとに異なるリモート LAN をサポートします。

リモート LAN マッピングは、デフォルト グループが使用されているか、または AP グループが使用されているかによって、次のように異なります。

- デフォルト グループ：デフォルト グループを使用している場合、偶数のリモート LAN ID を持つ単一のリモート LAN がポート 4 にマッピングされます。たとえば、リモート LAN ID 2 のリモート LAN は、ポート 4 (Cisco 600 OEAP 上) にマッピングされます。奇数のリモート LAN ID を持つリモート LAN は、ポート 3 (Cisco 600 OEAP 上) にマッピングされます。たとえば、リモート LAN ID 1 のリモート LAN は、ポート 3 (Cisco 600 OEAP 上) にマッピングされます。
- AP グループ：AP グループを使用する場合、OEAP-600 ポートへのマッピングは AP グループの順序によって決定します。AP グループを使用するには、まず、AP グループからすべてのリモート LAN および WLAN を削除して、空にする必要があります。次

に、2つのリモート LAN を AP グループに追加します。最初にポート 3 AP リモート LAN を追加してから、ポート 4 リモート グループを追加し、続けて WLAN を追加します。

- 次のコマンドを入力して、スプリット トンネリングを有効または無効にします。  
**config network oeap-600 split-tunnel {enable | disable}**  
ここでスプリット トンネリングを無効にすると、すべての WLAN およびリモート LAN のスプリット トンネリングが無効になります。特定の WLAN またはリモート LAN のスプリット トンネリングを無効にすることもできます。
- 次のコマンドを入力して、変更を保存します。  
**save config**



(注) コントローラが OfficeExtend アクセス ポイントのみをサポートする場合は、「無線リソース管理の設定」の項で、DCA 間隔に推奨される値を設定する手順を参照してください。

## WLAN またはリモート LAN のスプリット トンネリングの設定

### WLAN またはリモート LAN のスプリット トンネリングの設定 (GUI)

- 
- ステップ 1** [WLANs] を選択し、[WLAN ID] をクリックして、[WLANs > Edit] ページを開きます。選択する WLAN はその設定によって WLAN またはリモート LAN を指定できます。
- ステップ 2** [Advanced] タブをクリックします。
- ステップ 3** [OEAP] 領域で、[Split Tunnel] チェックボックスをオンまたはオフにします。
- ステップ 4** [Apply] をクリックします。
- ステップ 5** [Save Configuration] をクリックします。
- 

### WLAN またはリモート LAN のスプリット トンネリングの設定 (CLI)

- 次のコマンドを入力して、WLAN のスプリット トンネリングを有効または無効にします。  
**config wlan split-tunnel wlan-id {enable | disable}**
- 次のコマンドを入力して、WLAN のスプリット トンネリングのステータスを表示します。  
**show wlan wlan-id**
- 次のコマンドを入力して、リモート LAN のスプリット トンネリングを有効または無効にします。  
**config remote-lan split-tunnel rlan-id {enable | disable}**



- 次のコマンドを入力して、リモート LAN のスプリット トンネリングのステータスを表示します。

```
show remote-lan rlan-id
```

## OfficeExtend アクセス ポイントでの個人 SSID の設定

**ステップ 1** 次のいずれかの手順で、OfficeExtend アクセス ポイントの IP アドレスを確認します。

- ホーム ルータにログインして OfficeExtend アクセス ポイントの IP アドレスを見つけます。
- 会社の IT 担当に OfficeExtend アクセス ポイントの IP アドレスを確認します。
- Network Magic などのアプリケーションを使用して、ネットワーク上のデバイスおよびデバイスの IP アドレスを検出します。

**ステップ 2** OfficeExtend アクセス ポイントがホーム ルータに接続された状態で、インターネット ブラウザの [Address] テキスト ボックスに OfficeExtend アクセス ポイントの IP アドレスを入力して [Go] をクリックします。

(注) バーチャルプライベート ネットワーク (VPN) 接続を使用して会社のネットワークに接続していないことを確認してください。

**ステップ 3** プロンプトが表示されたら、ユーザ名とパスワードを入力してアクセス ポイントにログインします。

**ステップ 4** [OfficeExtend Access Point Welcome] ページで、[Enter] をクリックします。OfficeExtend アクセス ポイントの [Home] ページが表示されます。

図 68 : OfficeExtend アクセス ポイントの [Home] ページ

The screenshot shows the Cisco OfficeExtend Access Point Home page. The page has a navigation bar with 'HOME', 'CONFIGURATION', 'EVENT LOG', and 'HELP'. The main content is divided into three sections: 'General Information', 'AP Statistics', and 'Association'.

**General Information**

AP Name	AP1	AP MAC Address	0022.9090.8f4e
AP IP Address	209.165.200.225	AP Uptime	1 day, 19 hours, 17 minutes
AP Mode	Remote	AP Status (Admin/Operational)	ADMIN_ENABLED/UP
AP Version	12.4(20090119:051918)	Software Version	6.0.75.0
Controller Name	5500		

**AP Statistics**

Radio	Freq/Channel	Tx Power	Pkts In/Out	Bytes In/Out
Radio0-802.11N <sup>2.4</sup> GHz	2437 MHz/6	-20 dBm	459874/50945734	223261/206709119
Radio1-802.11N <sup>5</sup> GHz	5320 MHz/64	-17 dBm	386601/37115856	630268/511013585

**Association**

To remove 'Local Wireless Connection' association or modify settings, click on [Configuration](#).

Client MAC	Client IP/Name	Pkts In/Out	Bytes In/Out	Duplicates Rcvd/Data Retries	Decrypt Failed/RTS Retries
001c.58cd.3e13	0.0.0.0/NONE	1142/916	79751/52378	0/2	0/0

このページには、アクセスポイント名、IPアドレス、MACアドレス、ソフトウェアバージョン、ステータス、チャンネル、送信電力、およびクライアントトラフィックが表示されます。

ステップ 5 [Configuration] を選択して、[Configuration] ページを開きます。

図 69 : OfficeExtend アクセス ポイントの [Configuration] ページ

- ステップ 6 [Personal SSID] チェックボックスをオンにして、このワイヤレス接続を有効にします。デフォルト値はディセーブルです。
- ステップ 7 [SSID] テキスト ボックスに、このアクセス ポイントに割り当てる個人の SSID を入力します。この SSID は、ローカルにスイッチされます。  
 (注) OfficeExtend アクセス ポイントを持つコントローラは、接続されたアクセス ポイントあたり 15 までの WLAN にのみ公開します。これは、個人の SSID ごとに WLAN を 1 つ確保するためです。
- ステップ 8 [Security] ドロップダウン リストから [Open]、[WPA2/PSK (AES)]、または [104 bit WEP] を選択して、このアクセス ポイントが使用するセキュリティ タイプを設定します。  
 (注) [WPA2/PSK (AES)] を選択する場合は、クライアントに WPA2/PSK および AES 暗号化が設定されていることを確認してください。
- ステップ 9 ステップ 8 で [WPA2/PSK (AES)] を選択した場合は、[Secret] テキスト ボックスに 8 ~ 38 文字の WPA2 パスフレーズを入力します。104 ビット WEP を選択した場合、[Key] テキスト ボックスに 13 文字の ASCII キーを入力します。
- ステップ 10 [Apply] をクリックします。  
 (注) 他のアプリケーションで OfficeExtend アクセス ポイントを使用する場合は、[Clear Config] をクリックしてこの設定をクリアし、アクセス ポイントを工場出荷時のデフォルトに戻せます。コントローラ CLI から **clear ap config Cisco\_AP** コマンドを入力してアクセス ポイントの設定をクリアすることもできます。

## OfficeExtend アクセス ポイント統計情報の表示

次の CLI コマンドを使用して、ネットワーク上の OfficeExtend アクセス ポイントの情報を表示します。

- 次のコマンドを入力して、すべての OfficeExtend アクセス ポイントのリストを表示します。

**show flexconnect office-extend summary**

- 次のコマンドを入力して、OfficeExtend アクセス ポイントのリンク遅延を表示します。

**show flexconnect office-extend latency**

- 次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントの暗号化状態を表示します。

**show ap link-encryption {all | Cisco\_AP}**

このコマンドにより、整合性チェックのエラー数を追跡する認証エラー、およびアクセス ポイントが同じパケットを受信する回数を追跡する再送エラーも表示されます。次のコマンドを入力して、すべてのアクセス ポイントまたは特定のアクセス ポイントのデータ プレーンステータスを表示します。

**show ap data-plane {all | Cisco\_AP}**





## 第 115 章

# 設定の Cisco 700 シリーズ アクセス ポイント

- [Cisco 700 シリーズ アクセス ポイントに関する情報, 919 ページ](#)
- [設定の Cisco 700 シリーズ アクセス ポイント, 919 ページ](#)

## Cisco 700 シリーズ アクセス ポイントに関する情報

The Cisco Aironet 700 シリーズは、コンパクトなアクセス ポイントで、安全で信頼性の高いワイヤレス接続を提供します。主な特徴：

- 2.4 GHz と 5 GHz に対応した同時デュアルバンド、デュアル無線。
- 最適化されたアンテナおよび無線設計：レート対範囲を最適化するための一貫性のあるネットワーク送受信。
- 無線リソース管理（RRM）：自動自己回復機能により、RF の予測不可能性が最適化され、デッドスポットが減少し、ハイアベイラビリティクライアントの接続が保護されます。
- Cisco BandSelect が混合クライアント環境における 5 GHz クライアント接続を強化します。
- 不正検出、wIPS、コンテキスト認識などの高度なセキュリティ機能。

## 設定の Cisco 700 シリーズ アクセス ポイント

Cisco 700 シリーズ アクセス ポイントには 4 つの LAN ポートがあります。これらのポートの設定はフラッシュ上のファイルに保存されます。AP は再起動時にこの設定を取得します。AP は join 後にこの情報をコントローラと共有し、コントローラに最新情報が表示されるようにします。



(注) コントローラが AP 上の既存の設定をすべて消去すると、AP は保存されたポート情報を削除して、デフォルト設定を適用します。すべての LAN ポートがデフォルトで無効になっています。

## LAN ポートの有効化 (CLI)

- 次のコマンドを入力して、アクセス ポイントの LAN ポートを有効または無効にします。  
**config ap lan port-id***port-id* {enable | disable} *AP-NAME*
- 次のコマンドを入力して、ポート情報を表示します。  
**showaplanport-id***port-id**AP-NAME*
- 次のコマンドを入力して、ポートの要約情報を表示します。  
**showaplanport-summary***AP-NAME*

### 702W LAN ポートの有効化

リリース 7.6 では、イーサネット ポートの管理またはそれらの別々の VLAN への割り当てはサポートされません。すべてのポートが、AP のスイッチ ポートが設定されている同じアクセス VLAN にマッピングされます。または、ポートがトランクの場合は、ネイティブ VLAN にマッピングされます。リリース 8.0 以降は、ポートを有効または無効にして、必要に応じてそれらを特定の VLAN にマッピングできます。これにより、トラフィックを無線ネットワークと有線ネットワーク間だけでなく、4 つのイーサネット ポート間でも分離することができます。

- 
- ステップ 1** 次のコマンドを入力して、アクセス ポイントの LAN ポートを有効または無効にします。  
**configaplanport-id***port-id* {enable| disable} *AP-NAME*
- ステップ 2** 次のコマンドを入力して、ポート ID を設定します。  
**Configaplanport-id***port-id**AP-NAME*
- ステップ 3** 次のコマンドを入力して、アクセス VLAN を有効にします。  
**Configaplanenableaccessvlan***vlan-id*
- ステップ 4** 次のコマンドを入力して、VLAN のポート ID を有効にします。  
**Configaplanenableaccessvlanport-id**
- ステップ 5** 次のコマンドを入力して、AP の VLAN を設定します。  
**Configaplanenableaccessvlanvlan-idport-id***Cisco AP*
-



# 第 116 章

## Cisco ワークグループブリッジの使用

---

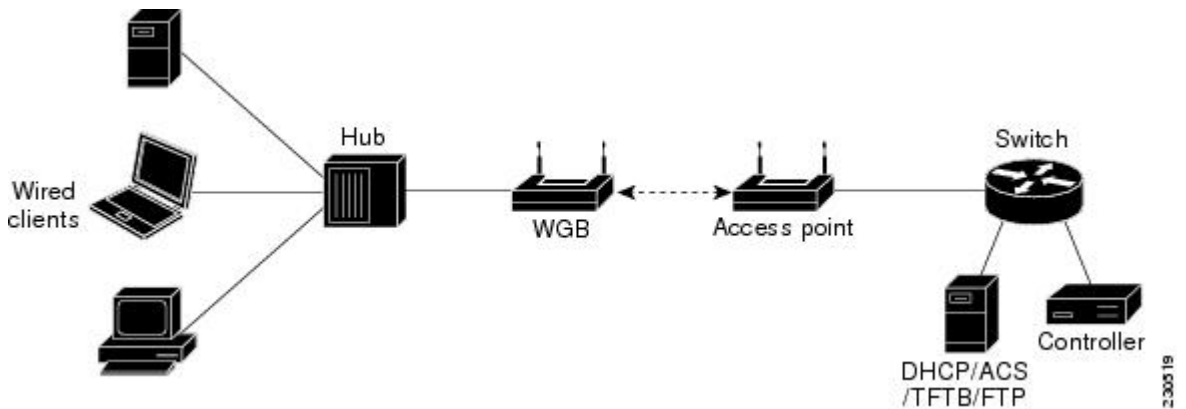
- [Cisco ワークグループブリッジについて, 921 ページ](#)
- [Cisco ワークグループブリッジの制約事項, 923 ページ](#)
- [WGB の設定例, 925 ページ](#)
- [ワークグループブリッジのステータスの表示 \(GUI\) , 925 ページ](#)
- [ワークグループブリッジのステータスの表示 \(CLI\) , 926 ページ](#)
- [WGB の問題のデバッグ \(CLI\) , 926 ページ](#)

### Cisco ワークグループブリッジについて

ワークグループブリッジ (WGB) は、Autonomous IOS アクセス ポイント上で設定でき、イーサネットに WGB アクセス ポイントに接続されたクライアントの代わりに Lightweight アクセス ポイントに無線で接続を提供するモードです。イーサネットインターフェイス上の有線クライアントの MAC アドレスを記憶し、それを Internet Access Point Protocol (IAPP) メッセージングを使用して Lightweight アクセス ポイントに報告することで、WGB は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。WGB は、単一の無線接続を Lightweight アクセス ポイントに確立して、有線クライアントに無線で接続できるようになります。Lightweight アクセス ポイントは、WGB をワイヤレスクライアントとして処理します。

Cisco IOS 15.2 以降のリリースを使用する WGB としての Cisco IOS AP は、コントローラを使用する保護拡張認証プロトコル (PEAP) をサポートします。

図 70 : WGB の例



(注) Lightweight アクセス ポイントが機能しない場合には、WGB は別のアクセス ポイントへのアソシエーションを試行します。

次に、Cisco ワークグループブリッジに関する注意事項を示します。

- ワークグループブリッジモードをサポートし、Cisco IOS Release 12.4 (3g) JA 以降のリリース (32 MB のアクセス ポイント上) または Cisco IOS Release 12.3 (8) JEB 以降のリリース (16 MB のアクセス ポイント上) を稼働している自律アクセス ポイントであれば、WGB を構成できます。これらのアクセス ポイントには、AP1120、AP1121、AP1130、AP1231、AP1240、および AP1310 が含まれます。12.4 (3g) JA および 12.3 (8) JEB より前の Cisco IOS リリースは、サポートされていません。



(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 番目の無線を無効にすることをお勧めします。

次の手順で、WGB に対してワークグループブリッジモードを有効にしてください。

- WGB アクセス ポイントの GUI で、[Settings] > [Network Interfaces] ページの無線ネットワークのロールに対する [Workgroup Bridge] を選択します。
- WGB アクセス ポイントの CLI で、**station-role workgroup-bridge** コマンドを入力します。





(注) 「WGB の設定例」の項の、WGB アクセス ポイントの設定サンプルを参照してください。

- 次の機能は WGB での使用をサポートされています。
  - ゲスト N+1 冗長性
  - ローカル EAP
  - Open、WEP 40、WEP 128、CKIP、WPA+TKIP、WPA2+AES、LEAP、EAP-FAST、および EAP-TLS 認証モード
- WGB に接続している有線クライアントは、セキュリティについて認証されません。代わりに WGB が、アソシエートしているアクセス ポイントに対して認証されます。そのため、WGB の有線側を物理的に保護することをお勧めします。
- WGB に接続された有線クライアントは、WGB の QoS および AAA Override 属性を継承します。
- WGB が Lightweight アクセス ポイントと通信できるようにするには、WLAN を作成して Aironet IE が有効であることを確認します。
- 実行時に ACL を WGB に適用する必要がある場合、実行時にコントローラのインターフェイスに対する ACL 設定を変更しないでください。ACL を変更する必要がある場合は、コントローラ内のすべての WLAN を無効にするか、802.11a と 80.11b の両方のネットワークを無効にしてください。さらに、そのインターフェイスに関連付けられ、マッピングされているクライアントがないことを確認してから、ACL の設定を変更できます。

## Cisco ワークグループブリッジの制約事項

- WGB は Lightweight アクセス ポイントのみとアソシエートできます。
- クライアントモード (デフォルト値) の WGB のみがサポートされています。インフラストラクチャモードのこれらの WGB はサポートされません。WGB 上で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。
  - WGB アクセス ポイントの GUI で、Reliable Multicast to WGB パラメータに対して [Disabled] を選択します。
  - WGB アクセス ポイントの CLI で、**no infrastructure client** コマンドを入力します。



(注) VLAN と WGB の併用はサポートされていません。



(注) 「[WGB の設定例](#)」の項の、WGB アクセス ポイントの設定サンプルを参照してください。

- 次の機能を WGB と使用することはサポートされていません。
  - Cisco Centralized Key Management (CCKM)
  - アイドル タイムアウト
  - Web 認証



(注) WGB が Web 認証 WLAN にアソシエートしている場合、その WGB は除外リストに追加され、その WGB 有線クライアントすべてが削除されます。

- WGB は、最大 20 の有線クライアントをサポートします。20 を超える有線クライアントがある場合は、ブリッジまたは他のデバイスを使用します。
- コントローラからの DirectStream 機能は、ワークグループブリッジの背後にあるクライアントに動作せず、ストリームが拒否されます。
- レイヤ 3 のローミングでは、WGB が別のコントローラ（外部コントローラなどに）にローミングした後で、有線クライアントをその WGB ネットワークに接続すると、有線クライアントの IP アドレスはアンカー コントローラにのみ表示され、外部コントローラには表示されません。
- 有線クライアントが長期間にわたってトラフィックを送信しない場合には、トラフィックが継続的にその有線クライアントに送信されていても、WGB 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。このトラフィック損失を避けるには、次の Cisco IOS コマンドを WGB で使用して WGB のエイジングアウトタイマーの値を大きく設定することで、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。

```
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。

- WGB レコードをコントローラから削除すると、すべての WGB 有線クライアントのレコードも削除されます。
- 次の機能は、WGB に接続された有線クライアントにはサポートされていません。
  - MAC フィルタリング
  - リンク テスト

◦ アイドル タイムアウト

- 有線 WGB クライアントに転送されるブロードキャストは、ネイティブの VLAN でのみ機能します。追加の VLAN が設定されると、ネイティブの VLAN のみがブロードキャストトラフィックを転送します。
- WGB の後方にある有線クライアントは、DMZ/アンカー コントローラに接続できません。WGB の後方にある有線クライアントを DMZ のアンカー コントローラに接続できるようにするには、**config wgb vlan enable** コマンドを使用して WGB で VLAN を有効にする必要があります。
- WGB モードのアクセス ポイントで入力できる **dot11 arp-cache** グローバル コンフィギュレーション コマンドはサポートされていません。

## WGB の設定例

次に、Static WEP と 40 ビットの WEP キーを使用した WGB アクセス ポイントの設定例を示します。

```
ap# configure 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)# ssid WGB_with_static_WEP
ap(config-if)# end
```

この WGB 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、WGB に次のコマンドを入力します。

### show dot11 association

以下に類似した情報が表示されます。

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address IP address Device Name Parent State
000b.8581.6aee 10.11.12.1 WGB-client map1 - Assoc
ap#
```

## ワークグループ ブリッジのステータスの表示 (GUI)

ステップ 1 [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。

このページの右側の [WGB] テキストボックスには、ネットワーク上の各クライアントについてワークグループブリッジであるかどうかが表示されます。

- ステップ 2** 目的のクライアントの MAC アドレスをクリックします。[Clients > Detail] ページが表示されます。このクライアントがワークグループブリッジの場合、[Client Properties] の下の [Client Type] テキストボックスに「WGB」が表示され、[Number of Wired Client(s)] テキストボックスに、この WGB に接続されている有線クライアントの番号が表示されます。
- ステップ 3** 次の手順に従って、特定の WGB に接続された有線クライアントの詳細を表示します。
- [Clients > Detail] ページで [Back] をクリックして、[Clients] ページに戻ります。
  - カーソルを目的の WGB の青いドロップダウン矢印の上に置いて、[Show Wired Clients] を選択します。  
[WGB Wired Clients] ページが表示されます。  
(注) 特定のクライアントを無効にしたり、削除したりする場合には、カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、それぞれ [Remove] または [Disable] を選択します。
  - 目的のクライアントの MAC アドレスをクリックすると、この特定のクライアントに関する詳細が表示されます。[Clients > Detail] ページが表示されます。  
[Client Properties] の下の [Client Type] テキストボックスには「WGB Client」と表示され、このページの他のテキストボックスにはこのクライアントに関するその他の情報が記載されています。

## ワークグループブリッジのステータスの表示 (CLI)

- ステップ 1** 次のコマンドを入力して、WGB をネットワークで表示します。  
**show wgb summary**

- ステップ 2** 次のコマンドを入力して、特定の WGB に接続された有線クライアントの詳細を表示します。  
**show wgb detail wgb\_mac\_address**

## WGB の問題のデバッグ (CLI)

はじめる前に

- 次のコマンドを入力して、IAPP メッセージ、エラー、およびパケットのデバッグを有効にします。
  - **debug iapp all enable** : IAPP メッセージのデバッグを有効にします。
  - **debug iapp error enable** : IAPP エラー イベントのデバッグを有効にします。

- **debug iapp packet enable** : IAPP パケットのデバッグを有効にします。
- 次のコマンドを入力して、ローミングの問題をデバッグします。  
**debug mobility handoff enable**
- 次のコマンドを入力して、DHCP が使用されている場合の IP 割り当ての問題をデバッグします。
  - **debug dhcp message enable**
  - **debug dhcp packet enable**
- 次のコマンドを入力して、静的 IP が使用されている場合の IP 割り当ての問題をデバッグします。
  - **debug dot11 mobile enable**
  - **debug dot11 state enable**





# 第 117 章

## Cisco 以外のワークグループブリッジの使用

- [Cisco 以外のワークグループブリッジについて, 929 ページ](#)
- [他社のワークグループブリッジの制約事項, 930 ページ](#)

### Cisco 以外のワークグループブリッジについて

Cisco ワークグループブリッジ (WGB) が使用されている場合、WGB は、アソシエートされているすべてのクライアントをアクセス ポイントに通知します。コントローラは、アクセス ポイントにアソシエートされたクライアントを認識します。Cisco 以外の WGB が使用されている場合、コントローラには、WGB の後方にある有線セグメントのクライアントの IP アドレスに関する情報は伝わりません。この情報がないと、コントローラは次のタイプのメッセージをドロップします。

- WGB クライアントに対するディストリビューション システムからの ARP REQ
- WGB クライアントからの ARP RPLY
- WGB クライアントからの DHCP REQ
- WGB クライアントに対する DHCP RPLY

次に、他社のワークグループブリッジに関する注意事項を示します。

- コントローラは Cisco 以外の WGB に適応し、パッシブクライアント機能を有効にすることで、ワークグループブリッジの後方にある有線クライアントとの間で ARP、DHCP、およびデータトラフィックを受け渡しできるようになりました。Cisco 以外の WGB と連携するようにコントローラを設定するには、パッシブクライアント機能を有効にして、有線クライアントからのすべてのトラフィックが WGB を介してアクセス ポイントにルーティングされるようにする必要があります。有線クライアントからのすべてのトラフィックは、ワークグループブリッジを介してアクセス ポイントにルーティングされます。

- WGB 有線クライアントがマルチキャストグループを離れると、他の WGB 有線クライアントへのダウンストリームマルチキャストトラフィックが一時的に中断されます。
- VMware のような PC 仮想化ソフトウェアを使用するクライアントを設置している場合は、この機能を有効にする必要があります。



(注) 複数のサードパーティデバイスに対して互換性のテストを実施しましたが、Cisco 以外のすべてのデバイスが機能することは保証できません。サードパーティデバイスに関する相互作用のサポートまたは設定の詳細については、デバイスの製造業者に確認してください。

- Cisco 以外のすべてのワークグループブリッジに対して、パッシブクライアント機能を有効にする必要があります。
- 次のコマンドを使用して、クライアントに DHCP を設定することが必要になる場合があります。
  - DHCP プロキシを無効にするには、**config dhcp proxy disable** コマンドを使用します。
  - DHCP ブートブロードキャストを有効にするには、**tconfig dhcp proxy disable bootp-broadcast enable** コマンドを使用します。

## 他社のワークグループブリッジの制約事項

- WGB デバイスに対しては、レイヤ 2 ローミングのみがサポートされます。
- WGB クライアントには、レイヤ 3 セキュリティ (Web 認証) はサポートされません。
- Cisco 以外の WGB デバイスは MAC 隠蔽 (hiding) を実行するので、コントローラでは WGB の後方にある有線ホストを表示できません。Cisco WGB では、IAPP がサポートされています。
- フラグが有効である場合に、WLAN での ARP ポイズニング検出は機能しません。
- WGB クライアントに対する VLAN 選択はサポートされていません。
- 一部のサードパーティ製 WGB は、非 DHCP リレーモードで動作する必要があります。Cisco 以外の WGB の後方にあるデバイスで、DHCP 割り当てに関する問題が発生した場合は、**config dhcp proxy disable** コマンドおよび **config dhcp proxy disable bootp-broadcast disable** コマンドを使用してください。

デフォルトの状態では、DHCP プロキシが有効になります。最適な組み合わせは、サードパーティの特性と設定によって異なります。





# 第 118 章

## バックアップコントローラの設定

- [バックアップコントローラの設定について, 931 ページ](#)
- [バックアップコントローラの設定に関する制約事項, 932 ページ](#)
- [バックアップコントローラの設定 \(GUI\) , 932 ページ](#)
- [バックアップコントローラの設定 \(CLI\) , 934 ページ](#)

### バックアップコントローラの設定について

中央のロケーションにある単一のコントローラは、アクセスポイントでローカルのプライマリコントローラとの接続を失った場合にバックアップとして機能できます。中央および地方のコントローラは、同じモビリティグループに存在する必要はありません。ネットワーク上の特定のアクセスポイントに対してプライマリ、セカンダリ、およびターシャリコントローラを指定できます。コントローラ GUI または CLI を使用して、バックアップコントローラの IP アドレスを指定できます。これにより、アクセスポイントはモビリティグループ外のコントローラをフェールオーバーできます。

次に、バックアップコントローラの設定に関する注意事項を示します。

- コントローラに接続されているすべてのアクセスポイントに対してプライマリとセカンダリのバックアップコントローラ（プライマリ、セカンダリ、ターシャリのコントローラが指定されていないか応答がない場合に使用される）や、ハートビートタイマーおよびディスクバリア要求タイマーなどの各種タイマーを設定できます。コントローラの障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセスポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビートタイマーの期限（ハートビート間隔ごとの）を過ぎると、アクセスポイントは最後のインターバルでコントローラからデータパケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセスポイントは高速エコー要求をコントローラへ送信します。
- アクセスポイントはバックアップコントローラのリストを維持し、リスト上の各エントリに対して定期的に **Primary discovery request** を送信します。アクセスポイントがコントローラから新しい **discovery response** を受信すると、バックアップコントローラのリストが更新されます。 **Primary discovery request** に 2 回連続で応答できなかったコントローラはすべて、リ

ストから削除されます。アクセスポイントのローカルコントローラに障害が発生した場合、プライマリ、セカンダリ、ターシャリ、プライマリ バックアップ、セカンダリ バックアップの順に、バックアップコントローラリストから使用可能なコントローラが選択されます。アクセス ポイントはバックアップ リストで使用可能な最初のコントローラからの **discovery response** を待機し、プライマリ ディスカバリ要求タイマーで設定された時間内に応答を受信した場合は、このコントローラに **join** します。制限時間に達すると、アクセス ポイントはコントローラを **join** できないものと見なし、リストで次に使用可能なコントローラからの **discovery response** を待ちます。

- アクセス ポイントのプライマリ コントローラが再度オンラインになると、アクセス ポイントはバックアップ コントローラからアソシエート解除してプライマリ コントローラに再接続します。アクセス ポイントはプライマリ コントローラにのみフォールバックします。設定されている使用可能なセカンダリ コントローラにはフォールバックしません。たとえば、アクセス ポイントがプライマリ、セカンダリ、およびターシャリ コントローラで設定されている場合、プライマリおよびセカンダリ コントローラが応答しなくなるとターシャリ コントローラにフェールオーバーします。プライマリ コントローラがダウンしている間、セカンダリ コントローラがオンラインに戻ると、アクセス ポイントはセカンダリ コントローラにフォールバックせず、ターシャリ コントローラへの接続が維持されます。アクセス ポイントは、プライマリ コントローラがオンラインに戻り、ターシャリ コントローラからプライマリ コントローラにフォールバックするまで待機します。ターシャリ コントローラに障害が発生し、プライマリ コントローラがまだダウンしている場合、アクセス ポイントは使用可能なセカンダリ コントローラにフォールバックします。

## バックアップコントローラの設定に関する制約事項

- 高速ハートビートタイマーは、ローカルモードまたはFlexConnectモードのアクセスポイントにのみ設定できます。

## バックアップコントローラの設定 (GUI)

- 
- ステップ 1** [Wireless]>[Access Points]>[Global Configuration] の順に選択して [Global Configuration] ページを開きます。
- ステップ 2** [Local Mode AP Fast Heartbeat Timer State] ドロップダウン リストから [Enable] を選択してローカルモードのアクセスポイントの高速ハートビートタイマーを有効にするか、または [Disable] を選択してタイマーを無効にします。デフォルト値は [Disable] です。
- ステップ 3** **ステップ 2** で [Enable] を選択した場合は、[Local Mode AP Fast Heartbeat Timeout] テキストボックスに入力して、ローカルモードのアクセスポイントに高速ハートビートタイマーを設定します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。Cisco Flex 7500 コントローラに対する AP 高速ハートビートタイムアウト値の範囲は、10 ~ 15 (両端の値を含む) であり、他のコントローラの場合は 1 ~ 10 (両端の値を含む) になります。Cisco Flex 7500

コントローラに対するハートビート タイムアウトのデフォルト値は、10 です。他のコントローラに対するデフォルト値は 1 秒です。

- ステップ 4** [FlexConnect Mode AP Fast Heartbeat Timer State] ドロップダウンリストから [Enable] を選択して FlexConnect アクセスポイントの高速ハートビートタイマーを有効にするか、または [Disable] を選択してこのタイマーを無効にします。デフォルト値は [Disable] です。
- ステップ 5** FlexConnect 高速ハートビートを有効にする場合は、[FlexConnect Mode AP Fast Heartbeat Timeout] テキストボックスに FlexConnect モード AP 高速ハートビート タイムアウト値を入力します。指定するハートビート間隔の値を小さくすると、コントローラの障害検出にかかる時間が短縮されます。  
Cisco Flex 7500 コントローラに対する FlexConnect モード AP 高速ハートビート タイムアウト値の範囲は 10 ~ 15 (両端の値を含む) であり、他のコントローラの場合は 1 ~ 10 になります。Cisco Flex 7500 コントローラに対するハートビート タイムアウトのデフォルト値は、10 です。他のコントローラに対するデフォルト値は 1 秒です。
- ステップ 6** [AP Primary Discovery Timeout] テキストボックスに 30 ~ 3600 秒 (両端の値を含む) の値を入力して、アクセスポイントのプライマリ ディスカバリ要求タイマーを設定します。デフォルト値は 120 秒です。
- ステップ 7** すべてのアクセスポイントにプライマリ バックアップコントローラを指定する場合は、プライマリ バックアップコントローラの IP アドレスを [Back-up Primary Controller IP Address] テキストボックスに、コントローラの名前を [Back-up Primary Controller Name] テキストボックスに入力します。  
(注) IP アドレスのデフォルト値は 0.0.0.0 であり、プライマリ バックアップコントローラは無効です。
- ステップ 8** すべてのアクセスポイントにセカンダリ バックアップコントローラを指定する場合は、セカンダリ バックアップコントローラの IP アドレスを [Back-up Secondary Controller IP Address] テキストボックスに、コントローラの名前を [Back-up Secondary Controller Name] テキストボックスに入力します。  
(注) IP アドレスのデフォルト値は 0.0.0.0 であり、セカンダリ バックアップコントローラは無効にします。
- ステップ 9** [Apply] をクリックして、変更を確定します。
- ステップ 10** 次の手順で、特定のアクセスポイントにプライマリ、セカンダリ、およびターシャリ バックアップコントローラを設定します。
- [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
  - プライマリ、セカンダリ、およびターシャリ バックアップコントローラを設定するアクセスポイントの名前をクリックします。
  - [High Availability] タブを選択して、[All APs > Details for] ([High Availability]) ページを開きます。
  - 必要に応じて、このアクセスポイントのプライマリ コントローラの名前と IP アドレスを [Primary Controller] テキストボックスに入力します。  
(注) この手順および次の 2 つの手順におけるバックアップコントローラの IP アドレスの入力はオプションです。バックアップコントローラが、アクセスポイントが接続されている (プライマリ コントローラ) モビリティグループの外にある場合、プライマリ、セカンダリ、またはターシャリ コントローラにそれぞれ IP アドレスを入力する必要があります。コントローラ名および IP アドレスは、同じプライマリ、セカンダリ、またはターシャリ コントローラに属する必要があります。そうでない場合、アクセスポイントはバックアップコントローラに join できません。

- e) 必要に応じて、このアクセスポイントのセカンダリコントローラの名前と IP アドレスを [Secondary Controller] テキストボックスに入力します。
- f) 必要に応じて、このアクセスポイントのターシャリコントローラの名前と IP アドレスを [Tertiary Controller] テキストボックスに入力します。
- g) [Apply] をクリックして、変更を確定します。

ステップ 11 [Save Configuration] をクリックして、変更を保存します。

## バックアップコントローラの設定 (CLI)

ステップ 1 次のコマンドを入力して、特定のアクセスポイントのプライマリコントローラを設定します。

**config ap primary-base controller\_name Cisco\_AP [controller\_ip\_address]**

(注) このコマンドの *controller\_ip\_address* パラメータおよびそれに続く 2 つのコマンドはオプションです。バックアップコントローラが、アクセスポイントが接続されている (プライマリコントローラ) モビリティグループの外にある場合、プライマリ、セカンダリ、またはターシャリコントローラにそれぞれ IP アドレスを入力する必要があります。各コマンドで、*controller\_name* および *controller\_ip\_address* は同じプライマリ、セカンダリ、またはターシャリコントローラに属する必要があります。そうでない場合、アクセスポイントはバックアップコントローラに join できません。

ステップ 2 次のコマンドを入力して、特定のアクセスポイントのセカンダリコントローラを設定します。

**config ap secondary-base controller\_name Cisco\_AP [controller\_ip\_address]**

ステップ 3 次のコマンドを入力して、特定のアクセスポイントのターシャリコントローラを設定します。

**config ap tertiary-base controller\_name Cisco\_AP [controller\_ip\_address]**

ステップ 4 次のコマンドを入力して、すべてのアクセスポイントのプライマリバックアップコントローラを設定します。

**config advanced backup-controller primary backup\_controller\_name backup\_controller\_ip\_address**

ステップ 5 次のコマンドを入力して、すべてのアクセスポイントのセカンダリバックアップコントローラを設定します。

**config advanced backup-controller secondary backup\_controller\_name backup\_controller\_ip\_address**

(注) プライマリまたはセカンダリバックアップコントローラエントリを削除するには、コントローラの IP アドレスとして *0.0.0.0* を入力します。

ステップ 6 次のコマンドを入力して、ローカルまたは FlexConnect アクセスポイントに対する高速ハートビートタイマーを有効または無効にします。

**config advanced timers ap-fast-heartbeat {local | flexconnect | all} {enable | disable} interval**

ここで、**all** はローカルおよび FlexConnect アクセスポイントの両方を表します。また、*interval* には 1 ~ 10 秒の値 (両端の値を含む) を指定します。指定するハートビート間隔の値を小さくすると、コントローラ

ラの障害検出にかかる時間が短縮されます。次のコマンドを入力して、デフォルト値では無効になっています。アクセス ポイントのハートビート タイマーを設定します。

**config advanced timers ap-heartbeat-timeout interval**

*interval* の値は、1～30 秒（両端の値を含む）です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。デフォルト値は 30 秒です。

**注意** 高遅延リンクと一緒に高速ハートビートタイマーを有効にしないでください。高速ハートビートタイマーを有効にする必要がある場合、タイマー値を遅延よりも大きくする必要があります。

**ステップ 7** 次のコマンドを入力して、アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。

**config advanced timers ap-primary-discovery-timeout interval**

*interval* の値は、30～3600 秒です。デフォルト値は 120 秒です。

**ステップ 8** 次のコマンドを入力して、アクセス ポイントのディスカバリ タイマーを設定します。

**config advanced timers ap-discovery-timeout interval**

*interval* の値は、1～10 秒です。デフォルト値は 10 秒です。

**ステップ 9** 次のコマンドを入力して、802.11 認証応答タイマーを設定します。

**config advanced timers auth-timeout interval**

*interval* の値は、10～600 秒（両端の値を含む）です。デフォルト値は 10 秒です。

**ステップ 10** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 11** 次のコマンドを入力して、アクセス ポイントの設定を表示します。

- **show ap config general Cisco\_AP**
- **show advanced backup-controller**
- **show advanced timers**

**show ap config general Cisco\_AP** コマンドに対しては、次のような情報が表示されます。

```
Cisco AP Identifier..... 1
Cisco AP Name..... AP5
Country code..... US - United States
Regulatory Domain allowed by Country..... 802.11bg:-AB 802.11a:-AB
AP Country code..... US - United States
AP Regulatory Domain..... 802.11bg:-A 802.11a:-N
Switch Port Number 1
MAC Address..... 00:13:80:60:48:3e
IP Address Configuration..... DHCP
IP Address..... 1.100.163.133
...
Primary Cisco Switch Name..... 1-5508
Primary Cisco Switch IP Address..... 2.2.2.2
Secondary Cisco Switch Name..... 1-4404
Secondary Cisco Switch IP Address..... 2.2.2.2
Tertiary Cisco Switch Name..... 2-4404
Tertiary Cisco Switch IP Address..... 1.1.1.4
```

...

**show advanced backup-controller** コマンドに対しては、次のような情報が表示されます。

```
AP primary Backup Controller controller1 10.10.10.10
AP secondary Backup Controller 0.0.0.0
```

**show advanced timers** コマンドに対しては、次のような情報が表示されます。

```
Authentication Response Timeout (seconds)..... 10
Rogue Entry Timeout (seconds)..... 1300
AP Heart Beat Timeout (seconds)..... 30
AP Discovery Timeout (seconds)..... 10
AP Local mode Fast Heartbeat (seconds)..... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)..... disable
AP Primary Discovery Timeout (seconds)..... 120
```

---



## 第 119 章

# アクセスポイントのフェールオーバープライオリティの設定

- [アクセスポイントに対するフェールオーバープライオリティの設定について](#), 937 ページ
- [アクセスポイントのフェールオーバープライオリティの設定 \(GUI\)](#), 938 ページ
- [アクセスポイントのフェールオーバープライオリティの設定 \(CLI\)](#), 938 ページ
- [フェールオーバープライオリティの設定の表示 \(CLI\)](#), 939 ページ

## アクセスポイントに対するフェールオーバープライオリティの設定について

各コントローラには、定義された数のアクセスポイント用通信ポートが装備されています。未使用のアクセスポイントポートがある複数のコントローラが同じネットワーク上に展開されている場合、1つのコントローラが故障すると、ドロップしたアクセスポイントは、自動的に未使用のコントローラポートをポーリングして、そのポートにアソシエートします。

次に、アクセスポイントのフェールオーバープライオリティを設定する際の注意事項を示します。

- バックアップコントローラがプライオリティレベルの高いアクセスポイントからの join 要求を認識できるよう、また、プライオリティレベルの低いアクセスポイントを必要に応じてアソシエーション解除してポートを使用可能にできるよう無線ネットワークを設定できます。
- フェールオーバーのプライオリティレベルは、通常の無線ネットワークの運用中は無効です。コントローラ障害後に使用できるバックアップコントローラポートよりも多くのアソシエーション要求が発生する場合のみ有効となります。
- この機能を設定するには、ネットワークのフェールオーバープライオリティレベルを設定して個別のアクセスポイントにプライオリティレベルを割り当てる必要があります。

- デフォルトでは、すべてのアクセスポイントはプライオリティレベル1に設定されています。これは、最も低いプライオリティレベルです。このため、これよりも高いプライオリティレベルを必要とするアクセスポイントにのみ、プライオリティレベルを割り当てる必要があります。

## アクセスポイントのフェールオーバープライオリティの設定 (GUI)

- ステップ 1 [Wireless] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。
- ステップ 2 [Global AP Failover Priority] ドロップダウンリストから [Enable] を選択してアクセスポイントフェールオーバープライオリティを有効にするか、または [Disable] を選択してこの機能を無効にし、アクセスポイントプライオリティの割り当てをすべて無視します。デフォルト値は [Disable] です。
- ステップ 3 [Apply] をクリックして、変更を確定します。
- ステップ 4 [Save Configuration] をクリックして、変更を保存します。
- ステップ 5 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 6 フェールオーバープライオリティを有効にするアクセスポイントの名前をクリックします。
- ステップ 7 [High Availability] タブを選択します。[All APs > Details for] ([High Availability]) ページが表示されます。
- ステップ 8 [AP Failover Priority] ドロップダウンリストで次のオプションのいずれかを選択して、アクセスポイントのプライオリティを指定します。
  - [Low] : アクセスポイントにプライオリティレベル1を割り当てます。これは最も低いプライオリティレベルです。これは、デフォルト値です。
  - [Medium] : アクセスポイントにプライオリティレベル2を割り当てます。
  - [High] : アクセスポイントにプライオリティレベル3を割り当てます。
  - [Critical] : アクセスポイントにプライオリティレベル4を割り当てます。これは最も高いプライオリティレベルです。
- ステップ 9 [Apply] をクリックして、変更を確定します。
- ステップ 10 [Save Configuration] をクリックして、変更を保存します。

## アクセスポイントのフェールオーバープライオリティの設定 (CLI)

- ステップ 1 次のコマンドを入力して、アクセスポイントフェールオーバープライオリティを有効または無効にします。

```
config network ap-priority {enable | disable}
```



**ステップ 2** 次のコマンドを入力して、アクセス ポイントのプライオリティを指定します。

```
config ap priority {1|2|3|4} Cisco_AP
```

ここで、1は最も低いプライオリティ レベルであり、4は最も高いプライオリティ レベルです。デフォルト値は、1です

**ステップ 3** **save config** コマンドを入力して、変更を保存します。

## フェールオーバー プライオリティの設定の表示 (CLI)

- 次のコマンドを入力して、ネットワーク上でアクセス ポイントのフェールオーバー プライオリティが有効かどうかを確認します。

```
show network summary
```

以下に類似した情報が表示されます。

```
RF-Network Name..... mrf
Web Mode..... Enable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High..... Disable
Secure Shell (ssh)..... Enable
Telnet..... Enable
Ethernet Multicast Mode..... Disable
Ethernet Broadcast Mode..... Disable
IGMP snooping..... Disabled
IGMP timeout..... 60 seconds
User Idle Timeout..... 300 seconds
ARP Idle Timeout..... 300 seconds
Cisco AP Default Master..... Disable
AP Join Priority..... Enabled
...

```

- 次のコマンドを入力して、各アクセス ポイントのフェールオーバー プライオリティを表示します。

```
show ap summary
```

以下に類似した情報が表示されます。

```
Number of APs..... 2
Global AP User Name..... user
Global AP Dot1x User Name..... Not Configured

AP Name Slots AP Model Ethernet MAC Location Port Country Priority

ap:1252 2 AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74 hallway 6 1 US 1
ap:1121 1 AIR-LAP1121G-A-K9 00:1b:d5:a9:ad:08 reception 1 US 3

```

特定のアクセス ポイントの概要を表示するには、アクセス ポイント名を指定します。また、アクセス ポイントのフィルタリングを行うときは、ワイルドカード検索を使用できます。





# 第 120 章

## AP の再送信間隔および再試行回数の設定

- [AP 再送信間隔および再試行回数の設定について](#), 941 ページ
- [アクセス ポイントの再送信間隔と再試行回数の制約事項](#), 941 ページ
- [AP の再送信間隔と再試行回数の設定 \(GUI\)](#), 942 ページ
- [アクセス ポイントの再送信間隔と再試行回数の設定 \(CLI\)](#), 942 ページ

### AP 再送信間隔および再試行回数の設定について

コントローラおよび AP は、信頼性のある CAPWAP 転送プロトコルを使用してパケットを交換します。各要求に対して、応答が定義されています。この応答を使用して、要求メッセージの受信を確認します。応答メッセージは明示的に確認されません。したがって、応答メッセージが受信されない場合は、再送信間隔後に元の要求メッセージが再送信されます。最大再送信回数が過ぎても要求が確認されないと、セッションが終了し、AP は別のコントローラに再アソシエートされます。

### アクセス ポイントの再送信間隔と再試行回数の制約事項

- 再送信間隔と再試行回数の両方とも、グローバルと特定のアクセス ポイントレベルで設定できます。グローバル設定では、これらの設定パラメータがすべてのアクセス ポイントに適用されます。つまり、再送信間隔と再試行回数は、すべてのアクセス ポイントに均一になります。また、特定のアクセス ポイントレベルで再送信間隔と再試行回数を設定すると、値はその特定のアクセス ポイントに適用されます。アクセス ポイント固有の設定は、グローバル設定よりも優先されます。
- 再送信間隔および再試行回数は、メッシュ アクセス ポイントには適用されません。

## APの再送信間隔と再試行回数の設定 (GUI)

再送信間隔と再試行回数は、すべてのAPにグローバルに設定することも、特定のAPに設定することもできます。

**ステップ1** コントローラ GUIを使用して、再送信間隔、および再試行回数をグローバルに設定するようにコントローラを設定するには、次の手順を実行します。

- a) [Wireless] > [Access Points] > [Global Configuration] の順に選択します。
- b) [AP Transmit Config Parameters] セクションから、次のいずれかのオプションを選択します。
  - [AP Retransmit Count] : アクセスポイントからコントローラに要求を再送信する回数を入力します。このパラメータには、3～8の値を指定できます。
  - [AP Retransmit Interval] : 要求の再送信から次の再送信までの時間を入力します。このパラメータには、2～5の値を指定できます。
- c) [Apply] をクリックします。

**ステップ2** 特定のアクセスポイントに対して、再送信間隔、および再試行回数を設定するようにコントローラを設定するには、次の手順を実行します。

- a) [Wireless] > [Access Points] > [All APs] の順に選択します。
- b) 値を設定するアクセスポイントに対応する [AP Name] リンクをクリックします。  
[All APs > Details] ページが表示されます。
- c) [Advanced] タブをクリックして、[Advanced Parameters] ページを開きます。
- d) [AP Transmit Config Parameters] セクションから、次のいずれかのパラメータを選択します。
  - [AP Retransmit Count] : アクセスポイントからコントローラに要求を再送信する回数を入力します。このパラメータには、3～8の値を指定できます。
  - [AP Retransmit Interval] : 要求の再送信から次の再送信までの時間を入力します。このパラメータには、2～5の値を指定できます。
- e) [Apply] をクリックします。

## アクセスポイントの再送信間隔と再試行回数の設定 (CLI)

再送信間隔と再試行回数は、すべてのアクセスポイントにグローバルに設定することも、特定のアクセスポイントに設定することもできます。

- 次のコマンドを入力して、すべてのアクセスポイントにグローバルに再送信間隔と再試行回数を設定します。

**config ap retransmit {interval | count} seconds all**

**interval** パラメータに有効な範囲は、3～8 です。 **count** パラメータに有効な範囲は、2～5 です。

- 次のコマンドを入力して、特定のアクセスポイントに再送信間隔と再試行回数を設定します。

**config ap retransmit {interval | count} seconds Cisco\_AP**

**interval** パラメータに有効な範囲は、3～8 です。 **count** パラメータに有効な範囲は、2～5 です。

- 次のコマンドを入力して、すべて、または特定の AP に設定した retransmit パラメータのステータスを表示します。

**show ap retransmit all**


---

(注) retransmit 値と retry 値は、メッシュモードのアクセスポイントに設定できないので、これらの値は N/A (適用外) として表示されます。

---

- 次のコマンドを入力して、特定のアクセスポイントに設定した retransmit パラメータのステータスを表示します。

**show ap retransmit Cisco\_AP**





# 第 121 章

## Country Code の設定

- [国番号の設定について](#), 945 ページ
- [国コードの設定に関する制約事項](#), 946 ページ
- [Country Code の設定 \(GUI\)](#) , 947 ページ
- [Country Code の設定 \(CLI\)](#) , 948 ページ

### 国番号の設定について

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制ドメインに割り当てられています（ヨーロッパの場合にはEなど）。しかし、国番号を使用すると、稼働する特定の国を指定できます（フランスの場合にはFR、スペインの場合にはESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャンネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

次に、国番号の設定に関する注意事項を示します。

- 通常、コントローラごとに1つの国番号を設定します。この国番号では、そのコントローラの物理的な場所とそのアクセスポイントが一致している必要があります。ただし、コントローラごとに最大 20 の国番号を設定できます。これによって、複数の国がサポートされ、1つのコントローラからさまざまな国にあるアクセスポイントを管理できます。
- コントローラは、さまざまな規制ドメイン（国）のさまざまなアクセスポイントをサポートしていますが、同一の規制ドメインについては、すべての無線を1つのアクセスポイントに設定する必要があります。たとえば、Cisco 1231 アクセスポイントの無線について、米国 (-A) の規制ドメインに対して 802.11b/g 無線を設定し、イギリス (-E) の規制ドメインに対して 802.11a 無線を設定しないでください。設定した場合、コントローラでアクセスポイントに選択した規制ドメインに応じて、コントローラによりアクセスポイントの無線のどちらか1つだけがオンになります。したがって、アクセスポイントの無線の両方には必ず同じ国番号を設定してください。

製品ごとにサポートされている国番号の完全なリストについては、次の Web サイトを参照してください。[http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL\\_SEARCH](http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH)

または

[http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product\\_data\\_sheet0900aecd80537b6a\\_ps6087\\_Products\\_Data\\_Sheet.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html)

- multiple-country 機能を使用している場合、同じ RF グループに join する予定のすべてのコントローラは、同じ国のセットを同じ順序で設定する必要があります。
- 複数の国が設定され、RRM 自動 RF 機能が有効になっている場合、RRM は AP の国番号ごとに許可されたチャンネルの統合を実行することによって取得したチャンネルを割り当てます。AP は、それぞれの PID 国番号に基づいて RRM によってチャンネルが割り当てられます。AP は、それぞれの PID 国番号と一致する法定周波数の使用のみが許可されます。AP の国番号が、配置されている国で合法であることを確認します。
- RF グループ リーダーに設定されている国リストによって、メンバーが動作するチャンネルが決定します。このリストは、RF グループ メンバーに設定されている国とは無関係です。

### 日本の国番号について

国番号は、各国で合法的に使用できるチャンネルを定義します。日本で使用できる国番号は、次のとおりです。

- JP : コントローラに join できるのは、-J 無線のみです。
- J2 : コントローラに join できるのは、-P 無線のみです。
- J3 : コントローラに join できるのは、-U、-P、および -Q (1550/1600/2600/3600 以外) 無線ですが、-U の周波数を使用します。
- J4 : コントローラに join できるのは、2.4G JPQU および 5G PQU です。




---

(注) 1550、1600、2600、および 3600 AP には J4 が必要です。

---

日本の規制ドメインのアクセス ポイントでサポートされているチャンネルと電力レベルの一覧については、『*Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points*』を参照してください。

## 国コードの設定に関する制約事項

- アクセス ポイントは、その国向けに設計されているチャンネルでのみ動作できます。





(注) アクセス ポイントがすでに規制の電力レベルより高く設定されていたり、手動入力で設定されている場合には、電力レベルはそのアクセス ポイントが割り当てられている特定の国によってのみ制限されます。

## Country Code の設定 (GUI)

- ステップ 1** 次の手順で 802.11 ネットワークを無効にします。
- [Wireless] > [802.11a/n/ac] > [Network] を選択します。
  - [802.11a Network Status] チェックボックスをオフにします。
  - [Apply] をクリックします。
  - [Wireless] > [802.11a/n/ac] > [Network] を選択します。
  - [802.11b/g Network Status] チェックボックスをオフにします。
  - [Apply] をクリックします。
- ステップ 2** [Wireless] > [Country] を選択して、[Country] ページを開きます。
- ステップ 3** アクセス ポイントがインストールされている各国のチェックボックスをオンにします。複数のチェックボックスをオンにした場合、RRM チャンネルと電力レベルが共通のチャンネルと電力レベルに制限されることを記載したメッセージが表示されます。
- ステップ 4** [OK] をクリックして続行するか、[Cancel] をクリックして操作をキャンセルします。
- ステップ 5** [Apply] をクリックします。  
ステップ 3 で複数の Country Code を選択した場合、各アクセス ポイントが国に割り当てられます。
- ステップ 6** 次の手順で、アクセス ポイントごとに選択されたデフォルトの国を表示し、必要に応じて別の国を選択します。
- (注) Country Code を設定から削除する場合、削除する国に現在割り当てられているアクセス ポイントはリブートし、コントローラに再 join される際に、必要に応じて残りの国のいずれかに再度割り当てられます。
- 次のいずれかの操作を行います。
    - 802.11 ネットワークを無効のままにします。
    - 802.11 ネットワークを再度有効にしてから、国コードを設定しているアクセス ポイントのみを無効にします。アクセス ポイントを無効にするには、[Wireless] > [Access Points] > [All APs] の順に選択し、目的のアクセス ポイントのリンクをクリックして、[Status] ドロップダウンリストで [Disable] を選択し、[Apply] をクリックします。
  - [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
  - 目的のアクセス ポイントのリンクをクリックします。
  - [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。  
このアクセス ポイントのデフォルトの国が [Country Code] ドロップダウンリストに表示されます。

- e) アクセスポイントが表示された国以外でインストールされている場合には、ドロップダウンリストから正しい国を選択します。このボックスに記載される Country Code は、アクセスポイントの無線のうち少なくとも1つの無線の規制ドメインに適合します。
- f) [Apply] をクリックします。
- g) コントローラに join されたすべてのアクセスポイントを特定の国に割り当てるには、この手順を繰り返します。
- h) ステップ a で無効にしたアクセスポイントを再び有効にします。

**ステップ 7** ステップ 6 でアクセスポイントを有効にしなかった場合は、802.11 ネットワークを再度有効にします。

**ステップ 8** [Save Configuration] をクリックします。

## Country Code の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、使用可能な Country Code をすべて表示します。

**show country supported**

**ステップ 2** 次のコマンドを入力して、802.11 ネットワークを無効にします。

**config 802.11a disable network**

**config 802.11b disable network**

**ステップ 3** 次のコマンドを入力して、アクセスポイントがインストールされた国の Country Code を設定します。

**config country code1[,code2,code3,...]**

複数の Country Code を入力する場合には、各 Country Code をカンマで区切ります (**config country US,CA,MX** など)。

**ステップ 4** 決定を確認するプロンプトが表示されたら、**Y** を入力します。

**ステップ 5** 次のコマンドを入力して、Country Code の設定を確認します。

**show country**

**ステップ 6** 次のコマンドを入力して、コントローラに設定された Country Code の使用可能なチャネルの一覧を表示します。

**show country channels**

**ステップ 7** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 8** 次のコマンドを入力して、アクセスポイントが割り当てられた国を表示します。

特定のアクセスポイントの概要を表示するには、アクセスポイント名を指定します。また、アクセスポイントのフィルタリングを行うときは、ワイルドカード検索を使用できます。

**show ap summary**

**ステップ 9** ステップ 3 で複数の Country Code を入力した場合は、次の手順に従って特定の国への各アクセス ポイントを割り当てます。

a) 次のいずれかの操作を行います。

- 802.11 ネットワークを無効のままにします。

- 802.11 ネットワークを再度有効にしてから、国コードを設定しているアクセス ポイントのみを無効にします。 ネットワークを再び有効にするには、次のコマンドを入力します。

**config 802.11 {a | b} enable network**

アクセス ポイントを無効にするには、次のコマンドを入力します。

**config ap disable ap\_name**

b) アクセス ポイントを特定の国に割り当てるには、次のコマンドを入力します。

**config ap country code {ap\_name | all}**

選択した Country Code が、アクセス ポイントの無線のうち少なくとも 1 つの無線の規制ドメインに適合していることを確認します。

(注) ネットワークを有効にしてアクセス ポイントを無効にしてから、**config ap country code all** コマンドを実行すると、指定した Country Code が無効にしたアクセス ポイントにのみ設定されます。他のアクセス ポイントは、すべて無視されます。

c) ステップ a で無効にしたアクセス ポイントを再び有効にするには、次のコマンドを入力します。

**config ap enable ap\_name**

**ステップ 10** ステップ 9 で 802.11 ネットワークを再度有効にしなかった場合には、ここで次のコマンドを入力して有効にします。

**config 802.11 {a | b} enable network**

**ステップ 11** 次のコマンドを入力して、変更を保存します。

**save config**

---





## 第 **122** 章

# アクセスポイントでのRFIDトラッキングの最適化

---

- [アクセスポイントでのRFIDトラッキングの最適化について](#), 951 ページ
- [アクセスポイントでのRFIDトラッキングの最適化 \(GUI\)](#), 952 ページ
- [アクセスポイントでのRFIDトラッキングの最適化 \(CLI\)](#), 952 ページ

## アクセスポイントでのRFIDトラッキングの最適化について

RFID タグの監視とロケーション計算を最適化するには、802.11b/g アクセスポイント無線用の 2.4GHz 帯域内で最高4つのチャンネルでトラッキングの最適化を有効化できます。この機能を使用して、通常、タグが動作するようにプログラムされているチャンネル（チャンネル1、6、11など）のみをスキャンすることができます。

コントローラのGUIまたはCLIを使用して、監視モード用アクセスポイントを設定し、このアクセスポイント無線でトラッキングの最適化を有効化できます。

## アクセスポイントでの RFID トラッキングの最適化 (GUI)

- 
- ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2 監視モードを有効にするアクセスポイントの名前をクリックします。[All APs > Details for] ページが表示されます。
- ステップ 3 [AP Mode] ドロップダウンリストから [Monitor] 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 アクセスポイントをリブートする警告が表示されたら、[OK] をクリックします。
- ステップ 6 [Save Configuration] をクリックして、変更を保存します。
- ステップ 7 [Wireless] > [Access Points] > [Radios] > [802.11b/g/n] の順に選択して、[802.11b/g/n Radios] ページを開きます。
- ステップ 8 カーソルを目的のアクセスポイントの青いドロップダウン矢印の上に置いて [Configure] を選択します。[802.11b/g/n Cisco APs > Configure] ページが表示されます。
- ステップ 9 アクセスポイント無線を無効にするには、[Admin Status] ドロップダウンリストから [Disable] を選択し、[Apply] をクリックします。
- ステップ 10 無線でトラッキングの最適化を有効にするには、[Enable Tracking Optimization] ドロップダウンリストから [Enable] を選択します。
- ステップ 11 4 つの [Channel] ドロップダウンリストから、RFID タグの監視対象となるチャンネルを選択します。  
(注) タグの監視対象となるチャンネルは少なくとも 1 つ設定する必要があります。
- ステップ 12 [Apply] をクリックします。
- ステップ 13 [Save Configuration] をクリックします。
- ステップ 14 アクセスポイント無線を再び有効にするには、[Admin Status] ドロップダウンリストから [Enable] を選択し、[Apply] をクリックします。
- ステップ 15 [Save Configuration] をクリックします。
- 

## アクセスポイントでの RFID トラッキングの最適化 (CLI)

- 
- ステップ 1 次のコマンドを入力して、監視モード用のアクセスポイントを設定します。  
**config ap mode monitor Cisco\_AP**
- ステップ 2 アクセスポイントがリブートされるが操作を続行するかどうかをたずねる警告が表示されたら、**Y** と入力します。
- ステップ 3 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 4** 次のコマンドを入力して、アクセスポイント無線を無効にします。

**config 802.11b disable** *Cisco\_AP*

**ステップ 5** 次のコマンドを入力して、使用国でサポートされている DCA チャンネルのみをスキャンするようアクセスポイントを設定します。

**config ap monitor-mode tracking-opt** *Cisco\_AP*

(注) スキャンするチャンネルを正確に指定するには、ステップ 6 で、**config ap monitor-mode tracking-opt** *Cisco\_AP* コマンドを入力します。

(注) このアクセスポイントのトラッキングの最適化を無効にするには、**config ap monitor-mode no-optimization** *Cisco\_AP* コマンドを入力します。

**ステップ 6** ステップ 5 のコマンドを入力してからこのコマンドを入力して、アクセスポイントがスキャンする 802.11b チャンネルを 4 つまで選択できます。

**config ap monitor-mode 802.11b fast-channel** *Cisco\_AP channel1 channel2 channel3 channel4*

(注) 米国では、*channel* 変数に 1 から 11 までの任意の値を割り当てられます。その他の国ではさらに多くのチャンネルがサポートされています。少なくともチャンネルを 1 つ割り当てる必要があります。

**ステップ 7** 次のコマンドを入力して、アクセスポイント無線を再度有効にします。

**config 802.11b enable** *Cisco\_AP*

**ステップ 8** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 9** 次のコマンドを入力して、監視モードのアクセスポイントすべての概要を表示します。

**show ap monitor-mode summary**

---







## プローブ要求フォワーディングの設定

- [プローブ要求フォワーディングの設定について](#), 955 ページ
- [プローブ要求フォワーディングの設定 \(CLI\)](#), 955 ページ

### プローブ要求フォワーディングの設定について

プローブ要求とはクライアントが送信する 802.11 管理フレームであり、SSID の機能についての情報を要求します。デフォルトでは、アクセス ポイントは応答済みの (acknowledged) プローブ要求をコントローラが処理できるよう送信します。応答済みの (acknowledged) プローブ要求とは、アクセス ポイントがサポートする SSID のプローブ要求です。必要に応じて、応答済みの (acknowledged) プローブ要求および未応答の (unacknowledged) プローブ要求の両方をフォワードするようアクセス ポイントを設定できます。コントローラは応答済みの (acknowledged) プローブ要求からの情報を使用してロケーションの精度を向上できます。

### プローブ要求フォワーディングの設定 (CLI)

**ステップ 1** 次のコマンドを入力して、アクセス ポイントからコントローラにフォワードされたプローブ要求のフィルタリングを有効または無効にします。

```
config advanced probe filter {enable | disable}
```

デフォルトのフィルタ設定であるプローブ フィルタリングを有効にすると、アクセス ポイントは応答済みの (acknowledged) プローブ要求のみをコントローラにフォワードします。プローブフィルタリングを無効にすると、アクセス ポイントは応答済みの (acknowledged) プローブ要求と未応答の (unacknowledged) プローブ要求の両方をコントローラにフォワードします。

**ステップ 2** 次のコマンドを入力して、一定期間内にコントローラに送信されるプローブ要求の、アクセス ポイント無線あたり、およびクライアントあたりの数を制限します。

```
config advanced probe limit num_probes interval
```

値は次のとおりです。

- *num\_probes* は、一定期間内にコントローラに送信されるプローブ要求のアクセス ポイント無線あたり、およびクライアントあたりの数 (1~100) です。
- *interval* は、プローブ制限間隔です (100 ~ 10000 ミリ秒)。

*num\_probes* のデフォルト値は 2 (プローブ要求数) であり、*interval* のデフォルト値は 500 ミリ秒です。

**ステップ 3** **save config** コマンドを入力して、変更を保存します。

**ステップ 4** 次のコマンドを入力して、Cisco AP のプローブ キューに対してバックオフ パラメータを設定します。  
**config advanced probe backoff {enable | disable}**

- **enable** : プローブ応答に追加されたバックオフパラメータを使用する場合にはこのパラメータを選択します。
- **disable** : プローブ応答にデフォルトのバックオフパラメータ値を使用する場合にはこのパラメータを選択します。

**ステップ 5** 次のコマンドを入力して、プローブ要求フォワーディングの設定を表示します。

**show advanced probe**

以下に類似した情報が表示されます。

```
Probe request filtering..... Enabled
Probes fwd to controller per client per radio.... 2
Probe request rate-limiting interval..... 500 msec
```



## 第 124 章

# コントローラとアクセス ポイント上の一意のデバイス ID の取得

- [コントローラとアクセス ポイント上の Unique Device Identifier の取得について](#), 957 ページ
- [コントローラとアクセス ポイント上の Unique Device Identifier の取得 \(GUI\)](#), 958 ページ
- [コントローラとアクセス ポイント上の Unique Device Identifier の取得 \(CLI\)](#), 958 ページ

## コントローラとアクセス ポイント上の Unique Device Identifier の取得について

Unique Device Identifier (UDI) 規格は、すべてのシスコ製ハードウェア製品ファミリにわたって、一意に製品を識別するので、ビジネスおよびネットワーク運用を通じてシスコ製品を識別および追跡し、資産管理システムを自動化できます。この規格は、すべての電子的、物理的、および標準のビジネスコミュニケーションにわたって一貫性があります。UDIは、次の5つのデータ要素で構成されています。

- 注文可能な製品 ID (PID)
- 製品 ID のバージョン (VID)
- シリアル番号 (SN)
- エンティティ名
- 製品の説明

UDIは、工場出荷時にコントローラと Lightweight アクセス ポイントの EEPROM に記録されます。UDIは、GUI または CLI のいずれかを使用して取得できます。

## コントローラとアクセス ポイント上の Unique Device Identifier の取得 (GUI)

- 
- ステップ 1** [Controller] > [Inventory] の順に選択して、[Inventory] ページを開きます。  
このページには、コントローラ UDI の 5 つのデータ要素が表示されています。
- ステップ 2** [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 3** 目的のアクセス ポイントの名前をクリックします。
- ステップ 4** [Inventory] タブを選択して、[All APs > Details for] ([Inventory]) ページを開きます。  
このページには、アクセス ポイントのコンポーネント情報が表示されます。
- 

## コントローラとアクセス ポイント上の Unique Device Identifier の取得 (CLI)

コントローラの CLI を使用して、次のコマンドを入力し、コントローラとアクセス ポイントの UDI を取得します。

- **show inventory** : コントローラの UDI 文字列を表示します。以下に類似した情報が表示されます。

```
...
...
NAME: "Chassis" , DESCR: "Cisco 5500 Series Wireless LAN Controller"
PID: AIR-CT5508-K9, VID: V01, SN: XXXXXXXXXXXX
```

- **show inventory ap *ap\_id*** : 指定したアクセス ポイントの UDI 文字列を表示します。



# 第 125 章

## リンク テストの実行

- [リンク テストの実行について](#), 959 ページ
- [リンク テストの実行 \(GUI\)](#), 960 ページ
- [リンク テストの実行 \(CLI\)](#), 961 ページ

### リンク テストの実行について

リンク テストを使用して、2つのデバイス間の無線リンクの質を決定します。リンク テストの際には、要求と応答の2種類のリンク テスト パケットを送信します。リンク テストの要求パケットを受信した無線は、適切なテキストボックスを記入して、応答タイプセットを使用して送信者にパケットを返信します。

クライアントからアクセスポイント方向への無線リンクの質は、アクセスポイントからクライアント方向へのものと異なることがあり、それは双方の送信電力と受信感度が非対称であることによるものです。2種類のリンク テスト (ping テストおよびCCX リンク テスト) を実行できます。

*ping* リンク テストでは、コントローラはクライアントからアクセスポイント方向でのみリンクの質をテストできます。アクセスポイントで受信された ping パケットの RF パラメータは、クライアントからアクセスポイント方向のリンクの質を決定するためにコントローラによりポーリングされます。

CCX リンク テストでは、コントローラはアクセスポイントからクライアント方向でもリンクの質をテストできます。コントローラはクライアントにリンク テストの要求を発行し、クライアントは RF パラメータ (受信信号強度表示 [RSSI]、信号対雑音比 [SNR] など) を記録します。応答パケット内の受信要求パケットの。リンク テストの要求ロールと応答ロールの両方を、アクセスポイントとコントローラに実装します。アクセスポイントまたはコントローラが CCX v4 クライアントまたは v5 クライアントに対してリンク テストを開始でき、同様に CCX v4 クライアントまたは v5 クライアントもアクセスポイントまたはコントローラに対してリンク テストを開始できます。

コントローラでは、CCX リンク テストに対する下記のリンクの質のメトリックが両方向で表示されます (アウト: アクセスポイントからクライアント、イン: クライアントからアクセスポイント)。

- RSSI の形式の信号強度 (最小、最大、および平均)
- SNR の形式の信号の質 (最小、最大、および平均)
- 再試行されたパケットの合計数
- 単一パケットの最大再試行回数
- 消失パケット数
- 正常に送信されたパケットのデータ レート

コントローラにより、方向とは無関係に次のメトリックが表示されます。

- リンク テストの要求/応答の往復時間 (最小、最大、および平均)

コントローラ ソフトウェアは、CCX バージョン 1～5 をサポートします。CCX サポートは、コントローラ上の各 WLAN について自動的に有効となり、無効にできません。コントローラでは、クライアント データベースにクライアントの CCX バージョンが格納されます。このクライアントの機能を制限するには、これを使用します。クライアントが CCX v4 または v5 をサポートしていない場合、コントローラはクライアント上で ping リンク テストを実行します。クライアントが CCX v4 または v5 をサポートしている場合、コントローラはクライアント上で CCX リンク テストを実行します。クライアントが CCX リンク テストの間にタイムアウトになった場合、コントローラは ping リンク テストに自動的に切り替わります。



(注)

この項の手順に従って、GUI または CLI のいずれかを使用してリンク テストを実行します。

## リンク テストの実行 (GUI)

- 
- ステップ 1** [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。
- ステップ 2** カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、[Link Test] を選択します。[Link Test] ページが表示されます。
- (注) 目的のクライアントの MAC アドレスをクリックしてから、[Clients > Detail] ページの上部にある [Link Test] ボタンをクリックしても、このページにアクセスできます。
- このページには、CCX リンク テストの結果が表示されます。
- (注) クライアントおよびコントローラ (またはそのいずれか) が CCX v4 以降のリリースをサポートしていない場合、コントローラは代わりにクライアント上で ping リンク テストを実行し、さらに制限された [Link Test] ページが表示されます。
- (注) CCX クライアントのリンク テストに失敗すると、クライアントが到達可能である場合は、デフォルトで ping テスト結果に設定されます。
- ステップ 3** [OK] をクリックして、[Link Test] ページを終了します。
-

## リンクテストの実行 (CLI)

コントローラ CLI を使用してリンクテストを実行するコマンドは、次のとおりです。

- 次のコマンドを入力して、リンクテストを実行します。

### **linktest ap\_mac**

コントローラとテストするクライアントの両方で CCX v4 以降のリリースを有効化すると、次のような情報が表示されます。

```

CCX Link Test to 00:0d:88:c5:8a:d1.
 Link Test Packets Sent..... 20
 Link Test Packets Received..... 10
 Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
 Link Test Packets round trip time (min/max/average)..... 5ms/20ms/15ms
 RSSI at AP (min/max/average)..... -60dBm/-50dBm/-55dBm

 RSSI at Client (min/max/average)..... -50dBm/-40dBm/-45dBm

 SNR at AP (min/max/average)..... 40dB/30dB/35dB
 SNR at Client (min/max/average)..... 40dB/30dB/35dB
 Transmit Retries at AP (Total/Maximum)..... 5/3
 Transmit Retries at Client (Total/Maximum)..... 4/2
 Transmit rate: 1M 2M 5.5M 6M 9M 11M 12M 18M 24M 36M 48M 54M 108M

 Packet Count: 0 0 0 0 0 0 0 0 0 2 0 18 0
 Transmit rate: 1M 2M 5.5M 6M 9M 11M 12M 18M 24M 36M 48M 54M 108M

 Packet Count: 0 0 0 0 0 0 0 0 0 2 0 8 0

```

CCX v4 以降のリリースがコントローラまたはテストするクライアントのいずれかで無効化されている場合には、表示される情報が少なくなります。

```

Ping Link Test to 00:0d:88:c5:8a:d1.
 Link Test Packets Sent..... 20
 Link Test Packets Received..... 20
 Local Signal Strength..... -49dBm
 Local Signal to Noise Ratio..... 39dB

```

- CCX リンクテストおよび ping テストの両方に使用できるリンクテストパラメータを調整するには、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。

**linktest frame-size size\_of\_link-test\_frames**

**linktest num-of-frame number\_of\_link-test\_request\_frames\_per\_test**







# 第 126 章

## リンク遅延の設定

- [リンク遅延の設定について](#), 963 ページ
- [リンク遅延の制約事項](#), 964 ページ
- [リンク遅延の設定 \(GUI\)](#), 964 ページ
- [リンク遅延の設定 \(CLI\)](#), 965 ページ

### リンク遅延の設定について

コントローラでリンク遅延を設定して、アクセスポイントおよびコントローラ間のリンクを計測できます。この機能はコントローラに join されたすべてのアクセスポイントで使用できますが、特に、リンクが低速または信頼性の低い WAN 接続の可能性のある FlexConnect および OfficeExtend アクセスポイントで役立ちます。

次に、リンク遅延の注意事項を示します。

- リンク遅延は、アクセスポイントからコントローラ、およびコントローラからアクセスポイントにおける CAPWAP ハートビートパケット（エコー要求および応答）のラウンドトリップ時間をモニタします。この時間は、ネットワークリンク速度およびコントローラの処理ロードによって異なります。アクセスポイントはコントローラへの発信エコー要求およびコントローラから受信するエコー応答をタイムスタンプ記録します。アクセスポイントはこのデルタ時間をシステムのラウンドトリップ時間としてコントローラに送信します。アクセスポイントは、30 秒のデフォルト間隔でコントローラにハートビートパケットを送信します。



(注) リンク遅延はアクセスポイントとコントローラ間の CAPWAP 応答時間を計算します。ネットワーク遅延や ping 応答は計測しません。

- コントローラにより、現在のラウンドトリップ時間および継続的な最短および最長ラウンドトリップ時間が表示されます。最短および最長時間はコントローラが動作している限り維持され、クリアして再開することもできます。

- コントローラ GUI または CLI を使用して特定のアクセス ポイントのリンク遅延を設定することも、CLI を使用してコントローラに接続されたすべてのアクセス ポイントのリンク遅延を設定することもできます。

## リンク遅延の制約事項

- リンク遅延は、接続モードの FlexConnect アクセス ポイントでのみサポートされます。スタンドアロン モードの FlexConnect アクセス ポイントはサポートされません。

## リンク遅延の設定 (GUI)

- 
- ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2 リンク遅延を有効にするアクセス ポイントの名前をクリックします。
- ステップ 3 [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。
- ステップ 4 [Enable Link Latency] チェックボックスを選択して、このアクセス ポイントのリンク遅延を有効にするか、または選択解除して、エコー応答受信ごとにアクセス ポイントがコントローラにラウンドトリップ時間を送信しないようにします。デフォルト値はオフです。
- ステップ 5 [Apply] をクリックして、変更を確定します。
- ステップ 6 [Save Configuration] をクリックして、変更を保存します。
- ステップ 7 [All APs] が再表示されたら、アクセス ポイントの名前をもう一度クリックします。
- ステップ 8 [All APs > Details for] ページが再表示されたら、もう一度 [Advanced] タブを選択します。リンク遅延およびデータ遅延の結果は、[Enable Link Latency] の下に表示されます。
- [Current] : アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットまたはデータ パケットの現在のラウンドトリップ時間 (ミリ秒)
  - [Minimum] : リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットまたはデータ パケットの最短ラウンドトリップ時間 (ミリ秒)
  - [Maximum] : リンク遅延が有効になってから、またはリセットされてからの、アクセス ポイントからコントローラ、およびコントローラからアクセス ポイントの間の CAPWAP ハートビート パケットまたはデータ パケットの最長ラウンドトリップ時間 (ミリ秒)
- ステップ 9 このアクセス ポイントのコントローラ上の現在、最短、および最長リンク遅延およびデータ遅延統計情報をクリアするには、[Reset Link Latency] をクリックします。
- ステップ 10 ページが更新されて [All APs > Details for] ページが再表示されたら、[Advanced] タブを選択します。[Minimum] テキストボックスおよび [Maximum] テキストボックスに更新された統計情報が表示されます。
-

## リンク遅延の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、現在コントローラにアソシエートされている特定のアクセスポイントまたはすべてのアクセスポイントに対してリンク遅延を有効または無効にします。

```
config ap link-latency {enable | disable} {Cisco_AP | all}
```

デフォルト値はディセーブルです。

(注) コマンド **config ap link-latency {enable | disable} all** は、現在コントローラに join しているアクセスポイントのリンク遅延のみを有効または無効にします。将来 join されるアクセスポイントには適用されません。

**ステップ 2** 次のコマンドを入力して、特定のアクセスポイントのリンク遅延結果を表示します。

```
show ap config general Cisco_AP
```

以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 1
Cisco AP Name..... AP1
...
AP Link Latency..... Enabled
Current Delay..... 1 ms
Maximum Delay..... 1 ms
Minimum Delay..... 1 ms
Last updated (based on AP Up Time)..... 0 days, 05 h 03 m 25 s
```

このコマンドの出力には、次のリンク遅延結果が含まれます。

- **[Current Delay]** : アクセスポイントからコントローラ、およびコントローラからアクセスポイントの間の CAPWAP ハートビートパケットの現在のラウンドトリップ時間 (ミリ秒)。
- **[Maximum Delay]** : リンク遅延が有効になってから、またはリセットされてからの、アクセスポイントからコントローラ、およびコントローラからアクセスポイントの間の CAPWAP ハートビートパケットの最長ラウンドトリップ時間 (ミリ秒)。
- **[Minimum Delay]** : リンク遅延が有効になってから、またはリセットされてからの、アクセスポイントからコントローラ、およびコントローラからアクセスポイントの間の CAPWAP ハートビートパケットの最短ラウンドトリップ時間 (ミリ秒)

**ステップ 3** 次のコマンドを入力して、特定のアクセスポイントのコントローラ上の現在、最短、および最長リンク遅延統計情報をクリアします。

```
config ap link-latency reset Cisco_AP
```

**ステップ 4** 次のコマンドを入力して、リセットの結果を表示します。

```
show ap config general Cisco_AP
```





# 第 127 章

## TCP MSS の設定

---

- [TCP MSS の設定について](#) , 967 ページ
- [TCP MSS の設定 \(GUI\)](#) , 967 ページ
- [TCP MSS の設定 \(CLI\)](#) , 968 ページ

### TCP MSS の設定について

トランスミッションコントロールプロトコル (TCP) スリーウェイハンドシェイクにおけるクライアントの最大セグメントサイズ (MSS) が、最大伝送単位で処理できるサイズよりも大きい場合、スループットの低下およびパケットのフラグメンテーションが発生する場合があります。コントローラ ソフトウェア リリース 6.0 以降のリリースでこの問題を回避するには、コントローラに join しているすべてのアクセスポイントまたは特定のアクセスポイントに MSS を指定します。

この機能を有効にすると、アクセスポイントがデータパスのワイヤレスクライアントと送受信する TCP パケットの MSS を選択します。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセスポイントは MSS を、設定された新しい値に変更します。

TCP MSS は、ローカルモードの AP でのみサポートされます。

### TCP MSS の設定 (GUI)

- 
- ステップ 1** [WIRELESS] > [Access Points] > [Global Configuration] の順に選択して [Global Configuration] ページを開きます。
  - ステップ 2** [TCP MSS] の下にある [Global TCP Adjust MSS] チェックボックスをオンして、コントローラにアソシエートされているすべてのアクセスポイントの MSS を設定します。有効な範囲は、536 ~ 1363 バイトです。
-

## TCP MSS の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、特定のアクセス ポイントまたはすべてのアクセス ポイントの TCP MSS を有効または無効にします。

```
config ap tcp-mss-adjust {enable | disable} {Cisco_AP | all} size
```

ここで、*size* パラメータは 536 ~ 1363 バイトの間の値です。デフォルト値はクライアントにより異なります。

**ステップ 2** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 3** 次のコマンドを入力して、特定のアクセス ポイントまたはすべてのアクセス ポイントの現在の TCP MSS 設定を表示します。

```
show ap tcp-mss-adjust {Cisco_AP | all}
```

以下に類似した情報が表示されます。

AP Name	TCP State	MSS Size
AP-1140	enabled	536
AP-1240	disabled	-
AP-1130	disabled	-



# 第 128 章

## Power over Ethernet の設定

- [Power over Ethernet の設定について](#), 969 ページ
- [Power over Ethernet の設定 \(GUI\)](#), 971 ページ
- [Power over Ethernet の設定 \(CLI\)](#), 973 ページ

### Power over Ethernet の設定について

Lightweight モードに変換されたアクセス ポイント (AP1131 または AP1242 など)、または 1250 シリーズ アクセス ポイントが Cisco pre-Intelligent Power Management (pre-IPM) スイッチに接続されたパワー インジェクタで電源を供給されている場合、インラインパワーとも呼ばれる Power over Ethernet (PoE) を設定する必要があります。

デュアル無線 1250 シリーズ アクセス ポイントは、PoE を使用して電力投入された場合、4 つの異なるモードで動作できます。

- **20.0 W (Full Power)** : このモードは、パワー インジェクタまたは AC/DC アダプタを使用した場合と同等です。
- **16.8 W** : 両方のトランスミッタを低電力で使用します。レガシーのデータ レートは影響を受けませんが、M0 ~ M15 のデータ レートは 2.4 GHz 帯域では低下します。すべてのデータ レートが有効であるため、スループットへの影響は最小限です。送信電力が低いため、レンジに影響があります。レシーバはすべて有効なままです。
- **15.4 W** : 単一のトランスミッタのみが有効です。レガシーデータ レートおよび M0 ~ M7 のレートは最小限の影響を受けます。M8 ~ M15 のレートは、両方のトランスミッタを必要とするため無効になります。スループットはレガシー アクセス ポイントよりも高いが、20 W および 16.8 W 電力モードよりも低くなります。
- **11.0 W (Low Power)** : アクセス ポイントは動作していますが、無線は両方とも無効です。

次に、Power over Ethernet の注意事項を示します。

- 15.4-W PoE でデュアル無線 1250 シリーズ アクセス ポイントに電源を供給する場合、全機能を動作させることはできません。全機能の動作には 20 W 必要です。アクセス ポイントは

15.4-WPoE でデュアル無線を動作させられますが、スループットおよびレンジのパフォーマンスは低下します。15.4W で全機能が必要な場合は、1250 シリーズ アクセスポイントシャーシから無線を 1 つ取り外すか、またはソフトウェア リリース 6.0 以降のリリースで無効にして、他の無線が完全な 802.11n モードで動作できるようにします。アクセスポイント無線が管理者により無効にされた後は、アクセスポイントをリブートして変更を適用する必要があります。無線を有効化しなおして低スループットモードに変更した後も、アクセスポイントをリブートする必要があります。

これらのモードは、使用できる有線インフラストラクチャで 1250 シリーズ アクセスポイントを動作させて、希望するパフォーマンスレベルを得られる柔軟性を提供します。拡張 PoE スイッチ (Cisco Catalyst 3750-E シリーズ スイッチなど) により、1250 シリーズ アクセスポイントは最大限の機能を最小限の総所有コストで提供できます。また、アクセスポイントに既存の PoE (802.3af) スイッチで電力供給する場合、アクセスポイントは無線の数 (1 または 2) によって適切な動作モードを選択します。



(注) Cisco PoE スイッチの詳細については、次の URL を参照してください。 <http://www.cisco.com/en/US/prod/switches/poe.html>

- ° 次の表に、PoE を使用する 1250 シリーズ アクセスポイントの最大送信電力設定を示します。

表 24 : PoE 使用の 1250 シリーズ アクセスポイントの最大送信電力設定

無線帯域	データ レート	トランスミッタ数	Cyclic Shift Diversity (CSD; サイクリックシフトダイバーシティ)	最大送信電力 (dBm) <sup>5</sup>		
				802.3af モード (15.4W)	ePoE 電力最適化モード (16.8W)	ePoE モード (20W)
2.4 GHz	802.11b	1	—	。	。	。
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1	ディセーブル有効 (デフォルト)	17	17	17
		2		ディセーブル	14 (トランスミッタあたり 11)	20 (トランスミッタあたり 17)
802.11n MCS 8-15	2	—	ディセーブル	14 (トランスミッタあたり 11)	20 (トランスミッタあたり 17)	



5 GHz	802.11a	1	—	17	17	17
	802.11n MCS 0-7	1	ディセーブル 有効 (デフォ ルト)	17	17	17
		2		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	—	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)	

<sup>5</sup> 最大送信電力は、チャンネルおよび国別の規制により異なります。特定の詳細については、製品ドキュメンテーションを参照してください。

- シスコ標準ではない PoE スイッチで電力供給する場合、1250 シリーズ アクセス ポイントは 15.4 W 未満で動作します。シスコ以外のスイッチまたはミッドスパン デバイスが高電力を供給できる場合でも、アクセス ポイントは拡張 PoE モードでは動作しません。

## Power over Ethernet の設定 (GUI)

**ステップ 1** [Wireless] > [Access Points] > [All APs] の順に選択し、目的のアクセス ポイントの名前を選択します。

**ステップ 2** [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。  
[PoE Status] テキスト ボックスには、アクセス ポイントが動作する電力レベルである、[High (20 W)]、[Medium (16.8 W)]、または [Medium (15.4 W)] が表示されます。このテキスト ボックスは設定できません。コントローラによりアクセス ポイントの電源が自動検出され、ここにその電力レベルが表示されます。

(注) このテキスト ボックスは、PoE を使用して電力供給している 1250 シリーズ アクセス ポイントにのみ適用されます。アクセス ポイントの電力レベルが低いかどうかを判断する方法は、ほかに 2 つあります。1 つは、[802.11a/n/ac (または 802.11b/g/n) Cisco APs > Configure] ページの [Tx Power Level Assignment] セクションに表示される「Due to low PoE, radio is transmitting at degraded power」というメッセージです。2 つめは、[Trap Logs] ページのコントローラのトラップ ログに表示される「PoE Status: degraded operation」というメッセージです。

**ステップ 3** 次のいずれかの操作を行います。

- アクセス ポイントが高電力の 802.3af Cisco スイッチである場合、[Pre-standard 802.3af switches] チェックボックスをオンにします。これらのスイッチは従来の 6 ワットを超える電力を供給しますが、Intelligent Power Management (IPM) 機能をサポートしません。

- パワー インジェクタによって電力が供給されている場合は、[Pre-standard 802.3af switches] チェックボックスをオフにします。これは、デフォルト値です。

**ステップ 4** 付属のスイッチが IPM をサポートしておらず、パワーインジェクタが使用されている場合、[Power Injector State] チェックボックスをオンにします。付属のスイッチが IPM をサポートしている場合、このチェックボックスをオンにする必要はありません。

**ステップ 5** 前の手順で [Power Injector State] チェックボックスをオンにした場合、[Power Injector Selection] パラメータおよび [Injector Switch MAC Address] パラメータが表示されます。Power Injector Selection パラメータは、パワー インジェクタが過失によりバイパスされた場合にスイッチ ポートが突発的に過負荷にならないよう保護します。ドロップダウン リストから次のオプションのいずれかを選択して、必要な保護のレベルを指定します。

- [Installed] : 現在接続されているスイッチ ポートの MAC アドレスを点検して記憶し、パワーインジェクタが接続されていることを想定します。ネットワークに従来のシスコ 6 W スイッチが装備されていて、再配置されたアクセス ポイントを強制的にダブルチェックしたときに発生する可能性のある過負荷を避けたい場合に、このオプションを選択します。

スイッチの MAC アドレスを設定する場合は、[Injector Switch MAC Address] テキストボックスに MAC アドレスを入力します。アクセス ポイントにスイッチの MAC アドレスを検知させる場合は、[Injector Switch MAC Address] テキストボックスは空白のままにします。

(注) アクセス ポイントが再配置されるたびに、新しいスイッチ ポートの MAC アドレスは記憶した MAC アドレスとの一致に失敗し、アクセス ポイントは低電力モードのままになります。その場合、パワーインジェクタの存在を物理的に検証し、このオプションを再選択して新しい MAC アドレスを記憶させます。

- [Override] : このオプションにより、アクセス ポイントは最初に MAC アドレスの一致を検証しなくても、高電力モードで稼働できます。ネットワークに、12 W アクセス ポイントへ直接接続すると過負荷が発生する可能性のある、従来のシスコ 6 W スイッチが装備されていない場合には、このオプションを選択できます。このオプションのメリットは、アクセス ポイントを再配置した場合、設定しなおさずに高電力モードで稼働を継続できることです。このオプションのデメリットは、アクセス ポイントが直接 6 W スイッチへ接続されていると、過負荷が発生することです。

**ステップ 6** [Apply] をクリックします。

**ステップ 7** デュアル無線 1250 シリーズ アクセス ポイントを所有しており、無線のうちの 1 つを無効にして他方の無線に最大電力を供給する場合の手順は次のとおりです。

- a) [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] の順に選択して、[802.11a/n/ac] (または 802.11b/g/n) Radios] ページを開きます。
- b) 無効にする無線の青いドロップダウンの矢印の上にカーソルを置いて、[Configure] を選択します。
- c) [802.11a/n/ac] (または 802.11b/g/n) Cisco APs > Configure] ページで、[Admin Status] ドロップダウン リストから [Disable] を選択します。
- d) [Apply] をクリックします。
- e) 手動でアクセス ポイントをリセットして、変更を適用します。

**ステップ 8** [Save Configuration] をクリックします。

## Power over Ethernet の設定 (CLI)

コントローラの CLI を使用して PoE を設定し、設定内容を表示するには、次のコマンドを使用します。

- ネットワークに、12 W アクセスポイントへ直接接続すると過負荷を発生する可能性のある、従来のシスコ 6 W スイッチが装備されている場合には、次のコマンドを入力します。

**config ap power injector enable {Cisco\_AP | all} installed**

アクセスポイントは、パワーインジェクタがこの特定のスイッチポートに接続されていることを記憶します。アクセスポイントを再配置する場合、新しいパワーインジェクタの存在を検証した後で、このコマンドを再度実行する必要があります。



(注) このコマンドを入力する前に、CDP が有効化されていることを確認します。有効になっていない場合、このコマンドは失敗します。CDP の有効化の詳細については、「[Cisco Discovery Protocol の設定](#)」の項を参照してください。

- 次のコマンドを入力して、安全確認の必要をなくし、アクセスポイントをどのスイッチポートにも接続できるようにします。

**config ap power injector enable {Cisco\_AP | all} override**

ネットワークに、12 W アクセスポイントに直接接続すると過負荷を発生する可能性のある従来のシスコ 6 W スイッチが装備されていない場合は、このコマンドを使用できます。アクセスポイントは、パワーインジェクタが常に接続されていることを前提としています。アクセスポイントを再配置した場合も、パワーインジェクタの存在を前提とします。

- 接続スイッチポートの MAC アドレスがわかっている、[Installed] オプションを使用して自動的に検出しない場合は、次のコマンドを入力します。

**config ap power injector enable {Cisco\_AP | all} switch\_port\_mac\_address**

- デュアル無線 1250 シリーズ アクセスポイントを所有しており、無線のうちの 1 つを無効にして他方の無線に最大電力を供給する場合は、次のコマンドを入力します。

**config {802.11a | 802.11b} disable Cisco\_AP**



(注) 手でアクセスポイントをリセットして、変更を適用する必要があります。

- 次のコマンドを入力して、特定のアクセスポイントの PoE 設定を表示します。

**show ap config general Cisco\_AP**

以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 1
Cisco AP Name..... AP1
...
PoE Pre-Standard Switch..... Enabled
PoE Power Injector MAC Addr..... Disabled
Power Type/Mode..... PoE/Low Power (degraded mode)
...
```

アクセス ポイントが最大電力で動作していない場合、[Power Type/Mode] テキスト ボックスには、「degraded mode」と表示されます。

- 次のコマンドを入力して、コントローラのトラップ ログを表示します。

#### **show traplog**

アクセス ポイントが最大電力で動作していない場合は、トラップには「PoE Status: degraded operation」が含まれます。

- 次のコマンドを入力して、Power over Ethernet (PoE) を搭載したシスコ準規格 15-W スイッチでアクセス ポイントに電源を投入できます。

#### **config ap power pre-standard {enable | disable} {all | Cisco\_AP}**

シスコ準規格 15-W スイッチは Intelligent Power Management (IPM) をサポートしていませんが、標準アクセス ポイントに十分な電力を供給できます。次のシスコ準規格 15-W スイッチを使用できます。

- WS-C3550、WS-C3560、WS-C3750
- C1880
- 2600、2610、2611、2621、2650、2651
- 2610XM、2611XM、2621XM、2650XM、2651XM、2691
- 2811、2821、2851
- 3631-telco、3620、3640、3660
- 3725、3745
- 3825、3845

アクセス ポイントがシスコ準規格 15-W スイッチにより電力供給されている場合、全機能を使用するには、このコマンドの **enable** バージョンが必要です。アクセス ポイントが IPM スイッチまたはパワー インジェクタを使用して電力を供給するか、またはアクセス ポイントが上記 15-W スイッチの 1 つを使用しない場合は使用しても安全です。

無線の動作ステータスが「Down」になっていて「Up」にする場合、このコマンドが必要になることがあります。PoE の障害を示しているこのエラーメッセージを検索する **show msglog** コマンドを入力します。

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable
to
verify sufficient in-line power. Radio slot 0 disabled.
```



# 第 129 章

## クライアントの表示

---

- [クライアントの表示 \(GUI\) , 975 ページ](#)
- [クライアントの表示 \(CLI\) , 977 ページ](#)

### クライアントの表示 (GUI)

---

**ステップ 1** [Monitor] > [Clients] の順に選択して、[Clients] ページを開きます。

このページには、コントローラのアクセスポイントにアソシエートされたすべてのクライアントのリストが表示されます。このリストには、各クライアントに関する次の情報が記載されます。

- クライアントの MAC 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の名前
- クライアントが使用する WLAN の名前
- クライアントのタイプ (802.11a、802.11ac、802.11b、802.11g、802.11n)
  - (注) 802.11n クライアントが 802.11n を有効にした 802.11a 無線にアソシエートされている場合、クライアントのタイプは 802.11a/n/ac と表示されます。802.11n クライアントが 802.11n を有効にした 802.11b/g 無線にアソシエートされている場合、クライアントのタイプは 802.11b/n と表示されます。
- クライアント接続のステータス
- クライアントの許可ステータス
- 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のポート数
- クライアントが WGB かどうかの表示

- (注) クライアントを削除したり無効にしたりする場合には、カーソルを目的のクライアントの青いドロップダウン矢印の上に置いて、[Remove] または [Disable] を選択します。クライアントとアクセスポイントの間の接続をテストするには、目的のクライアントの青いドロップダウンの矢印の上にカーソルを置いて、[Link Test] を選択します。

**ステップ 2** 次の手順でフィルタを作成し、特定の基準 (MAC アドレス、ステータス、無線のタイプなど) を満たすクライアントのみを表示します。

- a) [Change Filter] をクリックして、[Search Clients] ダイアログボックスを開きます。
- b) 次のチェックボックスの 1 つまたは複数をおんにして、クライアントを表示する際に使用する基準を指定します。
  - [MAC Address] : クライアントの MAC アドレスを入力します。

(注) [MAC Address] フィルタを有効にすると、その他のフィルタは自動的に無効になります。その他のフィルタのいずれかを有効にすると、[MAC Address] フィルタは自動的に無効になります。
  - [AP Name] : アクセスポイントの名前を入力します。
  - [WLAN Profile] : ドロップダウンリストから、使用可能な WLAN プロファイルのいずれかを選択します。
  - [Status] : [Associated]、[Authenticated]、[Excluded]、[Idle] のいずれか、または複数のチェックボックスをおんにします。
  - [Radio Type] : [802.11a]、[802.11b]、[802.11g]、[802.11an]、[802.11bn]、または [Mobile] を選択します。
  - [WGB] : コントローラのアクセスポイントにアソシエートされた WGB クライアントを入力します。
- c) [Apply] をクリックします。[Clients] ページの上部にある Current Filter パラメータは、現在適用されているフィルタを示します。

(注) フィルタを削除してクライアントリスト全体を表示するには、[Clear Filter] をクリックします。

**ステップ 3** クライアントの MAC アドレスをクリックして、特定のクライアントの詳細情報を表示します。[Clients > Detail] ページが表示されます。

このページには、次の情報が表示されます。

- クライアントの一般的なプロパティ
- クライアントのセキュリティ設定
- クライアントの QoS のプロパティ
- クライアントの統計
- 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のプロパティ

## クライアントの表示 (CLI)

クライアント情報を表示するには、次のコマンドを使用します。

- 次のコマンドを入力して、特定のアクセスポイントにアソシエートされたクライアントを表示します。

```
show client ap {802.11a | 802.11b} Cisco_AP
```

- 次のコマンドを入力して、コントローラのアクセスポイントにアソシエートされたクライアントの概要を表示します。

```
show client summary
```

- 次のコマンドを入力して、特定のクライアントの詳細情報を表示します。

```
show client detail client_mac
```







# 第 130 章

## アクセスポイントの LED 状態の設定

---

- [LED 状態の設定, 979 ページ](#)
- [点滅する LED の設定, 980 ページ](#)

### LED 状態の設定

#### アクセスポイントに対する LED 状態の設定について

多数のアクセスポイントの無線 LAN ネットワークでは、コントローラに関連付けられた特定のアクセスポイントを検出することは困難です。アクセスポイントの LED が点灯し、アクセスポイントを見つけられるように、コントローラでアクセスポイントの LED 状態が設定されるようにすることができます。この設定は、ワイヤレスネットワークでグローバルに行うことも、AP レベルごとに行うこともできます。

グローバルレベルの LED 状態の設定は、AP レベルよりも優先されます。

#### ネットワーク内のアクセスポイントの LED 状態のグローバル設定 (GUI)

- 
- ステップ 1** [Wireless]>[Access Points]>[Global Configuration] の順に選択して [Global Configuration] ページを開きます。
  - ステップ 2** [LED state] チェックボックスをオンにします。
  - ステップ 3** このチェックボックスの横にあるドロップダウンリストから [Enable] を選択します。
  - ステップ 4** [Apply] をクリックします。
-

## ネットワーク内のアクセスポイントの LED 状態のグローバル設定 (CLI)

- 次のコマンドを入力して、コントローラに関連付けられているすべてのアクセスポイントの LED 状態を設定します。

```
config ap led-state {enable | disable} all
```

## 特定のアクセスポイントで LED 状態の設定 (GUI)

- 
- ステップ 1 [Wireless] > [Access Points] > [All APs] の順に選択し、目的のアクセスポイントの名前を選択します。
  - ステップ 2 [Advanced] タブを選択して、[All APs > Details for] ([Advanced]) ページを開きます。
  - ステップ 3 [LED state] チェックボックスをオンにします。
  - ステップ 4 このテキストボックスの横にあるドロップダウンリストから [Enable] を選択します。
  - ステップ 5 [Apply] をクリックします。
- 

## 特定のアクセスポイントで LED 状態の設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、LED 状態を設定するアクセスポイントの ID を決定します。  

```
show ap summary
```
  - ステップ 2 次のコマンドを入力し、LED 状態を設定します。  

```
config ap led-state {enable | disable} Cisco_AP
```
- 

## 点滅する LED の設定

### 点滅する LED の設定について

コントローラソフトウェアでは、アクセスポイントの LED を点滅させて、その場所を示すことができます。すべての Cisco IOS Lightweight アクセスポイントがこの機能をサポートしています。

### 点滅する LED の設定 (CLI)

LED の点滅をコントローラの特権 EXEC モードから設定するには、次のコマンドを使用します。

- 1 次のコマンドを入力して、AP 用の LED の点滅を設定します。

```
config ap led-state flash {seconds | indefinite | disable} {Cisco_AP}
```

AP の有効な LED が点滅間隔は 1~3600 秒です。LED が無期限に点滅するように設定したり、LED の点滅が停止するように設定することもできます。

- 2 次のコマンドを入力して、LED 点滅を有効にしてから AP に対して無効にします。

```
config ap led-state flash disable Cisco_AP
```

コマンドによって LED 点滅はただちに無効化されます。たとえば、前のコマンドを実行してから (60 秒に設定した *seconds* パラメータを使用して) わずか 20 秒で LED 点滅を無効にした場合でも、アクセスポイントの LED はただちに点滅を停止します。

- 3 次のコマンドを入力して、変更を保存します。

```
save config
```

- 4 次のコマンドを入力して、AP 用の LED 点滅の状態を確認します。

```
show ap led-flash Cisco_AP
```

以下に類似した情報が表示されます。

```
(Cisco Controller)> show ap led-flash AP1040_46:b9
Led Flash..... Enabled for 450 secs, 425 secs left
```




---

(注) コマンドがコンソールで入力されたか TELNET/SSH CLI セッションで入力されたかに関係なく、これらのコマンドの出力はコントローラ コンソールにのみ送信されます。

---





# 第 131 章

## デュアルバンド無線によるアクセスポイントの設定

- [デュアルバンド無線によるアクセスポイントの設定 \(GUI\) , 983 ページ](#)
- [デュアルバンド無線によるアクセスポイントの設定 \(CLI\) , 984 ページ](#)

### デュアルバンド無線によるアクセスポイントの設定 (GUI)

- ステップ 1** [Wireless] > [Access Points] > [Radios] > [Dual-Band Radios] を選択して、[Dual-Band Radios] ページを開きます。
- ステップ 2** AP の青いドロップダウン矢印の上にカーソルを置いて、[Configure] をクリックします。
- ステップ 3** 管理状態を設定します。
- ステップ 4** 次のいずれかとして CleanAir の管理状態を設定します。
- 有効
  - 無効
  - 5 GHz のみ
  - 2.4 GHz のみ
- ステップ 5** [Apply] をクリックします。
- ステップ 6** [Save Configuration] をクリックします。

#### 次の作業

[Monitor] > [Access Points] > [Radios] > [Dual-Band Radios] と移動して、デュアルバンド無線でアクセスポイントをモニタできます。

## デュアルバンド無線によるアクセスポイントの設定 (CLI)

- 次のコマンドを入力して、デュアルバンド無線でアクセスポイントを設定します。  
**config 802.11-abgn {enable | disable} ap-name**
- 次のコマンドを入力して、デュアルバンド無線でアクセスポイントのCleanAir機能を設定します。  
**config 802.11-abgn cleanair {enable | disable} ap-name band 2.4-or-5-GHz**



# 第 132 章

## UDP Lite の設定

- [UDP Lite について](#), 985 ページ
- [UDP Lite のグローバル設定 \(GUI\)](#), 986 ページ
- [AP 上での UDP Lite の設定 \(GUI\)](#), 986 ページ
- [UDP Lite の設定 \(CLI\)](#), 987 ページ

### UDP Lite について

リリース 8.0 の CAPWAP 機能は IPv4 と IPv6 の両方をカバーします。CAPWAP の変更はコントローラと AP に及びます。IPv6 に対応していない古いイメージを実行している AP は、IPv4 アドレスとダウンロードイメージを持っていれば、IPv6 対応コントローラに接続できます。その逆も同様です。

IPv6 の実装には、AP とコントローラのパフォーマンスを低下させる User Datagram Protocol (UDP) の完全なペイロードチェックサムが必須です。パフォーマンスの影響を最小限に抑える目的で、コントローラと AP は、データグラムのヘッダーチェックサムのみが必須の UDP Lite をサポートしているため、パケット全体のチェックサムが回避されます。UDP Lite を有効にすると、パケット処理時間が短縮されます。

UDP Lite プロトコルは、IP プロトコル ID 136 を使用して、UDP で使用されるものと同じ CAPWAP ポートを使用します。UDP Lite を有効にする場合は、ネットワーク ファイアウォールでプロトコル 136 を許可する必要があります。UDP と UDP Lite を切り替えると、AP が接続解除されてから、再接続されます。UDP Lite はデータトラフィックに使用され、UDP は制御トラフィックに使用されます。

UDP Lite が有効になっているコントローラは、IPv4 しかサポートしない既存の AP とともに IPv6 対応 AP とメッセージを交換できます。



(注) デュアルスタック コントローラは、IPv4 AP マネージャと IPv6 AP マネージャの両方を使用してディスカバリ要求に応答します。

AP ディスカバリ メカニズムは、AP に割り当てられた IPv4 アドレスと IPv6 アドレスの両方を使用します。AP は、送信元アドレス選択を使用して、IPv6 コントローラに到達するためのアドレスを決定します。

## UDP Lite のグローバル設定 (GUI)

- 
- ステップ 1** [Wireless] > [Access Points] > [Global Configuration] の順に選択して、[Global Configuration] ページを開きます。
- ステップ 2** [Global UDP Lite] セクションで、[UDP Lite] チェックボックスをオンにして、UDP Lite をグローバルに有効にします。
- (注) IPv6 UDP Lite は CAPWAPv4 トンネルを使用して接続された AP には適用されません。これらは CAPWAPv6 トンネルを使用してコントローラに接続している AP にのみ適用されます。
- ステップ 3** [Apply] をクリックして、グローバル UDP Lite 構成を設定します。
- ステップ 4** 必要に応じて、ステップ 2 で説明したグローバル IPv6 UDP Lite を選択解除することによって、グローバル UDP Lite 構成をオーバーライドすることができます。
- (注) UDP と UDP Lite を切り替えると、AP が接続解除されてから、再接続されます。
- ステップ 5** [Save Configuration] をクリックして変更を保存します。
- 

## AP 上での UDP Lite の設定 (GUI)

- 
- ステップ 1** [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
- ステップ 2** IPv6 アドレスを含む [AP Name] を選択して、それをクリックし、選択した AP の [Details] ページを開きます。
- ステップ 3** [Advanced] タブで、[UDP Lite] チェックボックスをオンにして、選択した AP の UDP Lite を有効にします。
- (注) このフィールドは CAPWAPv6 トンネル経由でコントローラに join している AP の場合にのみ表示されます。Web UI ページでは、CAPWAPv4 トンネル経由でコントローラに join している AP のこのフィールドが表示されません。
- ステップ 4** [Apply] をクリックして、変更を確定します。
- ステップ 5** [Save Configuration] をクリックして変更を保存します。
-



## UDP Lite の設定 (CLI)

- ステップ 1** UDP Lite をグローバルに有効にするには、次のコマンドを使用します。  
**config ipv6 capwap udpliteenable all**
- ステップ 2** 選択した AP 上で UDP Lite を有効にするには、次のコマンドを使用します。  
**config ipv6 capwap udpliteenable <Cisco AP>**
- ステップ 3** UDP Lite をグローバルに無効にするには、次のコマンドを使用します。  
**config ipv6 capwap udplitedisable all**
- ステップ 4** 選択した AP 上で UDP Lite を無効にするには、次のコマンドを使用します。  
**config ipv6 capwap udplitedisable <Cisco AP>**
- ステップ 5** コントローラ上の UDP Lite のステータスを表示するには、次のコマンドを使用します。

**show ipv6 summary**

```
(Cisco Controller) >show ipv6 summary
```

```
Global Config..... Disabled
Reachable-lifetime value..... 300
Stale-lifetime value..... 86400
Down-lifetime value..... 30
RA Throttling..... Disabled
RA Throttling allow at-least..... 1
RA Throttling allow at-most..... 1
RA Throttling max-through..... 10
RA Throttling throttle-period..... 600
RA Throttling interval-option..... passthrough
NS Multicast CacheMiss Forwarding..... Disabled
NA Multicast Forwarding..... Enabled
IPv6 Capwap UDP Lite..... Enabled
Operating System IPv6 state Disabled
```

```
(Cisco Controller) >
```





# 第 133 章

## Cisco Hyperlocation

- [Cisco Hyperlocation](#) について, 989 ページ
- [Cisco Hyperlocation](#) の設定, 990 ページ

### Cisco Hyperlocation について

Cisco Hyperlocation の無線モジュールには、以下の機能があります。

- 以下の拡張性を備えた WSM 無線モジュール機能：
  - 802.11ac
  - Wi-Fi 送信
  - 20 MHz、40 MHz、80 MHz チャンネル帯域幅に拡張された WSM、RRM チャンネル スキャン。
- 拡張ロケーション機能：
  - 低遅延ロケーション最適化チャンネルのスキャン
  - 32 アンテナ到達角度 (AoA)
- Bluetooth Low Energy (BLE) 機能

屋内メッシュは Cisco Aironet 3600 と 3700 シリーズ アクセス ポイントで利用可能です。

Cisco Hyperlocation の詳細については、以下の文書を参照してください。

- 『[Cisco Hyperlocation Solution](#)』
- 『[Cisco CMX 10.2 Configuration Guide to enable Cisco Hyperlocation](#)』
- 『[Cisco ASA 10.2 Release Notes](#)』

# Cisco Hyperlocation の設定

## Cisco Hyperlocation の設定 (GUI)

この項では、Cisco Hyperlocation 無線モジュールがあり、Cisco WLC に接続されているすべての AP で Cisco Hyperlocation を設定する手順について説明します。個々のアクセス ポイントまたはアクセス ポイント グループに Cisco Hyperlocation 設定を適用することもできます。

**ステップ 1** [Wireless] > [Access Points] > [Global Configuration] を選択します。

**ステップ 2** [Hyperlocation Config Parameters] セクションで、次の手順を実行します。

- a) [Enable Hyperlocation] チェックボックスをオンにします。  
[Enable Hyperlocation] チェックボックスをオンにすると、AP と取り付けられているモジュールに基づいて、異なるロケーション サービス (PRL ベースまたは AoA ベース) が有効になります。
- b) [Packet Detection RSSI Minimum (dBm)] 値を入力します。  
これは、ロケーション計算で使用するために、データ パケットが WSM モジュールで受信される最小レベルです。デフォルト値は -100 dB です。  
ロケーションの計算に強い信号のみを使用する場合は、この値を増やすことをお勧めします。
- c) [Scan Count Threshold for Idle Client Detection] 値を入力します。  
スキャン数のしきい値は、AP がアイドル状態のクライアントにブロック確認応答要求 (BAR) を送信する前に待機するオフチャネル スキャン サイクル数を表します。デフォルト値の 10 は、オフチャネル スキャン サイクル内のチャネル数に応じて、約 40 秒に相当します。
- d) NTP サーバの IPv4 アドレスを入力します。  
これは、この計算に関係するすべての AP が同期する NTP サーバの IPv4/IPv6 アドレスです。  
一般的な WLC インフラストラクチャで使用されるのと同じ NTP サーバを使用することをお勧めします。ロケーションを正確に計算するためには、複数の AP からのスキャンが同期されている必要があります。IPv4 アドレスが必要です。

**ステップ 3** [BLE Beacon Config Parameters] セクションで、次の手順を実行します。

- a) [Interval (1-10)Hz] ボックスに BLE 伝送間隔を入力します。
- b) [Beacon ID] を選択します。
- c) 必要に応じて、[Delete Beacon] チェックボックスをオンにして、選択されたビーコンを削除します。
- d) [Beacon Status] を有効または無効にします。
- e) ビーコンの [UUID] を指定します。
- f) [TxPower (-52 to 0)dBm] ボックスで選択されたビーコンの伝送パワーを指定します。

**ステップ 4** 設定を保存します。

## Cisco Hyperlocation の設定 (CLI)

- 次のコマンドを入力して、Cisco Hyperlocation をグローバルに設定します。  
**config advanced hyperlocation {enable | disable}**
- 次のコマンドを入力して、Cisco Hyperlocation グローバル コンフィギュレーションの概要を確認します。  
**show advanced hyperlocation summary**
- 次のコマンドを入力して、AP グループごとに Cisco Hyperlocation を設定します。  
**config advanced hyperlocation apgroupgroup-name {enable | disable}**





# 第 134 章

## Cisco Air Time Fairness

- [Cisco Air Time Fairness](#) について, 993 ページ
- [Cisco Air Time Fairness](#) の設定 (GUI) , 997 ページ
- [Cisco Air Time Fairness](#) の設定 (CLI) , 998 ページ

### Cisco Air Time Fairness について

High Density Experience (HDX) 向けの Cisco Air Time Fairness (ATF) を利用してネットワーク管理者は、定義したカテゴリでデバイスをグループにまとめて、一部のグループに、他のグループよりも頻繁にWLANからトラフィックを受信させることができます。これにより、一部のグループには他のグループよりも長い通信時間を利用する権利を与えることができます。

Cisco ATF には次の機能があります。

- ユーザグループまたはデバイスカテゴリに Wi-Fi の通信時間を割り当てる
- Air Time Fairness は、ネットワークではなくネットワーク管理者が定義する
- 簡単な仕組みで通信時間を割り当てることができる
- WLAN の状態の変化に動的に対応できる
- サービスレベル契約を効率的に実行できる
- 各種の標準規格に準拠した Wi-Fi QoS のメカニズムを強化できる

環境内でクライアントグループごとの通信中時間面の公平さの意味するものを定義する能力をネットワークマネージャに与えることで、トラフィック量も制御することができます。

通信時間をパーセンテージ単位で制御するために、クライアント/SSIDアップリンクとダウンリンク送信の両方が含まれる通信時間を継続的に測定します。

AP が正確に制御できるのは、ダウンリンク方向 (AP からクライアント方向) の通信時間のみです。アップリンク方向 (クライアントから AP 方向) の通信時間は測定できますが、正確に制御することはできません。AP は、クライアントに発信するパケットの通信時間を制限できますが、

AP が測定できるのはその AP がクライアントから受信したパケットの通信時間のみです。これは、AP は受信時の通信時間を正確には制限できないためです。

Cisco ATF は通信時間の限度（全通信時間に対する割合）を設定し、その限度を SSID 単位で適用します。このとき、SSID はクライアントグループを定義するパラメータとして使用します。他のパラメータも、クライアントグループの定義に利用できます。さらに、1つの通信時間の限度（全通信時間に対する割合）をそれぞれのクライアントに適用できます。

SSID（またはクライアント）の通信時間の限度を超えると、ダウンリンク方向のパケットはドロップされます。ダウンリンク パケット（AP からクライアント方向）をドロップすると通信時間が解放されます。これに対して、アップリンク パケット（クライアントから AP 方向）をドロップしても、通信時間の解放にはつながりません。これは、そのパケットがクライアントによって無線で送信済みであるためです。

### クライアント フェア シェアリング

Cisco Wireless Release 8.2 では、Cisco Air Time Fairness を SSID/WLAN に関連付けられたクライアントで実施できます。これにより、SSID/WLAN 内のすべてのクライアントは、それぞれの無線帯域幅の使用率に応じて均等に処理されます。この機能は、1つまたは2、3のクライアントが、SSID/WLAN に割り当てられたすべての通信時間を消費して、同じ SSID/WLAN に関連付けられた他のクライアントの Wi-Fi エクスペリエンスを奪ってしまう状況で便利です。

- 各クライアントに割り当てる通信時間の割合は、クライアントの接続や切断のたびに計算し直されます。
- クライアント フェア シェアリングを適用できるのは、ダウンストリーム トラフィックのみです。
- クライアントはポリシー レベルで、低、中、高の使用率グループに分類できます。
- クライアントベースのATFメトリックは、送信完了ルーチンで累積します。これにより、使用率が中から低のグループのクライアントが未使用の通信時間をシェア プール パケットに累積して、使用率が高いクライアントに通信時間を融通することができます。

### サポート対象のアクセス ポイント プラットフォーム

Cisco ATF は、次のアクセス ポイントでサポートしています。

- Cisco Aironet 1260 シリーズ アクセス ポイント
- Cisco Aironet 1260 シリーズ アクセス ポイント
- Cisco Aironet 1570 シリーズ アクセス ポイント
- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 2600 シリーズ アクセス ポイント
- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 3500 シリーズ アクセス ポイント
- Cisco Aironet 3600 シリーズ アクセス ポイント



- Cisco Aironet 3700 シリーズ アクセス ポイント



(注) Cisco ATF はローカル モードと FlexConnect モードの AP でのみサポートしています。

### Cisco ATF モード

Cisco ATF は以下のモードで動作します。

- 次の操作をユーザが実行できる監視モード：
  - 通信時間の表示
  - すべての AP 送信の通信時間の報告
  - レポートの表示
    - SSID/WLAN 単位
    - AP グループ単位
    - AP 単位
    - クライアントごと
  - 通信時間の使用量の定期報告
  - ブロック ACK は報告しません
  - モニタ モードの一部としての適用なし
- 次の操作をユーザが実行できるポリシー適用モード：
  - 設定したポリシーに基づいて通信時間を適用
  - 次の項目に通信時間を適用
    - 単独の WLAN
    - Cisco WLC ネットワーク内で接続されているすべての AP
    - 単独の AP グループ
    - 単独の AP
    - 単独のクライアント
  - 複数のポリシーを持った複数の WLAN を 1 つの AP に設定できます (1:16)
  - WLAN 単位の厳密な適用：無線 WLAN で使用する通信時間は、ポリシーの設定限度を上限として厳密に適用されます
  - WLAN 単位の最適な適用：他の SSID が未使用の通信時間を共有します

- すべてのポリシーを合計すると、100 パーセントになります。これを超過することはありません。

### Cisco Air Time Fairness の制限

- ATF を実装できるのはダウン ストリーム方向のデータ フレームのみです。
- SSID 単位モードで ATF を設定すると、すべての WLAN を無効にしないと ATF 設定コマンドを入力できません。すべての ATF コマンドを入力したら WLAN を有効にできます。

### Cisco Air Time Fairness (ATF) の使用例

#### 公共ホットスポット (スタジアム/空港/会議場/その他)

この場合、パブリック ネットワークは2つ (またはそれ以上) のサービスプロバイダーと施設間で WLAN を共有しています。各サービス プロバイダーのサブスクリバをグループに分けて、各グループに一定割合の通信時間を割り当てることができます。

#### Education

この場合、大学は、学生、教員、およびゲスト間でWLANを共有しています。ゲストネットワークは、サービスプロバイダーによってさらに分割できます。各グループに一定割合の通信時間を割り当てることができます。

#### エンタープライズ/サービス/小売

この場合、施設は、従業員とゲスト間でWLANを共有しています。ゲストネットワークは、サービスプロバイダーによってさらに分割できます。これらのゲストをサービスの種類別の層でさらに細分化したサブグループに分けて、一定割合の通信時間を割り当てることができます。たとえば、有料グループには、無料グループより多くの通信時間が与えられます。

#### 時間を共有する管理型ホットスポット

この場合、サービスプロバイダーや企業などのホットスポットを管理するビジネスエンティティは、通信時間を割り当てて他のビジネス エンティティにリースすることができます。

次に、Cisco ATF の設定手順の概要を示します。

- 1 モニタ モードを有効にして、ネットワーク使用量を測定します (オプション)。
- 2 Cisco ATF ポリシーを作成します。
- 3 ネットワーク、AP グループ、または個別の AP 単位で WLAN ATF ポリシーを追加します。AP または AP グループに設定したポリシーは、ネットワークポリシーごとにオーバーライドしません。
- 4 最適化を有効にするかどうかを決定します。
- 5 Cisco ATF の統計情報を定期的に確認します。

### 関連資料

Air Time Fairness の詳細については、[『Air Time Fairness\(ATF\) Phase 1 and Phase 2 Deployment Guide』](#)を参照してください。

## Cisco Air Time Fairness の設定 (GUI)

### Cisco ATF モニタ モードの設定 (GUI)

- 
- ステップ 1 [Wireless] > [ATF] > [Monitor Configuration] の順に選択します。
  - ステップ 2 [ATF Monitor Mode Configuration] ページで、AP、AP グループ、またはネットワーク全体を選択します。ネットワーク全体を選択した場合、無線タイプを指定します。
  - ステップ 3 [Enable] をクリックします。
  - ステップ 4 設定を保存します。
- 

### Cisco ATF ポリシーの設定 (GUI)

- 
- ステップ 1 [Wireless] > [ATF] > [Policy Configuration] の順に選択します。
  - ステップ 2 [ATF Policy Configuration] ページで、ATF ポリシーの ID、名前、またはウェイトを指定して、[Create] をクリックします。  
合計が 100 を超えることができるよう、パーセンテージではなくウェイト比率が使用されます。設定可能なウェイトの最小値は 10 です。
  - ステップ 3 ポリシーに Client Fair Sharing を適用するには [Client Fair Sharing] チェックボックスをオンにします。
  - ステップ 4 設定を保存します。
-

## Cisco ATF Enforcement SSID の設定 (GUI)

- 
- ステップ 1 [Wireless] > [ATF] > [Enforcement SSID Configuration] の順に選択します。
- ステップ 2 [ATF Enforcement SSID Configuration] ページで、作成された ATF ポリシーを無線タイプが指定された AP、AP グループ、またはネットワーク全体に適用します。
- ステップ 3 適用タイプとして [Optimized] または [Strict] を選択します。
- ステップ 4 [Enable] をクリックします。
- ステップ 5 WLAN および ATF ポリシーを選択し、[Add] をクリックして WLAN に ATF ポリシーを適用します。
- ステップ 6 設定を保存します。
- 

## ATF 統計情報のモニタリング (GUI)

---

使用された時間のパーセンテージで AP ATF 統計情報あたり WLAN ごとにモニタするには、[Wireless] > [ATF] > [ATF Statistics] の順に選択します。統計情報を表示するには、ドロップダウン リストの AP 名を選択します。

- abs : SSID ごとに使用される通信時間単位の数
  - 相対時間 : SSID ごとに使用される時間のパーセンテージ
  - 合計通信時間 : SSID ごとに使用される通信時間の合計
- 

## Cisco Air Time Fairness の設定 (CLI)

- 次のコマンドを入力して、ネットワーク レベル (グローバル) で Cisco ATF を設定します。
  - `config atf 802.11 {a | b} mode disable`
  - `config atf 802.11 {a | b} mode monitor`
  - `config atf 802.11 {a | b} mode enforce-policy`
  - `config atf 802.11 {a | b} optimization {enable | disable}`
- 次のコマンドを入力して、AP グループごとに Cisco ATF を設定します。
  - `config wlan apgroup atf 802.11 {a | b} mode disable ap-group-name`
  - `config wlan apgroup atf 802.11 {a | b} mode monitor ap-group-name`
  - `config wlan apgroup atf 802.11 {a | b} mode enforce-policy ap-group-name`

- **config wlan apgroup atf 802.11 {a | b} optimization {enable | disable} ap-group-name**
- 次のコマンドを入力して、AP の無線ごとに Cisco ATF を設定します。
  - **config ap atf 802.11 {a | b} mode disable ap-name**
  - **config ap atf 802.11 {a | b} mode monitor ap-name**
  - **config ap atf 802.11 {a | b} mode enforce-policy ap-name**
  - **config ap atf 802.11 {a | b} optimization {enable | disable} ap-name**
- 次のコマンドを入力して、ATF ポリシーを設定します。
  - **config atf policy create policy-id policy-name policy-weight**
  - **config atf policy modify {weight policy-weight policy-name} | {client-sharing {enable | disable} policy-name}**
  - **config atf policy delete policy-name**
- 次のコマンドを入力して、ポリシー ID のある WLAN を設定します。
  - **config wlan atf wlan-id policy policy-id**
- 次のコマンドを入力して、WLAN で Cisco ATF ポリシーの AP グループ レベルの Override を設定します。
  - **config wlan apgroup atf 802.11 {a | b} policy ap-group-name wlan-id policy-name override {enable | disable}**
- 次のコマンドを入力して、WLAN で Cisco ATF ポリシーの AP レベルの Override を設定します。
  - **config ap atf 802.11 {a | b} policy wlan-id policy-name ap-name override {enable | disable}**
- 次のコマンドを入力して、Cisco ATF 設定をモニタします。
  - **show atf config all**
  - **show atf config ap-name ap-name**
  - **show atf config apgroup ap-group-name**
  - **show atf config 802.11 {a | b}**
  - **show atf config policy**
  - **show atf config wlan**
  - **show atf statistics ap ap-name 802.11 {a | b} summary**
  - **show atf statistics ap ap-name 802.11 {a | b} wlan wlan-id**
  - **show atf statistics ap ap-name 802.11 {a | b} policy policy-name**





# 第 135 章

## Cisco Universal Small Cell 8x18 デュアルモード モジュール

- [Cisco Universal Small Cell 8x18 デュアルモード モジュールについて, 1001 ページ](#)
- [Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定, 1002 ページ](#)
- [さまざまなシナリオでの USC8x18 デュアルモード モジュールの設定, 1003 ページ](#)

### Cisco Universal Small Cell 8x18 デュアルモード モジュールについて

Cisco Universal Small Cell 8x18 デュアルモード モジュールは、Cisco Aironet 3600I AP または Cisco Aironet 3700I AP に接続できる外部モジュール（4G/LTE）です。次の機能を使用できます。

- 次のモードの外部モジュールのトラフィックの VLAN タギングを設定できます。

モード	ネイティブ VLAN	非ネイティブ VLAN
FlexConnect ローカル スイッチング	サポートあり	サポートあり
ローカルモードの中央スイッチング	サポートあり	サポートあり

- このモジュールは、PoE+ 電源を使用できます
- 2.4 GHz Wi-Fi と 3G/4G モジュールを有効にしたときの共存検出と警告
- モジュールのインベントリ詳細は、Cisco WLC GUI から、[Wireless] > [Access Points] > *Access Point name* > [Inventory] で入手できます。
- 以下のシスコ ワイヤレス コントローラ モデルでサポートしています。
  - Cisco 2504 WLC

- Cisco 5508 WLC
  - Cisco 5520 WLC
  - Cisco Flex 7510 WLC
  - Cisco 8510 WLC
  - Cisco 8540 WLC
  - Cisco Virtual Controller
  - Cisco WiSM2
- 以下のシスコ アクセス ポイント モデルでサポートしています。
- Cisco Aironet 3600I AP
  - Cisco Aironet 3700I AP

#### 機能制限

Cisco Universal Small Cell 8x18 デュアルモード モジュールは、以下のシスコ アクセスポイント モデルではサポートしていません。

- Cisco Aironet 3600E AP
- Cisco Aironet 3700E AP

Cisco Universal Small Cell 8x18 デュアルモード モジュールの詳細については、<http://www.cisco.com/c/en/us/support/wireless/universal-small-cell-8000-series/tsd-products-support-series-home.html> を参照してください。

## Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定

### Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定 (GUI)

- 
- ステップ 1** [Wireless] > [Access Points] > [All APs] を選択します。
- ステップ 2** AP 名をクリックします。  
[All APs > Details] ページが表示されます。
- ステップ 3** [Advanced] タブで、[External Module Status] チェックボックスをオフにします。  
2.4 GHz の Wi-Fi と 3G/4G モジュールを有効にすると、共存の警告が表示される場合があります。
-



## Cisco Universal Small Cell 8x18 デュアルモード モジュールの設定 (CLI)

- 次のコマンドを入力して、Cisco USC 8x18 デュアルモード モジュールを有効または無効にします。

```
config ap module3G {enable | disable} ap-name
```

2.4 GHz の Wi-Fi と 3G/4G モジュールを有効にすると、共存の警告が表示される場合があります。

## さまざまなシナリオでの USC8x18 デュアルモード モジュールの設定

### FlexConnect ローカルスイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (GUI)

- 
- ステップ 1** [Wireless] > [Access Points] > [All APs] を選択します。
- ステップ 2** AP 名をクリックします。  
[All APs > Details] ページが表示されます。
- ステップ 3** [FlexConnect] タブで [VLAN Support] チェックボックスをオンにし、[Native VLAN ID] ボックスにリモートネットワーク上のネイティブ VLAN の番号 (100 など) を入力します。
- ステップ 4** 0 以外の VLAN ID を使用して FlexConnect ローカルスイッチングを有効にするには、以下の手順を実行します。
- [External Module] の下の [FlexConnect Local Switching] を有効にします。
  - VLAN ID ボックスに 2 ~ 4096 の範囲の値を入力します。
  - [Apply] をクリックします。
- ステップ 5** 0 に等しい VLAN ID を使用して FlexConnect ローカルスイッチングを有効にするには、以下の手順を実行します。
- [External Module] の下の [FlexConnect Local Switching] を有効にします。
  - [Apply] をクリックします。
- ステップ 6** AP 設定ごとに FlexConnect ローカルスイッチングを削除するには、[Remove AP Specific Config] をクリックします。
- ステップ 7** 設定を保存します。
- 

### FlexConnect ローカルスイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (CLI)

- `config ap flexconnect module-vlan enable ap-name` : 外部モジュールに対し、ネイティブ VLAN を使用して FlexConnect ローカルスイッチングを有効にします。

- **config ap flexconnect module-vlan remove***ap-name* : AP 固有の外部モジュール VLAN 構成を削除します。
- **config ap flexconnect module-vlan enable***ap-name***vlan***vlan-id* : 外部モジュールに対し、非ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にします。
- **show ap module summary** {*ap-name* | **all**} : 外部モジュールに関する詳細情報を表示します。
- **show ap inventory** {*ap-name* | **all**} : AP のインベントリと外部モジュール（モジュールが存在する場合）に関する情報を表示します。
- **show ap flexconnect module-vlan***ap-name* : FlexConnect ローカル スイッチングのステータスと VLAN ID 値を表示します。
- **show ap config general***ap-name* : 外部モジュールに関する情報を表示します（モジュールが存在する場合）。

## FlexConnect グループ ローカル スイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (GUI)

- 
- ステップ 1 [Wireless] > [FlexConnect Groups] を選択します。
- ステップ 2 [New] をクリックし、FlexConnect グループ名を入力して [Apply] をクリックします。
- ステップ 3 [FlexConnect Groups] > [Edit] ページの [FlexConnect APs] 領域で、[Add AP] をクリックします。
- ステップ 4 Cisco WLC に関連付けられた AP のリストから AP を選択することも、Cisco WLC に関連付けられた AP のイーサネット MAC アドレスを直接指定することもできます。
- ステップ 5 [Add] をクリックします。
- ステップ 6 VLAN ID を使用して FlexConnect ローカル スイッチングを有効にするには、以下の手順を実行します。
- [External Module Configuration] の下の [FlexConnect Local Switching] を有効にします。
  - VLAN ID ボックスに 2 ~ 4096 の範囲の値を入力します。
  - [Apply] をクリックします。
- ステップ 7 設定を保存します。
- 

## FlexConnect グループ ローカル スイッチングにおける USC8x18 デュアルモード モジュール用の VLAN タギングの設定 (CLI)

- **config flexconnect group***group-name***module-vlan enable** **vlan***vlan-id* : FlexConnect グループに対して FlexConnect ローカル スイッチングを有効にします。
- **config flexconnect group***group-name***module-vlan disable** : FlexConnect グループに対して FlexConnect ローカル スイッチングを無効にします。

- **show flexconnect group detail***group-name***module-vlan** : グループ内の FlexConnect ローカル スイッチングのステータスと VLAN ID を表示します。

## ローカル モード中央スイッチングでの USC8x18 デュアルモード モジュールの設定 (GUI)

- 
- ステップ 1** リモート LAN を作成します。  
リモート LAN を作成するための手順については、「*WLAN*」の「リモート *LAN* の設定」を参照してください。
- ステップ 2** [WLANs > Edit] ページで [Security] タブをクリックします。
- ステップ 3** [Layer 2] サブタブで、[MAC Filtering] チェックボックスをオフにします。  
(注) リモート LAN はオープンセキュリティでのみ設定する必要があります。802.1X セキュリティはサポートされていません。
- ステップ 4** 3G/4G クライアントの現在の状態を表示するには、[Monitor] > [Clients] を選択して [Clients] ページを開きます。
- ステップ 5** 設定を保存します。
- 

## ローカル モード中央スイッチングでの USC8x18 デュアルモード モジュールの設定 (CLI)

- リモート LAN を作成します。  
リモート LAN を作成するための手順については、「*WLAN*」の「リモート *LAN* の設定」を参照してください。
- **config interface 3g-vlan***interface-name* {**enable** | **disable**} : 3G/4G-VLAN インターフェイスを有効または無効にします。
- **show interface detailed***interface-name* : 3G/4G-VLAN フラグのステータスを表示します。
- **show client summary ip** : 3G/4G クライアントのステータスを表示します。





## 第 **VII** 部

### 無線リソース管理の設定

- [RRM の設定, 1009 ページ](#)
- [RF グループの設定, 1033 ページ](#)
- [RRM の無効化, 1041 ページ](#)
- [CCX 無線管理機能の設定, 1049 ページ](#)
- [設定の最適化されたローミング, 1055 ページ](#)
- [パケットの検出しきい値設定のレシーバ起動, 1059 ページ](#)





# 第 136 章

## RRM の設定

- 無線リソース管理について, 1009 ページ
- RRM の設定に関する制限, 1015 ページ
- RF グループ モードの設定 (GUI) , 1015 ページ
- RF グループ モードの設定 (CLI) , 1016 ページ
- 送信電力制御の設定 (GUI) , 1017 ページ
- Off-Channel Scanning Defer の設定, 1018 ページ
- RRM の設定 (CLI) , 1027 ページ
- RRM 設定の表示 (CLI) , 1031 ページ
- RRM 問題のデバッグ (CLI) , 1032 ページ

### 無線リソース管理について

無線リソース管理 (RRM) ソフトウェアは Cisco ワイヤレス LAN コントローラに組み込まれており、ワイヤレスネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、Cisco WLC は次の情報について、アソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- **トラフィックの負荷**：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- **干渉**：他の 802.11 発信元から送られてくるトラフィック量。
- **ノイズ**：現在割り当てられているチャンネルに干渉している 802.11 以外のトラフィック量。
- **カバレッジ**：接続されているすべてのクライアントの受信信号強度インジケータ (RSSI) と信号対雑音比 (SNR)。
- **その他**：近くにあるアクセス ポイントの数。

RRM は、この情報を使用して、最も効率がよくなるように 802.11 RF ネットワークを定期的に再設定できます。そのために、RRM では次の機能を実行します。

- 無線リソースの監視
- 送信電力の制御
- 動的チャネル割り当て
- カバレッジ ホールの検出と修正

## 無線リソースの監視

RRM は、ネットワークに追加された新しい Cisco WLC や Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントは、使用国で有効なすべての 802.11a/b/g チャネルに加えて、他の地域で使用可能なチャネルも同時にスキャンできます。アクセス ポイントは、これらのチャネルのノイズや干渉を監視する際、最大で 60 ミリ秒の間「オフチャネル」になります。不正アクセス ポイント、不正クライアント、アドホッククライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。



(注) 過去 100 ミリ秒の間に音声トラフィックがある場合、アクセス ポイントによるオフチャネル測定が延期されます。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。



(注) ネットワーク内に不正なアクセス ポイントが多数存在する場合は、FlexConnect またはローカルモード アクセス ポイントでチャネル 157 または 161 上の不正を検出する可能性が小さくなります。このような場合は、監視モード AP を不正の検出に使用できます。

## 送信電力の制御

Cisco WLC は、リアルタイム ワイヤレス LAN の状況に基づいて、アクセス ポイントの送信電力を動的に制御します。TPCv1 および TPCv2 の 2 つのバージョンの送信電力制御から選択できます。TPCv1 では、通常電力を低く維持することでキャパシティを増やし、干渉を減らします。TPCv2 では、干渉を最小にするために、送信電力を動的に調整します。TPCv2 は、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジホールのインシデントが多く発生する可能性があります。

送信電力制御 (TPC) アルゴリズムによって、RF 環境での変化に応じて、アクセス ポイントの電力が増減します。多くの場合、TPC は干渉を低減させるため、アクセス ポイントの電力を下げよ



うとします。しかし、アクセスポイントで障害が発生したり、アクセスポイントが無効になったりして、RF カバレッジに急激な変化があると、TPC は周囲のアクセスポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジホールの検出とは異なります。TPC はアクセスポイント間におけるチャネルの干渉を最小限に抑えながら、必要なカバレッジレベルを達成するため、十分な RF 電力を提供します。

次の表に、電力レベルマッピングを示します。

電力レベル	2.4 GHz	5 GHz
1	23 dBm (200 mW) CCK のみ	20 dBm (100 mW)
2	20 dBm (100 mW)	17 dBm (50 mW)
3	17 dBm (50 mW)	14 dBm (25 mW)
4	14 dBm (25 mW)	11 dBm (12.5 mW)
5	11 dBm (12.5 mW)	8 dBm (6.25 mW)
6	8 dBm (6.25 mW)	5 dBm (3.13 mW)
7	5 dBm (3.13 mW)	2 dBm (1.56 mW)
8	2 dBm (1.56 mW)	-1 dBm (0.78 mW)
	-1 dBm (0.78 mW)	

### 最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPC アルゴリズムは、数多くのさまざまな RF 環境で RF 電力を分散させます。ただし、自動パワー制御では、アーキテクチャの制約事項またはサイトの制約事項のため、適切な RF 設計を実装できなかった一部のケースは解消できない可能性があります。たとえば、すべてのアクセスポイントが互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPC の推奨を無効化することができます。最大および最小の TPC 電力設定は、RF ネットワークの RF プロファイルを通じてすべてのアクセスポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ページのテキストボックスに RRM が使用する最大および最小の送信電力を入力します。これらのパラメータの範囲は -10 ~ 30 dBm です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM では、コントローラに接続されているすべてのアクセスポイントはこの送信電力レベルを上回ることはできません（電力は RRM TPC またはカバレッジホールの検出により設定されます）。たとえば、最大送信電力を 11 dBm に設定すると、アクセスポイントを手動で設定しない限りは、11 dBm を上回って伝送を行うアクセスポイントはありません。

## 動的チャネル割り当て

同じチャネル上の2つの隣接するアクセスポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突の場合、アクセスポイントではデータが受信されません。この動作は問題になることがあります。たとえば、誰かがカフェで電子メールを読むことで、近隣の会社のアクセスポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル1を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。コントローラはアクセスポイントチャネル割り当てを動的に割り当てて、衝突を回避し、キャパシティとパフォーマンスを改善することができます。チャネルは「再利用」され、希少なRFリソースが浪費されるのを防ぐことができます。つまり、チャネル1はカフェから離れた別のアクセスポイントに割り当てられます。これは、チャネル1をまったく使用しない場合に比べてより効率的です。

コントローラの動的チャネル割り当て（DCA）機能は、アクセスポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、1や2など、802.11b/g帯域の2つのオーバーラップするチャネルでは、両方が同時に11/54Mbpsを使用することはできません。コントローラは、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。



（注） 重複しないチャネル（1、6、11、など）だけの使用を推奨します。

コントローラは、さまざまなリアルタイムのRF特性を検証して、次のようにチャネルの割り当てを効率的に処理します。

- **アクセスポイントの受信エネルギー**：各アクセスポイントとその近隣のアクセスポイント間で測定された受信信号強度。チャネルを最適化して、ネットワークキャパシティを最大にします。
- **ノイズ**：ノイズによって、クライアントおよびアクセスポイントの信号の品質が制限されます。ノイズが増加すると、有効なセルサイズが小さくなり、ユーザエクスペリエンスが低下します。コントローラでは、ノイズ源を避けるようにチャネルを最適化することで、システムキャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- **802.11干渉**：干渉とは、不正アクセスポイントや近隣の無線ネットワークなど、無線LANに含まれない802.11トラフィックのことです。Lightweightアクセスポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。802.11干渉の量が定義済みの設定可能なしきい値（デフォルトは10%です）を超えると、アクセスポイントからコントローラにアラートが送信されます。その場合、コントローラでは、RRMアルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステムパフォーマンスを向上させることができます。このような調整によって、隣接するLightweightアクセスポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセスポイントが原因で使用できないチャネルにアクセスポイントを割り当てたままにしておくよりも効果的です。

また、他の無線ネットワークがある場合、コントローラは、他のネットワークを補足するようにチャンネルの使用を変更します。たとえば、チャンネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャンネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャンネルにキャパシティがほとんど残っていない場合、コントローラはそのチャンネルを回避できます。すべての非オーバーラップチャンネルが使用される非常に高密度の展開では、コントローラでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。

- 負荷および利用率：利用率の監視が有効な場合、（たとえば、ロビーとエンジニアリングエリアを比較して）一部のアクセスポイントが他のアクセスポイントよりも多量のトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。これによってコントローラは、最も低いパフォーマンスが報告されているアクセスポイントを改善するようにチャンネルを割り当てることができます。チャンネル構造を変更する際には、負荷を考慮して、現在無線 LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセスポイントの送信パケットおよび受信パケットの数が追跡されて、アクセスポイントのビジー状態が測定されます。新しいクライアントは過負荷のアクセスポイントを回避し、別のアクセスポイントにアソシエートします。このパラメータはデフォルトでは無効になっています。

コントローラは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、軟判定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3次元空間における最適なチャンネル設定が実現します。この場合、上下のフロアにあるアクセスポイントが全体的な無線 LAN 設定において主要な役割を果たします。



(注) 2.4GHz 帯域の 40 MHz チャンネル、または 80 MHz チャンネルを使用する無線は、DCA ではサポートされていません。

RRM スタートアップ モードは、次のような状況で起動されます

- シングルコントローラ環境では、RRM スタートアップ モードは、コントローラがリブートしてから起動されます。
- マルチコントローラ環境では、RRM スタートアップ モードは、RF グループ リーダーが選定されてから起動されます。

CLI から RRM スタートアップ モードを開始できます。

RRM スタートアップ モードは、100 分間（10 分間隔で 10 回繰り返し）実行されます。RRM スタートアップ モードの持続時間は、DCA 間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードには、定常ステートチャンネル計画に収束するために 10 回の高感度な（チャンネルを容易に環境に対して敏感に変更する）DCA 実行が含まれます。スタートアップ モードが終了した後、DCA は指定した間隔と感度で実行を継続します。

## カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線LANの無線カバレッジの領域を検出することができます。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）でLightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントから コントローラに「カバレッジホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセスポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。コントローラでは、修正可能なカバレッジホールと不可能なカバレッジホールが識別されます。修正可能なカバレッジホールの場合、コントローラでは、その特定のアクセスポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジホールがコントローラによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

## RRM の利点

RRMによって、最適なキャパシティ、パフォーマンス、および信頼性を備えたネットワークが構築されます。一過性でトラブルシューティングが困難なノイズや干渉の問題を確認するために常時ネットワークを監視する必要がなくなります。RRMによって、クライアントはCisco Unified Wireless Network 経由による、シームレスで円滑な接続を利用できるようになります。

RRMでは、配備されているネットワーク（802.11a および 802.11b/g）ごとに監視と制御が実施されます。つまり、無線タイプ（802.11a および 802.11b/g）ごとにRRMアルゴリズムが実行されます。RRMでは、測定とアルゴリズムの両方が使用されます。RRMによる測定については、監視間隔を使用して調整できます。ただし、RRMを無効にすることはできません。RRMアルゴリズムは自動的に有効になりますが、チャネルや電力の割り当てを静的に設定することで無効にすることができます。RRMアルゴリズムは、指定された更新間隔（デフォルトでは600秒）で実行されます。

## RRM の設定について

コントローラで事前設定されたRRM設定は、ほとんどの展開向けに最適化されています。ただし、GUIまたはCLIを使用して、コントローラのRRM設定パラメータをいつでも変更できます。

RFグループの一部であるコントローラ上、またはRFグループの一部でないコントローラ上で、これらのパラメータを設定できます。

RRMパラメータは、RFグループ内のすべてのコントローラで同じ値に設定する必要があります。RFグループリーダーは、コントローラのレポートの結果として、または互いに受信する無線に応じて変更される可能性があります。RRMパラメータの異なるRFグループメンバがある場合は、グループリーダーが変更されると、異なる結果が生じることがあります。

コントローラの GUI を使用して設定できる RRM パラメータは、RF グループ モード、送信電力の制御、動的チャンネル割り当て、カバレッジ ホールの検出、プロファイルしきい値、監視チャンネル、および監視間隔です。

## RRM の設定に関する制限

- OEAP 600 シリーズのアクセス ポイントは、RRM をサポートしません。600 シリーズ OEAP アクセス ポイントの無線は、Cisco WLC ではなく、600 シリーズ アクセス ポイントのローカル GUI で管理されます。Cisco WLC からスペクトラム チャンネルや電力を管理しようとして、無線を無効化したりしても、600 シリーズ OEAP には反映されません。

## RF グループ モードの設定 (GUI)

**ステップ 1** [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [RF Grouping] の順に選択して、[802.11a (または 802.11b/g) > RRM > RF Grouping] ページを開きます。

**ステップ 2** [Group Mode] ドロップダウン リストから、この Cisco WLC に対して設定するモードを選択します。次のモードで RF グループ化を設定できます。

- auto : RF グループ選択を自動更新モードに設定します。
- leader : RF グループ選択を静的モードに設定し、この Cisco WLC をグループ リーダーとして設定します。
- off : RF グループ選択をオフに設定します。すべての Cisco WLC が自身のアクセス ポイント パラメータを最適化します。

(注) 設定したスタティック リーダーは、モードが「auto」に設定されるまで、他の Cisco WLC のメンバになることはできません。

(注) 優先順位が高い Cisco WLC が使用可能な場合、優先順位がより低い Cisco WLC はグループ リーダーのロールを担うことはできません。ここでの優先順位は、Cisco WLC の処理能力に関連しています。

(注) Cisco WLC が自動 RF グループ化に加わるように設定することをお勧めします。RRM の設定を無効にする際には、自動 RF グループ化への参加を無効にする必要はありません。

**ステップ 3** [Apply] をクリックして設定を保存し、[Restart] をクリックして RRM RF グループ化アルゴリズムを再起動します。

**ステップ 4** この Cisco WLC に対して、スタティック リーダーとして RF グループ化モードを設定した場合、次のように [RF Group Members] セクションからグループ メンバを追加することができます。

- 1 [Cisco WLC Name] テキスト ボックスに、このグループにメンバーとして追加する Cisco WLC を入力します。
- 2 [IP Address] テキスト ボックスに、Cisco WLC の IP アドレスを入力します。

3 [Add Member] をクリックして、このグループにメンバを追加します。

(注) メンバがスタティックリーダーにjoinされない場合は、失敗の理由がカッコ内に表示されません。

ステップ5 [Apply] をクリックします。

ステップ6 [Save Configuration] をクリックします。

## RF グループモードの設定 (CLI)

ステップ1 次のコマンドを入力して、RF グループ化モードを設定します。

```
config advanced {802.11a | 802.11b} group-mode {auto | leader| off| restart}
```

- auto : RF グループ選択を自動更新モードに設定します。
- leader : RF グループ選択を静的モードに設定し、この Cisco WLC をグループリーダーとして設定します。
- off : RF グループ選択をオフに設定します。すべての Cisco WLC が自身のアクセスポイントパラメータを最適化します。
- restart : RF グループ選択を再起動します。

(注) 設定したスタティックリーダーは、モードが「auto」に設定されるまで、他の Cisco WLC のメンバになることはできません。

(注) 優先順位が高い Cisco WLC が使用可能な場合、優先順位がより低い Cisco WLC はグループリーダーのロールを担うことはできません。ここでの優先順位は、Cisco WLC の処理能力に関連しています。

ステップ2 次のコマンドを入力して、RF グループのスタティックメンバとして Cisco WLC を追加または削除します (モードが「leader」に設定されている場合)。

- **config advanced {802.11a | 802.11b} group-member add controller\_name controller\_ip\_address**
- **config advanced {802.11a | 802.11b} group-member remove controller\_name controller\_ip\_address**

ステップ3 次のコマンドを入力して、RF グループ化のステータスを表示します。

```
show advanced {802.11a | 802.11b} group
```

## 送信電力制御の設定 (GUI)

**ステップ 1** [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [TPC] の順に選択して、[802.11a/n/ac (または 802.11b/g/n) > RRM > Tx Power Control (TPC)] ページを開きます。

**ステップ 2** 次のオプションから送信電力制御のバージョンを選択します。

- **[Interference Optimal Mode (TPCv2)]** : ボイスコールが広く使用されている場合に選択します。干渉を最小にするために、送信電力が動的に調整されます。これは、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジホールのインシデントが多く発生する可能性があります。

(注) RF 問題が TCPv1 で解決できない場合 TCPv2 のみを使用することを推奨します。シスコサービスの支援を受けて、TPCv2 の使用を評価し、テストしてください。

- **[Coverage Optimal Mode (TPCv1)]** : (デフォルト) 強力な信号カバレッジと安定性を提供します。このモードでは、送信電力を低く維持することでキャパシティを増やし、干渉を減らします。

**ステップ 3** [Power Level Assignment Method] ドロップダウンリストから次のオプションのいずれかを選択して、Cisco WLC の動的電力割り当てモードを指定します。

- **[Automatic]** : Cisco WLC よって、join しているすべてのアクセスポイントの送信電力が定期的に評価され、必要に応じて更新されます。これは、デフォルト値です。
- **[On Demand]** : Cisco WLC によって、join しているすべてのアクセスポイントの送信電力が定期的に評価されます。ただし、[Invoke Power Update Now] をクリックした場合のみ、必要に応じて Cisco WLC によって電力が更新されます。

(注) [Invoke Power Update Now] をクリックしても、Cisco WLC による送信電力の評価と更新がすぐに行われるわけではありません。次の間隔 (600 秒) まで待機します。この値は設定可能です。

- **[Fixed]** : Cisco WLC によって、join しているアクセスポイントの送信電力が評価されたり、必要に応じて更新されたりすることはありません。電力レベルは、ドロップダウンリストから選択した固定値に設定されます。

(注) 送信電力レベルには、mW 単位または dBm 単位の値の代わりに整数値が割り当てられます。この整数は、アクセスポイントが展開されている規制ドメイン、チャンネル、およびアンテナによって異なる電力レベルに対応します。

(注) 最適なパフォーマンスを確保するには、[Automatic] 設定を使用することを、お勧めします。

**ステップ 4** [Maximum Power Level Assignment] および [Minimum Power Level Assignment] テキストボックスに最大および最小の電力レベル割り当て値を入力します。

[Maximum Power Level Assignment] の範囲は、-10 ~ 30 dBm です。

[Minimum Power Level Assignment] の範囲は、-10 ~ 30 dBm です。

**ステップ 5** [Power Threshold] テキスト ボックスに、アクセス ポイントの電力を減らすかどうか判断する際に RRM で使用する切断信号レベルを入力します。このパラメータのデフォルト値は TPCv1 で -70 dBm、TPCv2 で -67 dBm ですが、アクセス ポイントの送信電力レベルが必要以上に高い（または低い）場合は変更できません。

このパラメータの範囲は -80 ~ -50 dBm です。この値を -65 ~ -50 dBm の範囲で増やすと、アクセス ポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。

多数のアクセス ポイントを使用しているアプリケーションでは、ワイヤレス クライアントが認識する BSSID（アクセス ポイント）やビーコンの数を少なくするために、しきい値を -80 dBm または -75 dBm に下げることが有用です。一部のワイヤレス クライアントは多数の BSSID や高速ビーコンを処理できない場合があります、デフォルトのしきい値では、問題のある動作を起こす可能性があります。

このページには、次のような送信電力レベルのパラメータの設定も表示されますが、これらは設定できません。

- [Power Neighbor Count] : 送信電力制御アルゴリズムを実行するためにアクセス ポイントに必要なネイバーの最小数です。
- [Power Assignment Leader] : パワー レベルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- [Last Power Level Assignment] : RRM が現在の送信電力レベルの割り当てを最後に評価した時間です。

**ステップ 6** [Apply] をクリックします。

**ステップ 7** [Save Configuration] をクリックします。

## Off-Channel Scanning Defer の設定

### オフチャネル スキャンの延期について

特定の省電力モードのクライアントが展開される環境で、小容量クライアント（たとえば、省電力モードを使用し定期的にテレメトリ情報を送信する医療用デバイス）からの重要情報の欠落を防ぐために、場合によっては、無線リソース管理（RRM）の正常なオフチャネルスキャンを延期する必要があります。この機能は、Quality of Service（QoS）と RRM スキャン延期機能との相互作用の方法を向上させます。

クライアントの Wi-Fi マルチメディア（WMM）UP マーキングを使用して、UP がマークされたパケットを受信した場合に、設定可能な期間中オフチャネルスキャンを延期するアクセス ポイントを設定することができます。

[Off-Channel Scanning Defer] は、ノイズや干渉など代替チャンネル選択に関する情報を収集する RRM を使用するとき重要となります。また、[Off-Channel Scanning Defer] は、不正検出を行います。[Off-Channel Scanning Defer] を提供する必要があるデバイスは、可能な限り、同じ WLAN を使用する必要があります。このようなデバイスが多くある場合（この機能を使用して Off-Channel Defer スキャンが完全に無効化されている可能性があります）、モニタ アクセス ポイントや、この



WLANが割り当てられていない同じ位置にあるその他のアクセスポイントなど、代わりにローカル AP で [Off-Channel Scanning Defer] を実装する必要があります。

QoS ポリシー (Bronze、Silver、Gold、Platinum) を WLAN に割り当てることで、クライアントからアップリンクでどのように受信されたかに関係なく、パケットがアクセスポイントからのダウンリンク接続でどのようにマーキングされるかを制御できます。UP=1,2 は最低の優先順位で、UP=0,3 はその次に高い優先順位です。各 QoS ポリシーのマーキング結果は次のとおりです。

- Bronze は、すべてのダウンリンク トラフィックを UP= 1 にマーキングします。
- Silver は、すべてのダウンリンク トラフィックを UP=0 にマーキングします。
- Gold は、すべてのダウンリンク トラフィックを UP= 4 にマーキングします。
- Platinum は、すべてのダウンリンク トラフィックを UP= 6 にマーキングします。

## WLAN に対する Off-Channel Scanning Defer の設定

### WLAN に対する Off-Channel Scanning Defer の設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 Off-Channel Scanning Defer を設定する WLAN の ID 番号をクリックします。
- ステップ 3 [WLANs > Edit] ページから [Advanced] タブを選択します。
- ステップ 4 [Off Channel Scanning Defer] セクションで、プライオリティ引数をクリックすることにより [Scan Defer Priority] を設定します。
- ステップ 5 [Scan Defer Time] テキスト ボックスにミリ秒単位で時間を設定します。  
有効な値は、100 ~ 60000 です。デフォルト値は 100 ミリ秒です。
- ステップ 6 設定を保存するには、[Apply] をクリックします。
- 

### WLAN に対する Off-Channel Scanning Defer の設定 (CLI)

- 
- ステップ 1 次のコマンドを入力して、チャンネル スキャンの延期プライオリティを割り当てます。  
**config wlan channel-scan defer-priority priority [enable | disable] WLAN-id**  
priority 引数の有効範囲は 0 ~ 7 です。  
priority は 0 ~ 7 です (この値は、クライアントおよび WLAN では 6 に設定する必要があります)。  
このコマンドを使用して、キュー内の UP パケットを受けてスキャンが延期される時間を設定します。このコマンドを使用して、キュー内の UP パケットを受けてスキャンが延期される時間を設定します。
- ステップ 2 次のコマンドを入力して、チャンネル スキャン延期時間 (ミリ秒単位) を割り当てます。

**config wlan channel-scan defer-time msec WLAN-id**

時間の値はミリ秒 (ms) 単位で、有効な範囲は 100 (デフォルト) ~ 60000 (60 秒) です。この設定は、お使いの無線 LAN の装置の要件に一致させる必要があります。

WLAN を選択して、既存の WLAN を編集するか、新規の WLAN を作成することによって、Cisco WLC GUI でこの機能を設定することもできます。

**動的チャンネル割り当ての設定 (GUI)**

RRM によるスキャンに使用するチャンネルの選択時に、Cisco WLC の GUI を使用して動的チャンネル割り当て (DCA) アルゴリズムで考慮されるチャンネルを指定できます。



(注) この機能は、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャンネルがサポートされないことがわかっている場合に役立ちます。

**ステップ 1** 次のように、802.11a/n/ac または 802.11b/g/n ネットワークを無効にします。

- a) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] を選択して、[Global Parameters] ページを開きます。
- b) [802.11a (または 802.11b/g) Network Status] チェックボックスをオフにします。
- c) [Apply] をクリックします。

**ステップ 2** [Wireless] > [802.11a/n/ac または 802.11b/g/n] > [RRM] > [DCA] を選択して、[Dynamic Channel Assignment (DCA)] ページを開きます。

**ステップ 3** [Channel Assignment Method] ドロップダウンリストから次のオプションのいずれかを選択して、Cisco WLC の DCA モードを指定します。

- **[Automatic]** : Cisco WLC によって、join しているすべてのアクセスポイントのチャンネル割り当てが定期的に評価され、必要に応じて更新されます。これは、デフォルト値です。
  - **[Freeze]** : Cisco WLC によって、join しているすべてのアクセスポイントのチャンネル割り当てが評価され、必要に応じて更新されます。(ただし **[Invoke Channel Update Once]** をクリックする場合のみ)。
- (注) **[Invoke Channel Update Once]** をクリックしても、Cisco WLC によるチャンネル割り当ての評価と更新がすぐに行われるわけではありません。次の間隔が経過するまで待機します。
- **[OFF]** : DCA を無効にし、すべてのアクセスポイントの無線を帯域の最初のチャンネル (デフォルトの値) に設定します。このオプションを選択する場合は、すべての無線のチャンネルを手動で割り当てる必要があります。

(注) 最適なパフォーマンスを確保するには、[Automatic] 設定を使用することを、お勧めします。Cisco WLC の動的チャンネルおよび電力の設定を無効にする手順については、[チャンネルおよび電力の動的割り当ての無効化 \(GUI\)](#)、(1048 ページ) の項を参照してください。

**ステップ 4** [Interval] ドロップダウン リストで、[10 minutes]、[1 hour]、[2 hours]、[3 hours]、[4 hours]、[6 hours]、[8 hours]、[12 hours]、または [24 hours] のいずれかのオプションを選択し、DCA アルゴリズムを実行する間隔を指定します。デフォルト値は 10 分です。

(注) Cisco WLC が OfficeExtend アクセス ポイントしかサポートしていない場合は、最適なパフォーマンスを得るために、DCA 間隔を 6 時間に設定することをお勧めします。OfficeExtend アクセス ポイントとローカルアクセス ポイントを組み合わせて展開している場合は、10 分から 24 時間までの範囲を使用できます。

**ステップ 5** [AnchorTime] ドロップダウン リストで、DCA アルゴリズムの開始時刻を指定する数値を選択します。オプションは、0 ~ 23 (両端の値を含む) の数値で、午前 12 時から午後 11 時の時刻を表す、0 ~ 23 (両端の値を含む) の数値です。

**ステップ 6** [Avoid Foreign AP Interference] チェックボックスをオンにすると、Cisco WLC の RRM アルゴリズムで、Lightweight アクセス ポイントにチャンネルを割り当てるときに、外部アクセス ポイント (無線ネットワークに含まれないもの) からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、外部アクセス ポイントに近いチャンネルをアクセス ポイントが回避するようにチャンネル割り当てを調整できます。デフォルト値はオンです。

**ステップ 7** [Avoid Cisco AP Load] チェックボックスをオンにすると、Cisco WLC の RRM アルゴリズムで、チャンネルを割り当てるときに、無線ネットワーク内の Cisco Lightweight アクセス ポイントからの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、トラフィックの負荷が高いアクセス ポイントに適切な再利用パターンを割り当てることができます。デフォルト値はオフです。

**ステップ 8** [Avoid Non-802.11a (802.11b) Noise] チェックボックスをオンにすると、Cisco WLC の RRM アルゴリズムで、Lightweight アクセス ポイントにチャンネルを割り当てるときに、ノイズ (802.11 以外のトラフィック) が考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、電子レンジなど、アクセス ポイント以外を原因とする重大な干渉があるチャンネルをアクセス ポイントに回避させることができます。デフォルト値はオンです。

**ステップ 9** [Avoid Persistent Non-WiFi Interference] チェックボックスをオンにして、Cisco WLC が継続的な WiFi 以外の干渉を無視できるようにします。

**ステップ 10** [DCA Channel Sensitivity] ドロップダウン リストから、次のオプションのいずれかを選択して、チャンネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する DCA アルゴリズムの感度を指定します。

- [Low] : 環境の変化に対する DCA アルゴリズムの感度は特に高くありません。
- [Medium] : 環境の変化に対する DCA アルゴリズムの感度は中程度です。
- [High] : 環境の変化に対する DCA アルゴリズムの感度が高くなります。

デフォルト値は [Medium] です。DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

表 25 : DCA の感度のしきい値

オプション	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

**ステップ 11** 802.11a/n/ac ネットワークの場合のみ、次のいずれかのチャンネル幅オプションを選択し、5 GHz 帯域のすべての 802.11n 無線でサポートするチャンネル帯域幅を指定します。

- [20 MHz] : 20 MHz のチャンネル帯域幅 (デフォルト)
- [40 MHz] : 40 MHz のチャンネル帯域幅
  - (注) [40 MHz] を選択する場合、ステップ 13 の [DCA Channel List] から少なくとも 2 つの隣接チャンネルを選択します (たとえば、プライマリ チャンネルとして 36、拡張チャンネルとして 40)。チャンネルを 1 つだけしか選択しない場合、そのチャンネルは 40 MHz のチャンネル帯域幅では使用されません。
  - (注) [40 MHz] を選択する場合、個々のアクセス ポイントで使用するプライマリ チャンネルおよび拡張チャンネルも構成できます。
  - (注) グローバルに設定した DCA チャンネル幅の設定を無効にする場合は、[802.11a/n Cisco APs > Configure] ページで 20 または 40 MHz モードのアクセス ポイントの無線を静的に設定できます。アクセス ポイント無線で静的 RF チャンネルの割り当て方法を [WLC Controlled] に変更すると、グローバルな DCA 設定によりアクセス ポイントが使用していたチャンネル幅設定は上書きされます。変更が有効になるには最長 30 分 (DCA を実行する間隔に応じて) かかる場合があります。
  - (注) A 無線で 40 MHz を選択した場合、チャンネル 116、140、および 165 を他のチャンネルと組み合わせることはできません。
- [80 MHz] : 802.11ac 無線用の 80 MHz 帯域幅。

このページには、次のような変更できないチャンネル パラメータの設定も表示されます。

- [Channel Assignment Leader] : チャンネルの割り当てを担当する RF グループ リーダーの MAC アドレスです。
- [Last Auto Channel Assignment] : RRM が現在のチャンネル割り当てを最後に評価した時刻です。

**ステップ 12** [Avoid check for non-DFS channel] を選択すると、Cisco WLC が非 DFS チャンネルのチェックを回避できるようになります。DCA 設定には、リスト内の非 DFS チャンネルが少なくとも 1 つ必要です。EU 各国では、屋外の展開は非 DFS チャンネルをサポートしていません。EU や同様の規制のある地域を拠点とするお客様は、AP がチャンネルをサポートしていなくても、このオプションを有効にするか、DCA リスト内の非 DFS チャンネルを少なくとも 1 つ持つ必要があります。

(注) このパラメータは、1522 や 1524 などの屋外アクセス ポイントを持つ展開にのみ適用されません。

**ステップ 13** [DCA Channel List] 領域の [DCA Channels] テキスト ボックスには、現在選択されているチャンネルが表示されます。チャンネルを選択するには、[Select] カラムでそのチャンネルのチェックボックスをオンにします。チャンネルの選択を解除するには、チャンネルのチェックボックスをオフにします。

範囲は次のとおりです。802.11a : 36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、165、190、196 802.11b/g : 1、2、3、4、5、6、7、8、9、10、11

デフォルトの設定は次のとおりです。802.11a : 36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161 802.11b/g : 1、6、11

(注) 802.11a 帯域の拡張 UNII-2 チャンネル (100、104、108、112、116、132、136、および 140) は、チャンネル リストには表示されません。-E 規制ドメインに Cisco Aironet 1520 シリーズ メッシュ アクセス ポイントがある場合、運用を開始する前に、DCA チャンネル リストにこれらのチャンネルを含める必要があります。以前のリリースからアップグレードしている場合は、これらのチャンネルが DCA チャンネル リストに含まれていることを確認します。チャンネル リストにこれらのチャンネルを含めるには、[Extended UNII-2 Channels] チェックボックスをオンにします。

**ステップ 14** ネットワーク内で Cisco Aironet 1520 シリーズ メッシュ アクセス ポイントを使用している場合は、動作させる 802.11a 帯域で 4.9 GHz チャンネルを設定する必要があります。4.9 GHz 帯域は、Public Safety に関わるクライアントアクセス トラフィック専用です。4.9 GHz チャンネルを選択するには、[Select] カラムでチェックボックスをオンにします。チャンネルの選択を解除するには、チャンネルのチェックボックスをオフにします。

範囲は次のとおりです。802.11a : 1、2、3、4、5、6、7、8、9、10、11、12、13、14、15、16、17、18、19、20、21、22、23、24、25、26

デフォルトの設定は次のとおりです。802.11a : 20、26

**ステップ 15** [Apply] をクリックします。

**ステップ 16** 次の手順で、802.11 ネットワークを再度有効にします。

- 1 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] を選択して、[Global Parameters] ページを開きます。
- 2 [802.11a (または 802.11b/g) Network Status] チェックボックスをオンにします。
- 3 [Apply] をクリックします。

**ステップ 17** [Save Configuration] をクリックします。

(注) DCA アルゴリズムによってチャンネルが変更された理由を参照するには、[Monitor] を選択して、次に [Most Recent Traps] で [View All] を選択します。トラップにより、チャンネルが変更された無線の MAC アドレス、前のチャンネルと新規のチャンネル、変更された理由、変更前後のエネルギー、変更前後のノイズ、変更前後の干渉が示されます。

## カバレッジ ホールの検出の設定 (GUI)

- ステップ 1** 次の手順で 802.11 ネットワークを無効にします。
- [Wireless]>[802.11a/n/ac] または [802.11b/g/n]>[Network] の順に選択して、[802.11a (または 802.11b/g) Global Parameters] ページを開きます。
  - [802.11a (または 802.11b/g) Network Status] チェックボックスをオフにします。
  - [Apply] をクリックします。
- ステップ 2** [Wireless]>[802.11a/n/ac] または [802.11b/g/n]>[RRM]>[Coverage] の順に選択して、[802.11a/ac (または 802.11b/g) > RRM > Coverage] ページを開きます。
- ステップ 3** カバレッジホールの検出を有効にする場合は [Enable Coverage Hole Detection] チェックボックスをオンにします。この機能を無効にする場合は、オフにします。カバレッジホールの検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセスポイントがあるかどうかを、アクセスポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。デフォルト値はオンです。
- ステップ 4** [Data RSSI] テキストボックスに、アクセスポイントで受信されたデータパケットの最小の受信信号強度インジケータ (RSSI) 値を入力します。入力する値は、ネットワーク内のカバレッジホール (またはカバレッジが不完全な領域) を特定するのに使用されます。アクセスポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータキューに受信される場合、潜在的なカバレッジホールが検出されています。有効な値の範囲は -90 ~ -60 dBm で、デフォルト値は -80 dBm です。アクセスポイントでは、データ RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。
- ステップ 5** [Voice RSSI] テキストボックスに、アクセスポイントで受信された音声パケットの最小の受信信号強度インジケータ (RSSI) 値を入力します。入力する値は、ネットワーク内のカバレッジホールを特定するのに使用されます。アクセスポイントによって、ここで入力する値より RSSI 値が小さいパケットが音声キューに受信される場合、潜在的なカバレッジホールが検出されています。有効な値の範囲は -90 ~ -60dBm で、デフォルト値は -75dBm です。アクセスポイントでは、音声 RSSI が 5 秒おきに測定され、それらが 90 秒間隔で Cisco WLC にレポートされます。
- ステップ 6** [Min Failed Client Count per AP] テキストボックスに、RSSI 値がデータ RSSI または音声 RSSI のしきい値以下である、アクセスポイント上のクライアントの最小数を入力します。有効な範囲は 1 ~ 75 で、デフォルト値は 3 です。
- ステップ 7** [Coverage Exception Level per AP] テキストボックスに、信号レベルが低くなっているにもかかわらず別のアクセスポイントにローミングできない、アクセスポイント上のクライアントの割合を入力します。有効な値の範囲は 0 ~ 100% で、デフォルト値は 25% です。

- (注) 5秒間で失敗したパケットの数と割合の両方が、[Failed Packet Count] および [Failed Packet Percentage] (Cisco WLC の CLI を使用して設定可能) に設定された値を超える場合、クライアントは事前アラーム状態と判断されます。Cisco WLC では、この情報を使用して、真のカバレッジホールと偽のカバレッジホールが区別されます。false positive は通常、大部分のクライアントに実装されているローミングロジックが不適切であることが原因です。90秒間で失敗したクライアントの数と割合の両方が、[Min Failed Client Count per AP] および [Coverage Exception Level per AP] テキストボックスに入力された値を満たすか超えている場合、カバレッジホールが検出されます。Cisco WLC では、カバレッジホールが修正可能かどうか判断され、適切な場合は、その特定のアクセスポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。

ステップ 8 [Apply] をクリックします。

ステップ 9 次の手順で 802.11 ネットワークを再度有効にします。

- a) [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] の順に選択して、[802.11a (または 802.11b/g) Global Parameters] ページを開きます。
- b) [802.11a (または 802.11b/g/n) Network Status] チェックボックスをオンにします。
- c) [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

## RRM プロファイルしきい値、監視チャンネル、および監視間隔の設定 (GUI)

ステップ 1 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [General] の順に選択して、[802.11a/n/ac (または 802.11b/g/n) > RRM > General] ページを開きます。

ステップ 2 次のように、アラームに使用されるプロファイルしきい値を設定します。

- (注) プロファイルしきい値は、RRM アルゴリズムの機能には関係ありません。これらのしきい値パラメータに設定された値を超えると、Lightweight アクセスポイントから Cisco WLC に SNMP トラップ (またはアラート) が送信されます。

- a) [Interference] テキストボックスに、1つのアクセスポイントにおける干渉 (無線ネットワーク外の発信元からの 802.11 トラフィック) の割合を入力します。有効な値の範囲は 0 ~ 100% で、デフォルト値は 10% です。
- b) [Clients] テキストボックスに、1つのアクセスポイントにおけるクライアントの数を入力します。有効な範囲は 1 ~ 75 で、デフォルト値は 12 です。
- c) [Noise] テキストボックスに、1つのアクセスポイントにおけるノイズ (802.11 以外のトラフィック) のレベルを入力します。有効な値の範囲は -127 ~ 0 dBm で、デフォルト値は -70 dBm です。
- d) [Utilization] テキストボックスに、1つのアクセスポイントで使用されている RF 帯域幅の割合を入力します。有効な値の範囲は 0 ~ 100% で、デフォルト値は 80% です。

ステップ 3 [Channel List] ドロップダウンリストから次のオプションのいずれかを選択して、アクセスポイントで RRM によるスキャンに使用されるチャンネルのセットを指定します。

- [All Channels] : 選択した無線でサポートされているすべてのチャンネルで、RRM によるチャンネル スキャンが実行されます。使用国で有効でないチャンネルも対象となります。
- [Country Channels] : 使用国内の D チャンネルのみで、RRM によるチャンネル スキャンが実行されます。これは、デフォルト値です。
- [DCA Channels] : DCA アルゴリズムによって使用されるチャンネルセットのみで、RRM によるチャンネル スキャンが実行されます。デフォルトでは、使用国で有効な、オーバーラップしないすべてのチャンネルが対象となります。ただし、必要に応じて、DCA で使用するチャンネルセットを指定できます。これを行うには、「動的チャンネル割り当て」の手順に従ってください。

**ステップ 4** 次のように、監視間隔を設定します。

- 1 [Channel Scan Interval] テキスト ボックスに、無線帯域内の各チャンネルでスキャンを実行する間隔の合計 (秒単位) を入力します。スキャンプロセス全体の所要時間はチャンネル、無線ごとに 50 ミリ秒であり、ここで設定された間隔で実行されます。各チャンネルをリッスンするための所要時間は、50 ミリ秒のスキャン時間 (設定不可) とスキャン対象チャンネル数によって決まります。たとえば、米国では、11 個の 802.11b/g チャンネルがすべて、デフォルトの 180 秒の間隔で、50 ミリ秒間ずつスキャンされます。したがって、各スキャンチャンネルで 16 秒ごとに 50 ミリ秒がリッスンに費やされます (180/11 = 約 16 秒)。スキャンが実行される間隔は、[Channel Scan Interval] パラメータによって決まります。有効な値の範囲は 60 ~ 3600 秒で、デフォルト値は 802.11a 無線で 60 秒、802.11b/g/n 無線で 180 秒です。

(注) Cisco WLC で OfficeExtend アクセス ポイントだけをサポートする場合は、最適なパフォーマンスのため、チャンネル スキャンの間隔は 1800 秒に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントの組み合わせを使用した展開では、60 から 3600 秒の範囲を使用できます。

- 2 [Neighbor Packet Frequency] テキスト ボックスに、ネイバー パケット (メッセージ) が送信される間隔を秒単位で入力します。ネイバー パケットによって最終的にネイバー リストが構築されます。有効な値の範囲は 60 ~ 3600 秒で、デフォルト値は 60 秒です。

(注) Cisco WLC で OfficeExtend アクセス ポイントだけをサポートする場合は、最適なパフォーマンスのため、ネイバー パケットの送信間隔は 600 秒に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントの組み合わせを使用した展開では、60 から 3600 秒の範囲を使用できます。

(注) アクセス ポイント無線が 60 分以内に既存のネイバーからネイバー パケットを受信しない場合、Cisco WLC によってネイバー リストからそのネイバーが削除されます。

**ステップ 5** [Apply] をクリックします。

**ステップ 6** [Save Configuration] をクリックします。

- (注) Cisco WLC の RRM 関連パラメータをすべて工場出荷時のデフォルト値に戻す場合は、[Set to Factory Default] をクリックします。



## RRM の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、802.11 ネットワークを無効にします。

```
config {802.11a | 802.11b} disable network
```

**ステップ 2** 次のコマンドを入力して、送信電力制御のバージョンを選択します。

```
config advanced {802.11a | 802.11b} tpc-version {1 | 2}
```

値は次のとおりです。

- TPCv1：最適カバレッジ：（デフォルト）セル間干渉およびスティッキー クライアント シンドロームに強力な信号カバレッジと安定性を提供します。
- TPCv2：干渉に最適：ボイスコールが広く使用されている場合に選択します。干渉を最小にするために、送信電力が動的に調整されます。これは、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジホールのインシデントが多く発生する可能性があります。

**ステップ 3** 送信電力の制御を設定するには、次のいずれかの操作を行います。

- 次のコマンドを入力して、RRM にすべての 802.11 無線の送信電力を定期的な間隔で自動的に設定させます。

```
config {802.11a | 802.11b} txPower global auto
```

- 次のコマンドを入力して、RRM にすべての 802.11a または 802.11b/g 無線の送信電力を自動的に 1 回リセットさせます。

```
config {802.11a | 802.11b} txPower global once
```

- 送信電力制御アルゴリズムを無効にする送信電力の範囲を設定します。次のコマンドを使用して、RRM で使用する最大および最小の送信電力を入力します。

（注） Cisco WLC ソフトウェア リリース 7.6 以降のリリースでは、このコマンドの使用にあたって 802.11 ネットワークを無効にする必要はありません。

```
config {802.11a | 802.11b} txPower global {max | min} txpower
```

*txpower* は、-10 ~ 30 dBm の値です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM ではアクセス ポイントがこの送信電力を上回ることにはできません（最大値は RRM スタートアップまたはカバレッジ ホールの検出で設定されます）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限りは、11 dBm を上回って伝送を行うアクセス ポイントはありません。

- 次のコマンドを入力して、手動でデフォルトの送信電力設定を変更します。

```
config advanced {802.11a | 802.11b} {tpcv1-thresh | tpcv2-thresh} threshold
```

ここで、*threshold* は、-80 ~ -50 dBm の値です。この値を増やすと、アクセス ポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。

多数のアクセス ポイントを設定している場合、ワイヤレス クライアントが認識する BSSID (アクセス ポイント) やビーコンの数を少なくするために、しきい値を  $-80$  dBm または  $-75$  dBm に下げることが有用です。一部のワイヤレス クライアントは多数の BSSID や高速ビーコンを処理できない場合があります。デフォルトのしきい値では、問題のある動作を起こす可能性があります。

- 次のコマンドを入力して、チャンネルごとに送信電力制御バージョン 2 を設定します。

```
config advanced {802.11a | 802.11b} tpcv2-per-chan {enable | disable}
```

**ステップ 4** 動的チャンネル割り当て (DCA) を設定するには、次のいずれかの操作を行います。

- 次のコマンドを入力して、RRM にすべての 802.11 チャンネルをアベイラビリティおよび干渉に基づいて自動的に設定させます。

```
config {802.11a | 802.11b} channel global auto
```

- 次のコマンドを入力して、RRM にすべての 802.11 チャンネルをアベイラビリティおよび干渉に基づいて自動的に 1 回再設定させます。

```
config {802.11a | 802.11b} channel global once
```

- 次のコマンドを入力して、RRM を無効にし、すべてのチャンネルをデフォルト値に設定します。

```
config {802.11a | 802.11b} channel global off
```

- 次のコマンドを入力して、アグレッシブ DCA サイクルを再開します。

```
config {802.11a | 802.11b} channel global restart
```

- DCA に使用するチャンネルセットを指定するには、次のコマンドを入力します。

```
config advanced {802.11a | 802.11b} channel {add | delete} channel_number
```

コマンドごとに 1 つのチャンネル番号のみを入力できます。このコマンドは、クライアントが古いデバイスであるため、またはクライアントに特定の制約事項があるために、クライアントで特定のチャンネルがサポートされないことがわかっている場合に役立ちます。

**ステップ 5** 次のコマンドを入力して、追加の DCA パラメータを設定します。

- **config advanced {802.11a | 802.11b} channel dca anchor-time value** : DCA アルゴリズムの開始時刻を指定します。value は、午前 12 時から午後 11 時の時刻を表す、0 ~ 23 (両端の値を含む) の数値です。
- **config advanced {802.11a | 802.11b} channel dca interval value** : DCA アルゴリズムの実行が許可される頻度を指定します。value には、時間単位で 1、2、3、4、6、8、12、または 24 のいずれかの値を指定するか、デフォルト値の 10 分 (すなわち 600 秒) を示す 0 を指定します。

(注) Cisco WLC が OfficeExtend アクセス ポイントしかサポートしていない場合は、最適なパフォーマンスを得るために、DCA 間隔を 6 時間に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントを組み合わせで展開している場合は、10 分から 24 時間までの範囲を使用できます。

- **config advanced {802.11a | 802.11b} channel dca sensitivity {low | medium | high}** : DCA アルゴリズムでチャンネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する感度を指定します。
  - **low** の場合、環境の変化に対する DCA アルゴリズムの感度は特に高くありません。
  - **medium** の場合、環境の変化に対する DCA アルゴリズムの感度は中程度です。
  - **high** の場合、環境の変化に対する DCA アルゴリズムの感度が高くなります。

DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

表 26 : DCA の感度のしきい値

オプション	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	10 dB	15 dB
Low	20 dB	20 dB

- **config advanced 802.11a channel dca chan-width-11n {20 | 40 | 80}** : 5 GHz 帯域におけるすべての 802.11n 無線の DCA チャンネル幅を設定します。  
値は次のとおりです。
  - **20** は 802.11n 無線のチャンネル幅を 20 MHz に設定します。これは、デフォルト値です。
  - **40** は 802.11n 無線のチャンネル幅を 40 MHz に設定します。
    - (注) **40** を選択する場合は、**config advanced 802.11a channel {add | delete} channel\_number** コマンド (ステップ 4) で少なくとも 2 つの隣接チャンネルを設定する必要があります (たとえば、プライマリ チャンネルとして 36、拡張チャンネルとして 40)。1 つのチャンネルしか設定しないと、そのチャンネルは 40 MHz チャンネル幅として使用されません。
    - (注) **40** を選択する場合、個々のアクセス ポイントで使用するプライマリ チャンネルおよび拡張チャンネルも構成できます。
    - (注) グローバルに設定した DCA チャンネル幅の設定を無効にする場合は、**config 802.11a chan\_width Cisco\_AP {20 | 40 | 80}** コマンドを使用して、20-MHz または 40-MHz、あるいは 80-MHz モードのアクセス ポイントの無線を静的に設定できます。後でこのアクセス ポイントの無線に対する静的な設定をグローバルに変更すると、それまでアクセス ポイントで使用されていたチャンネル幅設定はグローバルな DCA 設定で上書きされます。変更が有効になるには最長 30 分 (DCA を実行する間隔に応じて) かかる場合があります。
  - **80** は 802.11ac 無線のチャンネル幅を 80 MHz に設定します。
- 次のコマンドを入力して、スロットに固有のチャンネル幅を設定します。

**config slot slot-id ap-name {20 | 40 | 80}**

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {enable | disable}** : 非 DFS チャンネルのチェックを回避するために Cisco WLC を有効または無効にします。

(注) このパラメータは、1522 や 1524 などの屋外アクセス ポイントを持つ展開にのみ適用されます。

- **config advanced {802.11a | 802.11b} channel foreign {enable | disable}** : チャンネル割り当てにおける外部アクセス ポイントの干渉の回避を有効または無効にします。
- **config advanced {802.11a | 802.11b} channel load {enable | disable}** : チャンネル割り当てにおける負荷の回避を有効または無効にします。
- **config advanced {802.11a | 802.11b} channel noise {enable | disable}** : チャンネル割り当てにおけるノイズの回避を有効または無効にします。
- **config advanced {802.11a | 802.11b} channel update** : すべての Cisco アクセス ポイントのチャンネル選択の更新を開始します。

**ステップ 6** 次のコマンドを入力して、カバレッジ ホールの検出を設定します。

(注) Cisco WLC ソフトウェア リリース 5.2 以降のリリースでは、カバレッジ ホールの検出は WLAN ごとに無効にできます。

- **config advanced {802.11a | 802.11b} coverage {enable | disable}** : カバレッジ ホールの検出を有効または無効にします。カバレッジ ホールの検出を有効にすると、カバレッジ が不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。デフォルト値はイネーブルです。
- **config advanced {802.11a | 802.11b} coverage {data | voice} rssi-threshold rssi** : アクセス ポイントによって受信されるパケットの受信信号強度インジケータ (RSSI) の最小値を指定します。入力する値は、ネットワーク内のカバレッジ ホール (またはカバレッジ が不完全な領域) を特定するのに使用されます。アクセス ポイントによって、ここで入力する値より RSSI 値が小さいパケットがデータキューまたは音声キューに受信される場合、潜在的なカバレッジ ホールが検出されています。有効な値の範囲は -90 ~ -60 dBm で、データ パケットのデフォルト値は -80 dBm、音声パケットのデフォルト値は -75 dBm です。アクセス ポイントでは、5 秒ごとに RSSI が測定され、90 秒間隔でそれらが Cisco WLC に報告されます。
- **config advanced {802.11a | 802.11b} coverage level global clients** : RSSI 値がデータ RSSI または音声 RSSI のしきい値以下である、アクセス ポイント上のクライアントの最小数を指定します。有効な範囲は 1 ~ 75 で、デフォルト値は 3 です。
- **config advanced {802.11a | 802.11b} coverage exception global percent** : 信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできない、アクセス ポイント上のクライアントの割合を指定します。有効な値の範囲は 0 ~ 100% で、デフォルト値は 25% です。
- **config advanced {802.11a | 802.11b} coverage {data | voice} packet-count packets** : アップリンク データまたは音声パケットの最小失敗回数のしきい値を指定します。有効な値の範囲は 1 ~ 255 パケットで、デフォルト値は 10 パケットです。

- **config advanced {802.11a | 802.11b} coverage {data | voice} fail-rate percent** : アップリンク データまたは音声パケットの失敗率のしきい値を指定します。有効な値の範囲は 1 ~ 100% で、デフォルト値は 20% です。

(注) 5 秒間で失敗したパケットの数と割合の両方が、**packet-count** および **fail-rate** コマンドに入力された値を超える場合、クライアントは事前アラーム状態と判断されます。Cisco WLC では、この情報を使用して、真のカバレッジホールと偽のカバレッジホールが区別されません。false positive は通常、大部分のクライアントに実装されているローミング ロジックが不適切であることが原因です。90 秒間で失敗したクライアントの数と割合の両方が、**coverage level global** および **coverage exception global** コマンドで入力された値を満たすか、これを超えている場合、カバレッジホールが検出されます。Cisco WLC では、カバレッジホールが修正可能かどうか判断され、適切な場合は、その特定のアクセスポイントの送信電力 レベルを上げることによってカバレッジ ホールが解消されます。

**ステップ 7** 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。

**config {802.11a | 802.11b} enable network**

(注) 802.11g ネットワークを有効にするには、**config 802.11b 11gSupport enable** の前に、**config 802.11b enable network** コマンドを入力します。

**ステップ 8** 次のコマンドを入力して、設定を保存します。

**save config**

## RRM 設定の表示 (CLI)

802.11a および 802.11b/g RRM 設定を表示するには、次のコマンドを使用します。

**show advanced {802.11a | 802.11b} ?**

ここで、? は、次のいずれかを示します。

- **ccx {global | Cisco\_AP}** : CCX RRM 設定を表示します。
- **channel** : チャネル割り当ての設定および統計情報を表示します。
- **coverage** : カバレッジ ホールの検出の設定および統計情報を表示します。
- **logging** : RF イベント ログおよびパフォーマンス ログを表示します。
- **monitor** : シスコの無線監視に関する情報を表示します。
- **profile {global | Cisco\_AP}** : アクセスポイントのパフォーマンスプロファイルを表示します。
- **receiver** : 802.11a または 802.11b/g 受信装置の設定および統計情報を表示します。
- **summary** : 802.11a または 802.11b/g アクセスポイントの設定および統計情報を表示します。
- **txpower** : 送信電力割り当ての設定および統計情報を表示します。

## RRM 問題のデバッグ (CLI)

RRM の動作のトラブルシューティングおよび検証には、次のコマンドを使用します。

**debug airewave-director ?**

ここで、? は、次のいずれかを示します。

- **all** : すべての RRM ログのデバッグを有効にします。
- **channel** : RRM チャンネル割り当てプロトコルのデバッグを有効にします。
- **detail** : RRM 詳細ログのデバッグを有効にします。
- **error** : RRM エラー ログのデバッグを有効にします。
- **group** : RRM グループ プロトコルのデバッグを有効にします。
- **manager** : RRM マネージャのデバッグを有効にします。
- **message** : RRM メッセージのデバッグを有効にします。
- **packet** : RRM パケットのデバッグを有効にします。
- **power** : RRM パワー割り当てプロトコルとカバレッジホールの検出のデバッグを有効にします。
- **profile** : RRM プロファイル イベントのデバッグを有効にします。
- **radar** : RRM レーダー検出/回避プロトコルのデバッグを有効にします。
- **rf-change** : RRM RF 変更のデバッグを有効にします。



# 第 137 章

## RF グループの設定

- [RF グループについて, 1033 ページ](#)
- [RF グループの設定, 1036 ページ](#)
- [RF グループ ステータスの表示, 1037 ページ](#)
- [RF グループ内の不正アクセス ポイント検出の設定, 1038 ページ](#)

### RF グループについて

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整する Cisco WLC の論理的な集合です。802.11 ネットワーク タイプごとに RF グループが存在します。単一の RF グループに Cisco WLC をクラスタリングすることによって、RRM アルゴリズムは単一の Cisco WLC の機能を拡張できます。

RF グループは、次のパラメータに基づいて作成されます。

- ユーザ設定の RF ネットワーク名。
- 無線レベルで実行されるネイバー探索。
- MC に設定されている国のリスト。

MCS 間で実行する RF グループ化。

Lightweight アクセス ポイントは、定期的にネイバーメッセージを無線で送信します。同じ RF グループ名を使用しているアクセス ポイントは、相互に送信されたメッセージを検証します。

検証されたネイバーメッセージを、異なるコントローラ上のアクセス ポイントが -80 dBm 以上の信号強度で受信すると、Cisco WLC によって自動モードの RF 領域が動的に形成されます。静的モードで、リーダーは手動で選択され、メンバが RF グループに追加されます。RF グループモードに関する詳細については、「[RF グループ リーダー](#)」の項を参照してください。



(注) RF グループとモビリティグループは、どちらも Cisco WLC のクラスターを定義するという点では同じですが、用途に関しては異なります。RF グループはスケラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティグループはスケラブルでシステム全体にわたるモビリティと Cisco WLC の冗長性を実現します。

## RF グループ リーダー

7.0.116.0 のリリースから、RF グループ リーダーを次の 2 つの方法で設定することができます。

- 自動モード：このモードでは、RF グループのメンバによって、グループの「マスター」電力およびチャンネルスキームを管理する RF グループ リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループ リーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバが大幅に変更された場合）。
- 静的モード：このモードでは、ユーザは RF グループ リーダーとして Cisco WLC を手動で選択します。このモードでは、リーダーおよびメンバは手動で設定され、固定されます。メンバが RF グループに join できない場合は、理由が表示されます。リーダーは、メンバが前の試行で join しなかった場合、1 分ごとにメンバとの接続を確立しようとします。

RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析して、パワーおよびチャンネルの割り当てを算出し、RF グループの各 Cisco WLC に送信します。RRM アルゴリズムによって、システム全体の安定性が保証され、チャンネルおよびパワースキームの変更を適切なローカル RF 領域に制限します。

6.0 より前の Cisco WLC のソフトウェア リリースでは、動的チャンネル割り当て (DCA) の検索アルゴリズムによって、RF グループの Cisco WLC にアソシエートされた無線について適切なチャンネル計画を判別しますが、現在の計画よりも大幅に優れていない限り、新しいチャンネル計画は適用されません。両方の計画で最も不適切な無線のチャンネルメトリックにより、適用する計画が決定されます。新しいチャンネル計画を適用するための唯一の基準として最もパフォーマンスの低い無線を使用すると、ピンニングまたはカスケードの問題が発生する可能性があります。

ピンニングは、アルゴリズムによって RF グループの一部の無線に適したチャンネル計画が検出されても、ネットワーク内の最も条件の悪い無線には適したチャンネルオプションがないため、チャンネル計画の変更は実施されないことを指します。RF グループ内の最も条件の悪い無線によって、グループ内の他の無線がより適切なチャンネル計画を探すことができなくなる場合があります。ネットワークの規模が大きければ大きいほど、よりピンニングになりやすいです。

1 つの無線のチャンネルが変更された場合に、RF 領域の残りの無線を最適化するため、連続してチャンネル変更が行われると、カスケードが発生します。このような無線を最適化すると、ネイバーおよびネイバーのネイバーのチャンネル計画が次善のものになり、チャンネル最適化が起動されます。この影響は、すべてのアクセスポイント無線が同じ RF グループに属している場合、複数のフロアまたは複数の建物に広がる場合があります。この変更は、大きなクライアントの混乱を引き起こし、ネットワークを不安定にします。



ピンニングとカスケードの主な原因は、新しいチャンネル計画を検索する方法と、起こる可能性のあるチャンネル計画の変更が単一の無線の RF 状態によって制御されていることです。Cisco WLC ソフトウェアリリース 6.0 の DCA アルゴリズムは、ピンニングとカスケードを回避するよう再設計されました。次の変更が実装されました。

- 複数のローカル検索：DCA 検索アルゴリズムでは、単一の無線による単一のグローバル検索ではなく、同じ DCA の処理内で異なる無線によって開始される複数のローカル検索が実行されます。この変更によって、ピンニングとカスケードの両方に対応できるだけでなく、安定性を損なうことなく、DCA に必要な柔軟性と適合性が維持されます。
- 複数のチャンネル計画変更イニシエータ（CPCI）：以前は、最も条件の悪い単一の無線が、チャンネル計画変更の唯一のイニシエータでした。しかし、RF グループ内の各無線が評価されて、イニシエータ候補として優先順位付けされるようになりました。生成されたリストはインテリジェントにランダム化されるので、最終的にすべての無線が評価され、ピンニングが発生する可能性はなくなります。
- チャンネル計画変更の適用制限（ローカリゼーション）：各 CPCI 無線の場合、DCA アルゴリズムは適切なチャンネル計画を求めてローカル検索を実行しますが、実際には CPCI 無線自身および 1 ホップ近隣のアクセスポイントのみが現在の送信チャンネルを変更できます。アクセスポイントによるチャンネル計画変更のトリガーの影響は、そのアクセスポイントの 2 RF ホップ内だけで認識され、実際のチャンネル計画変更は 1 ホップ RF 領域内に制限されます。この制限はすべての CPCI 無線にわたって適用されるため、カスケードが発生する可能性はありません。
- 非 RSSI ベースの累積コストメトリック：累積コストメトリックによって、全範囲、領域、またはネットワークが指定のチャンネル計画でどの程度のパフォーマンスを示すのかを測定します。チャンネル計画の品質全体を把握する目的で、その領域内にあるすべてのアクセスポイントに関する個々のコストメトリックが考慮されます。これらのメトリックを使用することで、すべてのチャンネル計画変更により単一の各無線の品質の向上または低下が含まれるようになります。その目的は、単一の無線の品質は向上するが、他の複数の無線のパフォーマンスが大幅に低下するような、チャンネル計画変更を避けることです。

RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。更新間隔の合間に、RF グループリーダーは各 RF グループメンバーにキープアライブメッセージを送信し、リアルタイムの RF データを収集します。



(注) 複数の監視間隔を使用することもできます。詳細については、「RRM の設定」の項を参照してください。

## RF グループ名

Cisco WLC には RF グループ名が設定されます。この RF グループ名は、その Cisco WLC に join しているすべてのアクセスポイントに送信され、アクセスポイントでは、この名前がハッシュ MIC をネイバーメッセージで生成するための共有秘密として使用されます。RF グループを作成するには、グループに含めるすべての Cisco WLC に同じ RF グループ名を設定します。

Cisco WLC に join しているアクセス ポイントが別の Cisco WLC 上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらの Cisco WLC に同じ RF グループ名を設定する必要があります。アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびコンテンションをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

## RF グループの設定

この項では、GUI または CLI によって RF グループを設定する方法について説明します。



(注) 通常、RF グループ名は展開時にスタートアップ ウィザードを使用して設定されます。ただし、必要に応じて変更できます。



(注) 複数の Country Code 機能を使用している場合、同じ RF グループに join する予定のすべての Cisco WLC は、同じ国を同じ順序で設定する必要があります。



(注) Cisco Prime インフラストラクチャを使用して RF グループを設定することもできます。

### RF グループ名の設定 (GUI)

- ステップ 1 [Controller] > [General] の順に選択して、[General] ページを開きます。
- ステップ 2 [RF-Network Name] テキストボックスに RF グループの名前を入力します。名前には、19 文字以内の ASCII 文字を使用できます。
- ステップ 3 [Apply] をクリックして、変更を確定します。
- ステップ 4 [Save Configuration] をクリックして、変更を保存します。
- ステップ 5 RF グループに含める各コントローラについて、この手順を繰り返します。

### RF グループ名の設定 (CLI)

- ステップ 1 `config network rf-network-name name` コマンドを入力して、RF グループを作成します。
  - (注) グループ名として 19 文字以内の ASCII 文字を入力します。

- ステップ 2 **show network** コマンドを入力して、RF グループを確認します。
- ステップ 3 **save config** コマンドを入力して、設定を保存します。
- ステップ 4 RF グループに含める各コントローラについて、この手順を繰り返します。

## RF グループ ステータスの表示

この項では、GUI または CLI を使用して RF グループのステータスを表示する方法について説明します。



- (注) Cisco Prime インフラストラクチャを使用して RF グループのステータスを表示することもできます。

### RF グループ ステータスの表示 (GUI)

- ステップ 1 [Wireless] > [802.11a/n/ac > (または 802.11b/g/n) > RRM] > [RF Grouping] を選択して、[802.11a/n/ac (または 802.11b/g/n) RRM > RF Grouping] ページを開きます。  
このページは RF グループの詳細を示し、設定可能なパラメータ [RF Group mode]、この Cisco WLC の [RF Group role]、[Update Interval]、およびこの Cisco WLC の [Group Leader] の Cisco WLC 名と IP アドレスを表示します。

- (注) RF グループ化モードは、[Group Mode] ドロップダウン リストを使用して設定できます。

ヒント：一度 Cisco WLC がスタティック メンバとして join されてから、グループ化モードを変更する場合は、メンバを設定したスタティック リーダーからそのメンバを削除することをお勧めします。メンバの Cisco WLC が複数のスタティック リーダーでメンバになるように設定されていないことも確認してください。これは、1 つまたは複数の RF スタティック リーダーから join 試行が繰り返されるのを回避します。

- ステップ 2 (任意) 選択しなかったネットワーク タイプ (802.11a/n/ac または 802.11b/g/n) について、この手順を繰り返します。

## RF グループ ステータスの表示 (CLI)

**ステップ 1** 次のコマンドを入力して、802.11a RF ネットワークの RF グループ リーダーである Cisco WLC を表示します。

**show advanced 802.11a group**

以下に類似した情報が表示されます。

```
Radio RF Grouping
 802.11a Group Mode..... STATIC
 802.11a Group Update Interval..... 600 seconds
 802.11a Group Leader..... test (209.165.200.225)
 802.11a Group Member..... test (209.165.200.225)
 802.11a Last Run..... 397 seconds ago
```

この出力は、RF グループの詳細を示しています。具体的には、Cisco WLC のグループ化モード、グループ情報の更新間隔（デフォルトでは 600 秒）、RF グループ リーダーの IP アドレス、この Cisco WLC の IP アドレス、およびグループ情報の最終更新時間です。

(注) グループ リーダーとグループ メンバの IP アドレスが同じ場合、その Cisco WLC は現在、グループ リーダーです。

(注) \* は、Cisco WLC がスタティック メンバーとして join されていないことを示します。

**ステップ 2** 次のコマンドを入力して、802.11b/g RF ネットワークの RF グループ リーダーである Cisco WLC を表示します。

**show advanced 802.11b group**

## RF グループ内の不正アクセス ポイント検出の設定

### RF グループ内の不正アクセス ポイント検出について

Cisco WLC の RF グループを作成したら、不正アクセス ポイントを検出するように、Cisco WLC に接続されたアクセス ポイントを設定する必要があります。アクセス ポイントによって、近隣のアクセス ポイントのメッセージ内のビーコン/プローブ応答フレームが選択され、RF グループの認証情報要素 (IE) と一致するものが含まれているかどうかを確認されます。選択が正常に終了すると、フレームは認証されます。正常に終了しなかった場合は、認証されているアクセス ポイントによって、近隣のアクセス ポイントが不正アクセス ポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルは Cisco WLC に送信されます。

## RF グループ内の不正アクセス ポイント検出の設定

### RF グループ内の不正アクセス ポイント検出の有効化 (GUI)

- 
- ステップ 1** RF グループ内の各 Cisco WLC に同じ RF グループ名が設定されていることを確認します。  
(注) この名前は、すべてのビーコンフレーム内の認証 IE を検証するために使用されます。Cisco WLC に異なる名前が設定されている場合は、障害アラームが生成されます。
- ステップ 2** [Wireless] を選択して、[All APs] ページを開きます。
- ステップ 3** アクセスポイントの名前をクリックして、[All APs > Details] ページを開きます。
- ステップ 4** [AP Mode] ドロップダウンリストから [local] または [monitor] を選択し、[Apply] をクリックして変更を確定します。
- ステップ 5** [Save Configuration] をクリックして、変更を保存します。
- ステップ 6** Cisco WLC に接続されているすべてのアクセスポイントについて、[ステップ 2](#) から [ステップ 5](#) を繰り返します。
- ステップ 7** [Security] > [Wireless Protection Policies] > [AP Authentication/MFP] の順に選択して、[AP Authentication Policy] ページを開きます。  
この Cisco WLC が属する RF グループの名前は、ページの上部に表示されます。
- ステップ 8** [Protection Type] ドロップダウンリストから [AP Authentication] を選択して、不正アクセスポイントの検出を有効にします。
- ステップ 9** [Alarm Trigger Threshold] 編集ボックスに数値を入力して、不正アクセスポイントに関するアラームがいつ生成されるようにするかを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセスポイントフレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。  
(注) しきい値の有効範囲は1～255で、デフォルト値は1です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。
- ステップ 10** [Apply] をクリックして、変更を確定します。
- ステップ 11** [Save Configuration] をクリックして、変更を保存します。
- ステップ 12** RF グループ内のすべての Cisco WLC について、この手順を繰り返します。  
(注) 不正アクセスポイントの検出が有効になっていない Cisco WLC が RF グループ内にある場合、この機能が無効になっている Cisco WLC のアクセスポイントは不正として報告されます。
- 

### RF グループ内の不正アクセス ポイント検出の設定 (CLI)

- 
- ステップ 1** RF グループ内の各 Cisco WLC に同じ RF グループ名が設定されていることを確認します。  
(注) この名前は、すべてのビーコンフレーム内の認証 IE を検証するために使用されます。Cisco WLC に異なる名前が設定されている場合は、障害アラームが生成されます。

- ステップ 2** 次のコマンドを入力して、特定のアクセス ポイントを local（通常）モードまたは monitor（リッスン専用）モードに設定します。  
**config ap mode local** *Cisco\_AP* または **config ap mode monitor** *Cisco\_AP*
- ステップ 3** 次のコマンドを入力して、変更を保存します。  
**save config**
- ステップ 4** Cisco WLC に接続されているすべてのアクセス ポイントについて、ステップ 2 とステップ 3 を繰り返します。
- ステップ 5** 次のコマンドを入力して、不正なアクセス ポイントの検出を有効にします。  
**config wps ap-authentication**
- ステップ 6** 次のコマンドを入力して、不正なアクセス ポイントのアラームが生成される時期を指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。  
**config wps ap-authentication threshold**
- （注） しきい値の有効範囲は 1 ～ 255 で、デフォルトのしきい値は 1 です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。
- ステップ 7** 次のコマンドを入力して、変更を保存します。  
**save config**
- ステップ 8** RF グループ内のすべての Cisco WLC について、ステップ 5 から ステップ 7 を繰り返します。  
（注） 不正アクセス ポイントの検出が有効になっていない Cisco WLC が RF グループ内にある場合、この機能が無効になっている Cisco WLC のアクセス ポイントは不正として報告されます。
-



# 第 138 章

## RRM の無効化

- [RRM の無効化について, 1041 ページ](#)
- [RRM を上書きするための前提条件, 1042 ページ](#)
- [アクセス ポイント無線へのチャンネルおよび送信電力設定の静的割り当て, 1042 ページ](#)
- [Cisco ワイヤレス LAN コントローラに対するチャンネルおよび電力の動的割り当てのグローバルな無効化, 1048 ページ](#)

### RRM の無効化について

展開方法によっては、シスコから提供されている RRM アルゴリズムを使用するよりも、チャンネルや送信電力の設定を静的にアクセスポイントに割り当てる方が適している場合があります。通常、これは厳しい RF 環境や一般的でない展開に該当し、カーペットを敷いた一般的なオフィスには該当しません。



(注) チャンネルおよびパワー レベルを静的にアクセスポイントに割り当てる場合や、チャンネルおよびパワーの動的割り当てを無効にする場合でも、自動 RF グループ化を使用して不要な不正デバイス イベントを回避することが必要です。

チャンネルおよびパワーの動的割り当てを Cisco WLC に対してグローバルに無効にすることも、チャンネルおよびパワーの動的割り当てを有効にしたまま、アクセスポイント無線ごとにチャンネルおよびパワーを静的に設定することもできます。Cisco WLC 上のすべてのアクセスポイント無線に適用されるグローバルなデフォルトの送信電力パラメータをネットワークタイプごとに指定できますが、チャンネルの動的割り当てを無効にした場合は、アクセスポイント無線ごとにチャンネルを設定する必要があります。また、グローバルな送信電力を有効にしておく代わりに、アクセスポイントごとに送信電力を設定することもできます。

## RRM を上書きするための前提条件

相互に隣接するアクセスポイントには、オーバーラップしない別のチャンネルを割り当てることをお勧めします。米国でのオーバーラップしないチャンネルは、802.11a ネットワークでは 36、40、44、48、52、56、60、64、149、153、157、および 161、802.11b/g ネットワークでは 1、6、および 11 です。

## アクセスポイント無線へのチャンネルおよび送信電力設定の静的割り当て

### チャンネルおよび送信電力設定の静的割り当て（GUI）

- ステップ 1** [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac または [802.11b/g/n] の順に選択して、[802.11a/n/ac（または 802.11b/g/n） Radios] ページを開きます。  
このページには、Cisco WLC に join しているすべての 802.11a/n/ac または 802.11b/g/n アクセスポイント無線とその現在の設定が表示されます。[Channel] テキストボックスでは、プライマリチャンネルおよび拡張チャンネルを表示し、それらのチャンネルがグローバルに割り当てられている場合はアスタリスクを使用して示します。
- ステップ 2** 無線設定を変更するアクセスポイントの青いドロップダウンの矢印の上にカーソルを置いて、[Configure] を選択します。[802.11a/n/ac（または 802.11b/g/n） Cisco APs > Configure] ページが表示されます。
- ステップ 3** 次のオプションから、[RF Channel Assignment] を指定します。
- [Global] : グローバル値を指定するには、このオプションを選択します。
  - [Custom] : カスタム値を指定するには、このオプションを選択して隣接するドロップダウンリストから値を選択します。
- ステップ 4** 次のように、この無線のアンテナパラメータを設定します。
- 1 アクセスポイント無線で使用するアンテナのタイプを指定するには、[Antenna Type] ドロップダウンリストから、[Internal] または [External] を選択します。
  - 2 [Antenna] テキストボックスのチェックボックスをオンおよびオフにして、このアクセスポイントに関して特定のアンテナの使用を有効にしたり、無効にしたりします。ここで、[A]、[B]、および [C] は特定のアンテナポートです。D のアンテナは、Cisco 3600 シリーズアクセスポイント用に表示されます。A は右のアンテナポート、B は左のアンテナポート、C は中央のアンテナポートです。たとえば、アンテナポート A と B からの送信およびアンテナポート C からの受信を有効にするには、[Tx] では [A] と [B]、[Rx] では [C] チェックボックスをオンにします。3600 AP で、有効な組み合わせは A、A+B、A+B+C または A+B+C+D です。1 本のデュアルモードアンテナを選択する場合は、1 つの空間 802.11n ストリームレート（MCS 0～7 データレート）のみを適用できます。2 本のデュアル



モードアンテナを選択する場合は、2つの空間 802.11n ストリーム レート (MCS 0 ~ 15 データ レート) のみを適用できます。

- 3 [Antenna Gain] テキスト ボックスに、外部アンテナの性能を指定する数値を入力し、特定の空間領域に無線エネルギーを向けたり収束させたりします。高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナ ゲインは 0.5 dBi 単位で測定され、デフォルト値は 0.5 dBi の 7 倍、つまり 3.5 dBi です。

高ゲインアンテナがある場合、実際の dBi 値を 2 倍にした値を入力します (アンテナの dBi 値については、『Cisco Aironet Antenna Reference Guide』を参照してください)。それ以外の場合は、0 と入力します。たとえば、アンテナのゲインが 4.4 dBi の場合は、4.4 dBi に 2 をかけた 8.8 で切り捨てを行い、整数部分 (8) のみを入力します。アンテナが各国の規制に違反しないように、Cisco WLC によって、実際の等価等方放射電力 (EIRP) が低減されます。

- 4 [Diversity] ドロップダウン リストから、次のオプションのいずれかを選択します。

[Enabled] : アクセスポイントの両側でアンテナ コネクタを有効にします。これは、デフォルト値です。

[Side A or Right] : アクセスポイントの右側にあるアンテナ コネクタを有効にします。

[Side B or Left] : アクセスポイントの左側にあるアンテナ コネクタを有効にします。

**ステップ 5** RF チャンネルをアクセスポイント無線に割り当てるには、[RF Channel Assignment] セクションで、[RF Channel Assignment] の [Assignment Method] で [Custom] を選択し、ドロップダウン リストからチャンネルを選択します。

**ステップ 6** 送信電力レベルをアクセスポイント無線に割り当てるには、[Tx Power Level Assignment] セクションで、[Custom] 割り当て方式を選択し、ドロップダウン リストから送信電力レベルを選択します。送信電力レベルには、mW 単位または dBm 単位の値の代わりに整数値が割り当てられます。この整数は、アクセスポイントが展開されている規制ドメインによって異なるパワー レベルに対応します。使用可能なパワー レベルの数は、アクセスポイントモデルによって異なります。ただし、パワー レベル 1 は常に各 Country Code の設定で有効な最大パワー レベルで、それ以降の各パワー レベルは前のパワー レベルの 50% を表します。たとえば、1 = 特定の規制ドメインの最大パワー レベル、2 = 50% のパワー、3 = 25% のパワー、4 = 12.5% のパワーとなります。

(注) 各規制ドメインでサポートされている最大送信電力レベルについては、お使いの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。また、サポートされている電力レベルの数については、お使いのアクセスポイントのデータシートを参照してください。

(注) アクセスポイントが全出力で動作していない場合、「Due to low PoE, radio is transmitting at degraded power」というメッセージが [Tx Power Level Assignment] セクションに表示されます。

**ステップ 7** [Admin Status] ドロップダウン リストから [Enable] を選択して、アクセスポイントに対するこの設定を有効にします。

**ステップ 8** [Apply] をクリックします。

**ステップ 9** 次の手順で、アクセスポイント無線の管理状態を Cisco WLC から Cisco Prime Infrastructure へ即座に送信するように設定します。

- 1 [Wireless] > [802.11a/n/ac または [802.11b/g/n] > [Network] を選択して、[802.11a (または 802.11b/g) Global Parameters] ページを開きます。
- 2 [802.11a (または 802.11b/g) Network Status] チェックボックスをオンにします。
- 3 [Apply] をクリックします。

ステップ10 [Save Configuration] をクリックします。

ステップ11 静的なチャンネルおよびパワー レベルを割り当てる各アクセス ポイント無線について、この手順を繰り返します。

## チャンネルおよび送信電力設定の静的割り当て (CLI)

ステップ1 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワーク上の特定のアクセス ポイント無線を無効にします。

```
config {802.11a | 802.11b} disable Cisco_AP
```

ステップ2 次のコマンドを入力して、特定のアクセス ポイントのチャンネル幅を設定します。

```
config {802.11a | 802.11b} chan_width Cisco_AP {20 | 40 | 80}
```

値は次のとおりです。

- **20** : 20 MHz チャンネルだけを使用して無線は通信できます。20 MHz チャンネルだけを使用して通信するレガシー 802.11a 無線、20 MHz 802.11n 無線、または 40 MHz 802.11n 無線の場合にこのオプションを選択します。これは、デフォルト値です。
- **40** : 結合された隣接する 2 つの 20 MHz チャンネルを使用して 40 MHz 802.11n 無線は通信できます。スループット向上のため、無線では、選択するプライマリ チャンネルおよびその拡張チャンネルを使用します。各チャンネルには、1 つの拡張チャンネルがあります (36 と 40 のペア、44 と 48 のペアなど)。たとえば、プライマリ チャンネルとして 44 を選択すると、Cisco WLC では拡張チャンネルとしてチャンネル 48 が使用されます。プライマリ チャンネルとして 48 を選択すると、Cisco WLC では拡張チャンネルとしてチャンネル 44 が使用されます。
  - (注) このパラメータは、プライマリ チャンネルが静的に割り当てられている場合にだけ設定できます。
  - (注) 20 または 40 MHz、あるいは 80-MHz モードのアクセス ポイント無線を静的に設定すると、グローバルに設定された DCA チャンネル幅の設定 (**config advanced 802.11a channel dca chan-width-11n {20 | 40 | 80}** コマンドを使用して設定) が無効になります。このアクセス ポイントの無線に対する静的な設定をグローバルに戻すように変更すると、それまでアクセス ポイントで使用されていたチャンネル幅がグローバルな DCA 設定で上書きされます。変更が有効になるには最長 30 分 (DCA を実行する間隔に応じて) かかる場合があります。
- **80** は 802.11ac 無線のチャンネル幅を 80 MHz に設定します。

(注) 米国およびカナダでは、チャンネル 116、120、124、および 128 は、40 MHz チャンネルボンディングに使用できません。

**ステップ 3** 次のコマンドを入力して、特定のアクセス ポイントでの個別のアンテナの使用を有効または無効にします。

**config {802.11a | 802.11b} 11nsupport antenna {tx | rx} Cisco\_AP {A | B | C} {enable | disable}**

ここで、A、B、および C はアンテナポートです。A は右のアンテナポート、B は左のアンテナポート、C は中央のアンテナポートです。たとえば、802.11a ネットワーク上のアクセス ポイント AP1 のアンテナポート C にあるアンテナからの送信を有効にするには、次のコマンドを入力します。

**config 802.11a 11nsupport antenna tx AP1 C enable**

(注) 802.11ac モジュールは内部アンテナであるため、802.11ac の個別のアンテナを有効または無効にできません。

**ステップ 4** 次のコマンドを入力して、特定の空間領域に無線エネルギーを向けたり収束させたりする外部アンテナの性能の目安になる、外部アンテナ ゲインを指定します。

**config {802.11a | 802.11b} antenna extAntGain antenna\_gain Cisco\_AP**

高ゲインアンテナの放射パターンは、特定の方向により収束したものになります。アンテナゲインは 0.5 dBi 単位で測定され、デフォルト値は 0.5 dBi の 7 倍、つまり 3.5 dBi です。

高ゲインアンテナがある場合、実際の dBi 値を 2 倍にした値を入力します（アンテナの dBi 値については、『Cisco Aironet Antenna Reference Guide』を参照してください）。それ以外の場合は、0 と入力します。たとえば、アンテナのゲインが 4.4 dBi の場合は、4.4 dBi に 2 をかけた 8.8 で切り捨てを行い、整数部分 (8) のみを入力します。アンテナが各国の規制に違反しないように、Cisco WLC によって、実際の等価等方放射電力 (EIRP) が低減されます。

**ステップ 5** 次のコマンドを入力して、すべての AP または特定の AP に対して、5 GHz の無線のビーム形成を設定します。

**config 802.11a {global | ap ap-name} {enable | disable}**

**ステップ 6** 次のコマンドを入力して、特定のアクセス ポイントで使用するチャンネルを指定します。

**config {802.11a | 802.11b} channel ap Cisco\_AP channel**

たとえば、802.11a チャンネル 36 を AP1 のデフォルト チャンネルとして設定するには、次のコマンドを入力します。 **config 802.11a channel ap AP1 36**

ユーザが選択するチャンネルはプライマリ チャンネル（たとえば、チャンネル 36）です。このチャンネルは、レガシー 802.11a 無線および 802.11n 20 MHz 無線による通信で使用されます。802.11n 40 MHz 無線は、チャンネル幅として 40 を選択した場合、このチャンネルをプライマリ チャンネルとして使用しますが、高速スループット用に追加で結合する拡張チャンネルも使用します。

(注) 動作チャンネルを変更すると、アクセス ポイント無線はリセットされます。

**ステップ 7** 次のコマンドを入力して、特定のアクセス ポイントで使用する送信電力レベルを指定します。

**config {802.11a | 802.11b} txPower ap Cisco\_AP power\_level**

たとえば、802.11a AP1 の伝送パワーをパワー レベル 2 に設定するには、次のコマンドを入力します。

**config 802.11a txPower ap AP1 2**

送信電力レベルには、mW単位またはdBm単位の値の代わりに整数値が割り当てられます。この整数は、アクセスポイントが展開されている規制ドメインによって異なるパワーレベルに対応します。使用可能なパワーレベルの数は、アクセスポイントモデルによって異なります。ただし、パワーレベル1は常に各Country Codeの設定で有効な最大パワーレベルで、それ以降の各パワーレベルは前のパワーレベルの50%を表します。たとえば、1=特定の規制ドメインの最大パワーレベル、2=50%のパワー、3=25%のパワー、4=12.5%のパワーとなります。

特定の場合において、シスコのアクセスポイントは一定のチャンネルに対して7つの電力レベルのみをサポートするので、Cisco ワイヤレス コントローラは電力レベル7と電力レベル8を同一とみなします。電力レベル8がそのチャンネルで設定されている場合、コントローラが電力レベル7を利用可能な最小電力レベルとみなすので設定は成功しません。これらの電力値は、シスコの各アクセスポイントによって異なる法規制の遵守の制限と最小ハードウェア制限に基づいて導き出されます。たとえば、Cisco 3700、3600、2600、1600 シリーズなどのすべての次世代アクセスポイントはコントローラに「合計電力値」をレポートする一方、Cisco 3500、1140、および1250シリーズのアクセスポイントは、コントローラに「パス電力ごと」にレポートするので、最低電力レベルの設定が可能であり、これにより新世代製品の許容電力レベルを削減します。たとえば3600E アクセスポイントの最低電力レベルの電力値が4dbm（総電力）の場合、実際の電力値は-2dbm（パス単位）となります。

(注) 各規制ドメインでサポートされている最大送信電力レベルについては、お使いの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。また、サポートされている電力レベルの数については、お使いのアクセスポイントのデータシートを参照してください。

**ステップ 8** 次のコマンドを入力して、設定を保存します。

**save config**

**ステップ 9** 静的なチャンネルおよびパワーレベルを割り当てる各アクセスポイント無線について、ステップ2からステップ7を繰り返します。

**ステップ 10** 次のコマンドを入力して、アクセスポイント無線を再度有効にします。

**config {802.11a | 802.11b} enable Cisco\_AP**

**ステップ 11** 次のコマンドを入力して、アクセスポイント無線の管理状態をCisco WLCからWCSへ即座に送信するように設定します。

**config {802.11a | 802.11b} enable network**

**ステップ 12** 次のコマンドを入力して、変更を保存します。

**save config**

**ステップ 13** 次のコマンドを入力して、特定のアクセスポイントの設定を表示します。

**show ap config {802.11a | 802.11b} Cisco\_AP**

以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 7
Cisco AP Name..... AP1
...
Tx Power
Num Of Supported Power Levels 8
 Tx Power Level 1 20 dBm
 Tx Power Level 2 17 dBm
 Tx Power Level 3 14 dBm
```

```
Tx Power Level 4 11 dBm
Tx Power Level 5 8 dBm
Tx Power Level 6 5 dBm
Tx Power Level 7 2 dBm
Tx Power Level 8 -1 dBm
Tx Power Configuration CUSTOMIZED
Current Tx Power Level 1
```

Phy OFDM parameters

```
Configuration CUSTOMIZED
Current Channel 36
Extension Channel 40
Channel Width..... 40 Mhz
Allowed Channel List..... 36,44,52,60,100,108,116,132,
..... 149,157
TI Threshold -50
Antenna Type..... EXTERNAL_ANTENNA
External Antenna Gain (in .5 dBi units).... 7
Diversity..... DIVERSITY_ENABLED
```

802.11n Antennas

```
Tx
A..... ENABLED
B..... ENABLED
Rx
A..... DISABLED
B..... DISABLED
C..... ENABLED
```

## Cisco ワイヤレス LAN コントローラに対するチャンネルおよび電力の動的割り当てのグローバルな無効化

### チャンネルおよび電力の動的割り当ての無効化（GUI）

- 
- ステップ 1 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [RRM] > [Auto RF] の順に選択して、[802.11a/n/ac]（または 802.11b/g/n）Global Parameters > Auto RF] ページを開きます。
- ステップ 2 [RF Channel Assignment] で [OFF] を選択して、動的チャンネル割り当てを無効にします。
- ステップ 3 [Tx Power Level Assignment] で [Fixed] を選択して、電力の動的割り当てを無効にし、ドロップダウンリストからデフォルトの送信電力レベルを選択します。
- ステップ 4 [Apply] をクリックします。
- ステップ 5 [Save Configuration] をクリックします。
- ステップ 6 無線ごとにチャンネルおよびパワーのデフォルト設定を無効にする場合は、Cisco WLC に join している各アクセスポイント無線にチャンネルおよびパワーの静的設定を割り当てます。
- ステップ 7 （任意）選択しなかったネットワークタイプ（802.11a/n/ac または 802.11b/g/n）について、この手順を繰り返します。
- 

### チャンネルおよび電力の動的割り当ての無効化（CLI）

- 
- ステップ 1 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを無効にします。  
**config {802.11a | 802.11b} disable network**
- ステップ 2 次のコマンドを入力して、すべての 802.11a または 802.11b/g 無線の RRM を無効にして、すべてのチャンネルをデフォルト値に設定します。  
**config {802.11a | 802.11b} channel global off**
- ステップ 3 次のコマンドを入力して、802.11a または 802.11b/g ネットワークを有効にします。  
**config {802.11a | 802.11b} enable network**  
  
（注） 802.11g ネットワークを有効にするには、**config 802.11b enable network** コマンドの後に、**config 802.11b 11gSupport enable** コマンドを入力します。
- ステップ 4 次のコマンドを入力して、変更を保存します。  
**save config**
-



## CCX 無線管理機能の設定

- [CCX 無線管理機能について, 1049 ページ](#)
- [CCX 無線管理の設定, 1050 ページ](#)

### CCX 無線管理機能について

クライアント ロケーションの計算に影響を与える次の 2 つのパラメータを設定できます。

- 無線測定要求
- ロケーション調整

これらのパラメータは、Cisco Client Extensions (CCX) v2 以降のリリースでサポートされており、参加する CCX クライアントのロケーションの正確性と適時性を強化するよう設計されています。

ロケーション機能が適切に動作するように、アクセス ポイントを `normal`、`monitor`、または `FlexConnect` モードに設定する必要があります。ただし、`FlexConnect` モードの場合、アクセス ポイントを Cisco WLC に接続する必要があります。

### 無線測定要求

無線測定要求機能を有効にすると、`Lightweight` アクセス ポイントは、CCXv2 以降のリリースを実行しているクライアントに、ブロードキャスト無線測定要求メッセージを発行します。`Lightweight` アクセス ポイントは、すべての SSID に対し、それぞれ有効になった無線インターフェイスを使用して、一定の設定間隔でこれらのメッセージを送信します。802.11 無線測定の実行プロセスでは、測定要求に指定されているすべてのチャンネル上の CCX クライアントが 802.11 ブロードキャストプローブ要求を送信します。`Cisco Location Appliance` は、アクセス ポイントで受信されたこれらの要求に基づいてアップリンク測定を使用し、すばやく正確にクライアントロケーションを計算します。測定するクライアントのチャンネルを指定する必要はありません。`Cisco WLC`、アクセス ポイント、およびクライアントによって、使用するチャンネルが自動的に特定されます。

無線測定機能により、(アクセス ポイントの観点だけでなく) クライアントの観点での無線環境に関する情報も `Cisco WLC` で取得できます。この場合、アクセス ポイントは、ユニキャスト無

線測定要求を特定の CCXv4 または v5 クライアントに対して発行します。クライアントは、さまざまな測定レポートをアクセスポイントおよび Cisco WLC に返します。これらのレポートには、無線環境に関する情報と、クライアントのロケーションを解釈するために使用されるデータが含まれています。アクセスポイントおよび Cisco WLC が無線測定要求およびレポートで過負荷状態になるのを防ぐため、各アクセスポイントのクライアント数は2つのみとし、各 Cisco WLC でサポートされるクライアント数は最大で 20 までとします。特定のアクセスポイントまたはクライアントの無線測定要求の状態および特定のクライアントに対する無線測定レポートは、Cisco WLC の CLI で確認できます。

Cisco WLC ソフトウェアでは、Mobility Services Engine の機能が向上しており、ロケーションベースのサービスと呼ばれる CCXv4 機能によりデバイスのロケーションを正確に解釈できます。Cisco WLC は、特定の CCXv4 または v5 クライアントにパス損失要求を発行します。クライアントが応答する場合、クライアントは Cisco WLC にパス損失測定レポートを送信します。これらのレポートには、クライアントのチャンネルおよび送信電力が含まれます。



(注) CCX 以外のクライアントおよび CCXv1 クライアントでは、CCX 測定要求を無視し、無線測定アクティビティには参加しません。

## ロケーション調整

たとえば、クライアント調整が実行される場合など、より厳密な追跡が必要な CCX クライアントの場合、アクセスポイントからこれらのクライアントに対して、一定の設定間隔で、また CCX クライアントが新しいアクセスポイントにローミングした場合は常に、ユニキャスト測定要求を送信させるように Cisco WLC を設定できます。このような特定の CCX クライアントに対するユニキャスト要求は、すべてのクライアントに送信されるブロードキャスト測定要求より頻繁に送信できます。ロケーション調整を CCX 以外のクライアントおよび CCXv1 クライアントに設定すると、それらのクライアントは設定された間隔で強制的にアソシエート解除され、ロケーション測定が生成されます。

# CCX 無線管理の設定

## CCX 無線管理の設定 (GUI)

- ステップ 1 [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] の順に選択して、[802.11a/n/ac (または 802.11b/g/n) Global Parameters] ページを開きます。
- ステップ 2 [CCX Location Measurement] の下にある [Mode] チェックボックスをオンにして、CCX 無線管理をグローバルに有効にします。このパラメータによって、この Cisco WLC に接続されているアクセスポイントから、



CCX2 以降のリリースを実行しているクライアントに対してブロードキャスト無線測定要求が発行されません。デフォルト値では無効（またはオフ）になっています。

- ステップ 3** 前の手順で [Mode] チェックボックスをオンにした場合、[Interval] テキスト ボックスに値を入力して、アクセス ポイントによるブロードキャスト無線測定要求の発行間隔を指定します。指定できる範囲は 60 ～ 32400 秒です。  
デフォルトは 60 秒です。
- ステップ 4** [Apply] をクリックします。
- ステップ 5** [Save Configuration] をクリックします。
- ステップ 6** 次の「[CCX 無線管理の設定 \(CLI\)](#)」の項のステップ 2 の手順に従い、アクセス ポイントのカスタマイズを有効にします。  
(注) 特定のアクセス ポイントの CCX 無線管理を有効にするには、アクセス ポイントのカスタマイズを有効にする必要があります。これは、Cisco WLC の CLI を使用してのみ実行できます。
- ステップ 7** 必要に応じて、もう一方の無線帯域 (802.11a/n/ac または 802.11b/g/n) について、この手順を繰り返します。

## CCX 無線管理の設定 (CLI)

- ステップ 1** 次のコマンドを入力して、CCX 無線管理をグローバルに有効にします。  
**config advanced {802.11a | 802.11b} ccx location-meas global enable interval\_seconds**  
*interval\_seconds* パラメータの範囲は、60 ～ 32400 秒で、デフォルト値は 60 秒です。このコマンドによって、802.11a または 802.11b/g ネットワークでこの Cisco WLC に接続されているすべてのアクセス ポイントから、CCXv2 以降のリリースを実行しているクライアントにブロードキャスト無線測定要求が発行されます。
- ステップ 2** 次のコマンドを入力して、アクセス ポイントのカスタマイズを有効にします。
- **config advanced {802.11a | 802.11b} ccx customize Cisco\_AP {on | off}**  
このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントの CCX 無線管理機能が有効または無効になります。
  - **config advanced {802.11a | 802.11b} ccx location-meas ap Cisco\_AP enable interval\_seconds**  
*interval\_seconds* パラメータの範囲は、60 ～ 32400 秒で、デフォルト値は 60 秒です。このコマンドによって、802.11a または 802.11b/g ネットワーク上の特定のアクセス ポイントから、CCXv2 以降を実行しているクライアントにブロードキャスト無線測定要求が発行されます。
- ステップ 3** 次のコマンドを入力して、特定のクライアントのロケーション調整を有効または無効にします。  
**config client location-calibration {enable | disable} client\_mac interval\_seconds**  
(注) 1 つの Cisco WLC につき最大 5 つのクライアントに対して、ロケーション調整を設定できません。

- ステップ 4 次のコマンドを入力して、設定を保存します。  
**save config**

## CCX 無線管理情報の表示 (CLI)

- 802.11a または 802.11b/g ネットワークでこの Cisco WLC に接続されているすべてのアクセスポイントの CCX ブロードキャスト ロケーション測定要求の設定を表示するには、次のコマンドを入力します。

**show advanced {802.11a | 802.11b} ccx global**

- 802.11a または 802.11b/g ネットワーク上の特定のアクセスポイントの CCX ブロードキャスト ロケーション測定要求の設定を表示するには、次のコマンドを入力します。

**show advanced {802.11a | 802.11b} ccx ap Cisco\_AP**

- 特定のアクセスポイントの無線測定要求の状態を表示するには、次のコマンドを入力します。

**show ap ccx rm Cisco\_AP status**

以下に類似した情報が表示されます。

A Radio

```
Beacon Request..... Enabled
Channel Load Request..... Enabled
Frame Request..... Disabled
Noise Histogram Request..... Disabled
Path Loss Request..... Disabled
Interval..... 60
Iteration..... 5
```

B Radio

```
Beacon Request..... Disabled
Channel Load Request..... Enabled
Frame Request..... Disabled
Noise Histogram Request..... Enabled
Path Loss Request..... Disabled
Interval..... 60
Iteration..... 5
```

- 特定のクライアントの無線測定要求の状態を表示するには、次のコマンドを入力します。

**show client ccx rm client\_mac status**

以下に類似した情報が表示されます。

```
Client Mac Address..... 00:40:96:ae:53:b4
Beacon Request..... Enabled
Channel Load Request..... Disabled
Frame Request..... Disabled
Noise Histogram Request..... Disabled
Path Loss Request..... Disabled
Interval..... 5
Iteration..... 3
```

- 特定のクライアントの無線測定レポートを表示するには、次のコマンドを入力します。  
**show client ccx rm *client\_mac* report beacon** : 特定のクライアントのビーコン レポートを表示します。  
**show client ccx rm *client\_mac* report chan-load** : 特定のクライアントのチャンネル負荷レポートを表示します。  
**show client ccx rm *client\_mac* report noise-hist** : 特定のクライアントのノイズヒストグラムレポートを表示します。  
**show client ccx rm *client\_mac* report frame** : 特定のクライアントのフレーム レポートを表示します。
- ロケーション調整が設定されているクライアントを表示するには、次のコマンドを入力します。  
**show client location-calibration summary**
- クライアントを検出した各アクセスポイントの両方のアンテナについてレポートされる RSSI を表示するには、次のコマンドを入力します。  
**show client detail *client\_mac***

## CCX 無線管理問題のデバッグ (CLI)

- 次のコマンドを入力して、CCX ブロードキャスト測定要求アクティビティをデバッグします。  
**debug airewave-director message {enable | disable}**
- 次のコマンドを入力して、クライアントのロケーション調整アクティビティをデバッグします。  
**debug ccxrm [all | error | warning | message | packet | detail {enable | disable}]**
- CCX 無線測定レポートパケットは、Inter-Access Point Protocol (IAPP) パケットでカプセル化されます。したがって、前の **debug ccxrm** コマンドでデバッグできない場合は、次のコマンドを入力すると IAPP レベルでデバッグできます。  
**debug iapp error {enable | disable}**
- 次のコマンドを入力して、転送されたプローブとそれらに含まれている両アンテナの RSSI の出力をデバッグします。  
**debug dot11 load-balancing**





# 第 140 章

## 設定の最適化されたローミング

- [ローミングの最適化に関する情報](#), 1055 ページ
- [ローミングの最適化の制約事項](#), 1056 ページ
- [ローミングの最適化の設定 \(GUI\)](#) , 1056 ページ
- [ローミングの最適化の設定 \(CLI\)](#) , 1057 ページ

### ローミングの最適化に関する情報

ローミングの最適化は、遠隔地のアクセスポイントに長時間アソシエートし続けているクライアントや、接続が不安定な Wi-Fi ネットワークに接続を試みるアウトバウンドクライアントの問題を解決します。この機能は、クライアントデータパケットの RSSI とデータレートに基づいてクライアントをアソシエート解除します。クライアントは、RSSI アラーム条件が満たされ、現在のデータレートが最適化ローミングデータレートのしきい値を下回っている場合にアソシエート解除されます。データレートオプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

ローミングの最適化は、クライアントの RSSI が低いときにもクライアントアソシエーションを阻止します。この機能は、RSSI しきい値に照らして受信クライアントの RSSI をチェックします。このチェックで、クライアントに有効な接続がない限り、クライアントの Wi-Fi ネットワークへの接続が阻止されます。クライアントはビーコンを受信して Wi-Fi ネットワークに接続できても、信号が弱いために安定した接続をサポートできない場合がよくあります。

ローミングの最適化を使用することによって、無線に対してクライアントカバレッジレポート間隔を設定することもできます。クライアントカバレッジの統計情報には、データパケット RSSI、カバレッジホールの検出および軽減 (CHDM) の事前アラーム障害、再送信要求と現在のデータレートが含まれます。

最適化されたローミングは次のシナリオで実行されます。

- 予防的にクライアントを切断して長時間接続しているクライアントの問題に対処します。
- データ RSSI パケットをアクティブに監視します。

- RSSI が、設定されたしきい値よりも低いクライアントの関連付けを解除します。

## ローミングの最適化の制約事項

- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。

## ローミングの最適化の設定 (GUI)

- 
- ステップ 1** [Wireless] > [Advanced] > [Optimized Roaming] を選択します。[Optimized Roaming] ページが表示されます。
- ステップ 2** 802.11 帯域のローミングの最適化を有効にするには、[Enable] チェックボックスをオンにします。802.11 帯域のローミングの最適化を有効にした後で、ローミングの最適化の間隔、およびデータ レートのしきい値を設定できます。
- ステップ 3** [Optimized Roaming Interval] テキスト ボックスで、アクセス ポイントがコントローラに対してクライアント カバレッジの統計情報をレポートする間隔を入力します。クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減 (CHDM) の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。範囲は 5 ~ 90 秒です。デフォルト値は 90 秒です。
- (注) ローミングの最適化のレポート間隔を設定する前に、802.11a/b ネットワークを無効にする必要があります。レポートの間隔に対して低い値を設定すると、カバレッジ レポートのメッセージでネットワークが過負荷になることがあります。
- ステップ 4** [Optimized Roaming Data Rate Threshold] テキスト ボックスに、クライアントのしきい値データ レートの値を入力します。次のデータ レートが使用可能です。
- 802.11a : 6、9、12、18、24、36、48、および 54。
  - 802.11b : 1、2、5.5、11、6、9、12、18、24、36、48、および 54。

ローミングの最適化は、クライアントのデータ パケットおよびデータ レートの RSSI に基づいてクライアントのアソシエートを解除します。クライアントの現在のデータ レートが、[Optimized Roaming Data Rate Threshold] よりも小さい値の場合は、クライアントはアソシエート解除されます。

---

### 次の作業

ローミングの最適化は、アソシエーションのときにクライアント RSSI をチェックします。この RSSI 値は、設定されている CHDM RSSI に対して 6 db ヒステリシスで検証されます。カバレッジ ホールの検出に対して設定された RSSI しきい値を検証するには、[Wireless] > [802.11a/n/ac] (または [802.11b/g/n]) > [RRM] > [Coverage] を選択して、802.11a/ac (または 802.11b/g/n) をオープンし、[RRM] > [Coverage page] を選択します。

## ローミングの最適化の設定 (CLI)

**ステップ 1** 次のコマンドを入力して、ローミングの最適化を有効または無効にします。

```
config advanced {802.11a| 802.11b} optimized-roaming {enable| disable}
```

デフォルトでは、ローミングの最適化は無効になっています。

**ステップ 2** 次のコマンドを入力して、802.11a/b ネットワークのクライアント カバレッジのレポート間隔を設定します。

```
config advanced {802.11a| 802.11b} optimized-roaming intervalseconds
```

範囲は 5 ~ 90 秒です。デフォルト値は 90 秒です。

(注) ローミングの最適化のレポート間隔を設定する前に、802.11a/b ネットワークを無効にする必要があります。

**ステップ 3** 次のコマンドを入力して、802.11a/b ネットワークのしきい値データ レートを設定します。

```
config advanced {802.11a| 802.11b} optimized-roaming datarateMbps
```

802.11a の場合、設定可能なデータ レートは 6、9、12、18、24、36、48、および 54 です。802.11b の場合、設定可能なデータ レートは、1、2、5.5、11、6、9、12、18、24、36、48、および 54 です。データ レートを無効にするには 0 を設定します。

**ステップ 4** このコマンドを入力して、各帯域のローミングの最適化の情報を表示します。

```
show advanced {802.11a| 802.11b} optimized-roaming
```

```
(Cisco Controller) > show advanced 802.11a optimized-roaming
OptimizedRoaming
 802.11a OptimizedRoaming Mode..... Enabled
 802.11a OptimizedRoaming Reporting Interval.... 20 seconds
 802.11a OptimizedRoaming Rate Threshold..... disabled
```

**ステップ 5** 次のコマンドを入力して、最適なローミング統計に関する情報を表示します。

```
show advanced {802.11a| 802.11b} optimized-roaming stats
```

```
(Cisco Controller) > show advanced 802.11a optimized-roaming stats
OptimizedRoaming Stats
 802.11a OptimizedRoaming Disassociations..... 0
 802.11a OptimizedRoaming Rejections..... 0
```







# 第 141 章

## パケットの検出しきい値設定のレシーバ起動

- [レシーバのパケット検出開始しきい値について, 1059 ページ](#)
- [Rx SOP の制約事項, 1060 ページ](#)
- [Rx SOP の設定 \(GUI\) , 1060 ページ](#)
- [RxSOP の設定 \(CLI\) , 1061 ページ](#)

### レシーバのパケット検出開始しきい値について

レシーバのパケット検出開始しきい値 (RxSOP) は、アクセスポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。Wi-Fi レベルが上がると、無線の受信感度が下がり、レシーバのセルサイズが小さくなります。セルサイズの減少は、ネットワークのクライアントの分散に影響します。

RF リンクが脆弱なクライアント、つながりっぱなしのクライアント、およびアクセスポイント全体で負荷分散しているクライアントに対処するために Rx SOP が使用されます。Rx SOP は、アクセスポイントが最も近くにある最も強力なクライアントを最適化する必要のあるスタジアムやホールなどの高密度展開でネットワーク性能を最大限引き出すのに役立ちます。



(注) RXSOP 設定は 3600 AP でプラグ着脱可能なサードパーティの無線モジュールには適用しません。

#### 関連トピック

- [Rx SOP の設定 \(GUI\) , \(1060 ページ\)](#)
- [RxSOP の設定 \(CLI\) , \(1061 ページ\)](#)
- [Rx SOP の制約事項, \(1060 ページ\)](#)

## Rx SOP の制約事項

- Rx SOP の設定は、Cisco 1600、2600、2700、3500、3600、3700、および 1550 シリーズのアクセス ポイントでのみサポートされます。
- 5 GHz 帯域の Rx SOP しきい値に対する許容範囲は、-76 dBm~-80 dBm で、2.4 GHz の帯域の場合は -79 dBm~-85 dBm です。

### 関連トピック

- [レシーバの packets 検出開始しきい値について](#), (1059 ページ)
- [Rx SOP の設定 \(GUI\)](#), (1060 ページ)
- [RxSOP の設定 \(CLI\)](#), (1061 ページ)

## Rx SOP の設定 (GUI)

**ステップ 1** [Wireless] > [Advanced] > [Rx SOP Threshold] を選択して、802.11 帯域ごとに高、中、低の Rx SOP しきい値を設定します。次の表に、各 802.11 帯域の高、中、低レベルの Rx SOP しきい値を示します。

表 27: Rx SOP しきい値

802.11 帯域	高しきい値	中しきい値	低しきい値
5 GHz	-76 dBm	-78 dBm	-80 dBm
2.4 GHz	-79 dBm	-82 dBm	-85 dBm

**ステップ 2** [Wireless] > [RF Profiles] を選択して、RF プロファイルの Rx SOP しきい値を設定します。RF プロファイル ページが表示されます。

- RF プロファイルをクリックして [RF Profile > Edit] ページを開きます。
- [High Density] タブの [Rx SOP Threshold] ドロップダウンリストから、Rx SOP しきい値を選択します。

### 次の作業

**show{802.11a| 802.11b} extended** コマンドを使用して、802.11 帯域の Rx SOP しきい値に関する情報を確認します。

### 関連トピック

- [レシーバの packets 検出開始しきい値について](#), (1059 ページ)
- [Rx SOP の制約事項](#), (1060 ページ)

## RxSOP の設定 (CLI)

- 
- ステップ 1** 802.11 帯域ごとに高、中、低の Rx SOP しきい値を設定するには、次のコマンドを入力します。  
**config**{802.11a|802.11b} **rx-sop threshold**{high|medium|low|auto} {*apap\_name*|default}
- 802.11 帯域のすべてのアクセスポイントまたは1つのアクセスポイントに対して Rx SOP しきい値を設定できます。
- ステップ 2** 次のコマンドを入力して、RF プロファイルの高、中、低の Rx SOP しきい値を設定します。  
**config rf-profile rx-sop threshold**{high|medium|low|auto} *profile\_name*
- ステップ 3** 次のコマンドを入力して、802.11 帯域の Rx SOP しきい値に関する情報を表示します。  
**show**{802.11a|802.11b} **extended**
- ```
(Cisco Controller) > show 802.11a extended
Default 802.11a band Radio Extended Configurations:
  Beacon period: 100, range: 0 (AUTO);
  Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
  RX SOP threshold: -76; CCA threshold: 0 (AUTO);

AP3600-XALE3 34:a8:4e:6a:7b:00
  Beacon period: 100, range: 0 (AUTO);
  Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
  RX SOP threshold: -76; CCA threshold: 0 (AUTO);

AP54B4 3c:ce:73:6c:42:f0
  Beacon period: 100, range: 0 (AUTO);
  Multicast buffer: 0 (AUTO), rate: 0 (AUTO);
  RX SOP threshold: -76; CCA threshold: -80;
```
-

関連トピック

[レシーバのパケット検出開始しきい値について, \(1059 ページ\)](#)

[Rx SOP の制約事項, \(1060 ページ\)](#)



第 **VIII** 部

Cisco CleanAir の設定

- [CleanAir について, 1065 ページ](#)
- [CleanAir の前提条件と制約事項, 1069 ページ](#)
- [Cisco CleanAir の設定, 1073 ページ](#)
- [干渉デバイスのモニタリング, 1083 ページ](#)
- [Spectrum Expert の接続の設定, 1091 ページ](#)



第 142 章

CleanAir について

この章では、CleanAir について説明します。

- [CleanAir について, 1065 ページ](#)

CleanAir について

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題に予防的に対応するスペクトラム インテリジェンスソリューションです。この機能を使用すると、共有スペクトラムの全ユーザを確認できます（ネイティブデバイスと外部干渉源の両方）。また、ネットワークにおいて、これらの情報に基づいて対処できるようになります。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルを変更して干渉を受けないようにすることができます。CleanAir は、スペクトラム管理と RF 可視性を提供します。

Cisco CleanAir システムは CleanAir 対応アクセス ポイント、Cisco ワイヤレス LAN コントローラ および Cisco Prime Infrastructure で構成されます。アクセス ポイントでは工業、科学、医療用（ISM）帯域で動作しているすべてのデバイスの情報を収集し、これらの情報を潜在的な干渉源として特定および評価し、Cisco WLC に転送します。Cisco WLC は、アクセス ポイントを制御してスペクトラムのデータを収集し、これらの情報を要求に応じて Cisco Prime Infrastructure または Cisco Mobility Services Engine（MSE）に転送します。

Cisco CleanAir では、ライセンス不要の帯域で動作している各デバイスについて、その種類、場所、ワイヤレス ネットワークに与える影響の程度、取るべき対策を提示します。これによって RF がシンプルになり、管理者が RF のエキスパートである必要がなくなります。

ワイヤレス LAN システムは、ライセンスが不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。この帯域では電子レンジ、コードレス電話、Bluetooth デバイスなどの多数の機器が動作しているため、Wi-Fi の動作に悪影響が生じる可能性があります。

Voice over Wireless や IEEE 802.11n 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他の機器からの干渉によって、重大な影響を受ける可能性があります。この無線周波数（RF）の干渉に関する問題は、Cisco Unified Wireless Network に Cisco CleanAir 機能を組み込むことによって解決できます。

CleanAir は、5 GHz の無線メッシュでメッシュ AP のバックホールでサポートされます。CleanAir をバックホール無線で有効にして、レポートインターフェイスの詳細と電波品質を提供できます。

Cisco CleanAir システムの Cisco ワイヤレス LAN コントローラの役割

Cisco WLC は、Cisco CleanAir システムにおいて次の処理を実行します。

- アクセスポイントにおける Cisco CleanAir 機能を設定する。
- Cisco CleanAir の機能の設定やデータ収集のためのインターフェイスを提供する（GUI、CLI、SNMP）。
- スペクトラム データを表示する。
- アクセスポイントから電波品質レポートを収集して処理し、電波品質データベースに保存する。電波品質レポート（AQR）には、特定されたすべての発生源からの干渉全体に関する情報（電波品質の指標（AQI）で表す）や、最も重大な干渉カテゴリの概要が記載されます。また CleanAir システムでは、干渉の種類ごとのレポートに未分類の干渉情報を含めることができ、未分類の干渉デバイスによる干渉が頻繁に生じる場合に対処することができます。
- アクセスポイントから干渉デバイスレポート（IDR）を収集して処理し、干渉デバイスデータベースに保存する。
- スペクトラム データを Prime インフラストラクチャおよび MSE に転送する。

Cisco CleanAir で検出できる干渉の種類

Cisco CleanAir では、干渉を検出し、その干渉の発生箇所や重大度をレポートし、さまざまな緩和方法を推奨することができます。これらの緩和方法には、Persistent Device Avoidance（PDA）と Event Driven RRM（EDRRM）という 2 つの方法があります。

Wi-Fi チップをベースとする RF 管理システムには、次のような共通の特性があります。

- Wi-Fi 信号として識別できない RF エネルギーはノイズとして報告される。
- チャネル計画の割り当てに使用するノイズの測定値は、一部のクライアントデバイスに悪影響を及ぼす可能性のある不安定さや急速な変化を避けるために、一定の期間において平均化される傾向がある。
- 測定値が平均化されることで、測定値の精度が低下する。そのため、平均化された後、クライアントに混乱をもたらす信号が緩和を必要とするものに見えない場合がある。
- 現在使用できる RF 管理システムは、本質的にはすべて事後対応型である。

Cisco CleanAir はこれらと異なり、ノイズの発生源だけでなく、その場所や WLAN に対する潜在的な影響まで明確に特定することができます。このような情報を入手することにより、ネットワーク内におけるノイズを考慮し、理にかなった、可能であれば予防的な判断を行うことができます。CleanAir では、次の 2 種類の干渉イベントが一般的です。

- 永続的干渉
- 突発的干渉

永続的干渉イベントは、本質的に固定型のデバイスから発生し、断続的ではあるものの、干渉が大規模に反復して繰り返されるものを指します。たとえば、休憩室に設置してある電子レンジの場合を考えます。このような装置が動作するのは、1回につき1～2分程度です。しかし一旦動作すると、ワイヤレスネットワークと、関係するクライアントのパフォーマンスに非常に大きな影響が生じます。Cisco CleanAirを使用すると、電子レンジなどの装置を無秩序なノイズとしてではなく明確に識別できるようになります。また、その装置によって影響を受ける帯域の部分の正確に特定できます。そして、その設置場所も特定できるため、最も大きな影響を受けるアクセスポイントを判別することができます。そして、この情報を使用してRRMに指示し、範囲内にあるアクセスポイントに対してこの干渉源を避けるようなチャンネル計画を選択させることができます。この干渉は1日の大部分にわたって発生するものではないため、既存のRF管理アプリケーションによって、影響を受けるアクセスポイントのチャンネルの再変更が試みられている場合もあります。しかし、永続的デバイスの回避は、干渉源が周期的に検出されて永続的な状態が新たに発生する限り影響があり続けるという点で独特です。Cisco CleanAirシステムでは、電子レンジが存在することを認識し、それを将来のすべての計画に取り込みます。電子レンジまたはその近くのアクセスポイントを移動させた場合は、このアルゴリズムによってRRMが自動的に更新されます。



(注) Event Driven RRM (EDRRM) は、Cisco CleanAir 対応でローカルモードにあるアクセスポイントによってのみ動作します。

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャンネル、またはある範囲内のチャンネルが完全に妨害を受けます。Cisco CleanAir の Event Driven RRM (EDRRM) 機能を使用すると、電波品質 (AQ) に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセスポイントに対してチャンネル変更がただちに行われます。ほとんどのRF管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir ではAQ測定値を使用してスペクトラムを連続的に評価するため、対応策を30秒以内に実行します。たとえば、アクセスポイントがビデオカメラからの干渉を受けた場合は、そのカメラが動作し始めてから30秒以内にチャンネル変更によってアクセスポイントを回復させることができます。Cisco CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Bluetooth デバイスの場合、Cisco CleanAir 対応のアクセスポイントで干渉の検出と報告を行うことができるのは、そのデバイスがアクティブに送信しているときだけです。Bluetooth デバイスには、さまざまなパワーセーブモードがあります。たとえば、接続されたデバイス間でデータまたは音声 streams がストリーミングされている最中に干渉が検出されます。

永続的デバイス

屋外型ブリッジや電子レンジなどの一部の干渉デバイスは、必要な場合にのみ送信を行います。通常のRF管理基準では短時間の定期的な動作はたいしては検出されないままになるため、このようなデバイスによってローカルのWLANに対する大規模な干渉が引き起こされる可能性があります。

ます。CleanAirを使用すると、RRMDCAアルゴリズムによって、この影響が検出、測定、登録、記録され、DCAアルゴリズムが調整されます。このため、その干渉源と同じ場所にあるチャンネル計画によって、その永続的デバイスによって影響を受けるチャンネルの使用が最小限に留められます。Cisco CleanAirでは、永続的デバイスの情報を検出してCisco WLCに保存し、チャンネルの干渉の緩和に利用します。

永続的デバイスの検出

CleanAir対応の監視モードのアクセスポイントでは、設定されているすべてのチャンネルで永続的デバイスに関する情報を収集して、この情報をCisco WLCに保存します。ローカル/ブリッジモードのAPは、稼働チャンネルでのみ干渉デバイスを検出します。

永続的デバイスの伝搬

ローカルモードまたは監視モードのアクセスポイントによって検出された永続的デバイス情報は、同じCisco WLCに接続されている隣接アクセスポイントに伝播されます。この機能により、永続的デバイスの制御や回避がより適切に行えるようになります。CleanAir対応アクセスポイントによって検出された永続的デバイスは、CleanAir非対応の隣接アクセスポイントにも伝搬されるため、チャンネル選択の品質が向上します。

アクセスポイントによる干渉源の検出

CleanAir対応のアクセスポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意のIDを割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラムセンサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。ダウンしたデバイスは、スペクトラムデータベースから適正に削除されます。ある特定のデバイスに対する干渉源検出がすべてレポートされる場合は、クラスタIDを長期間にわたって有効とし、デバイス検出が増大しないようにします。同じデバイスが再度検出された場合は、元のクラスタIDとマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAirでは、このようなデバイスを管理するために、クラスタIDをより長く保持し、検出時には同じ1つのレコードに再度マージされるようにします。この処理によってユーザレコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。



第 143 章

CleanAir の前提条件と制約事項

この章では、Cisco CleanAir を設定する際の前提条件および制約事項について説明します。

- [CleanAir の前提条件, 1069 ページ](#)
- [CleanAir の制約事項, 1070 ページ](#)

CleanAir の前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

次のアクセス ポイント モードを使用して、Cisco CleanAir スペクトラム モニタリングを実行できるのは、Cisco CleanAir 対応のアクセス ポイントだけです。

- **Local** : このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャンネルだけに関する電波品質と干渉検出のレポートが作成されます。
- **FlexConnect** : FlexConnect アクセス ポイントがコントローラに接続しているとき、その Cisco CleanAir 機能はローカル モードと同じになります。
- **Monitor** : Cisco CleanAir が監視モードで有効になっていると、そのアクセス ポイントによって、モニタされているすべてのチャンネルに関する電波品質と干渉検出のレポートが作成されます。

次のオプションを使用できます。

- **All** : すべてのチャンネル
- **DCA** : DCA リストによって管理されるチャンネル選択
- **Country** : 規制区域内で合法的なすべてのチャンネル



(注) AP が 2 台あり、一方が FlexConnect モード、もう一方が監視モードであると仮定します。また、802.1x 認証に対する EAP 攻撃を有効にしたプロファイルを作成済みと仮定します。Airmagnet (AM) ツールは、さまざまな種類の攻撃を発生させることのできるツールですが、有効な AP MAC アドレスおよび STA MAC アドレスを指定していても、攻撃の発生に失敗します。しかし、AM ツールで AP MAC アドレスと STA MAC アドレスを交換すると（つまり、AP MAC アドレスを STA MAC フィールドに指定し、STA MAC アドレスを AP MAC フィールドに指定すると）、攻撃を発生させることができ、監視モードの AP でこれを検出できるようになります。



(注) アクセス ポイントは Prime インフラストラクチャでは AQ ヒートマップに参加しません。

- SE-Connect : このモードを使用すると、外部の Microsoft Windows XP または Vista PC で実行されている Spectrum Expert アプリケーションを Cisco CleanAir 対応のアクセス ポイントに接続して、詳細なスペクトラムデータを表示および分析できるようになります。Spectrum Expert アプリケーションは、コントローラをバイパスしてアクセス ポイントに直接接続します。SE-Connect モードのアクセス ポイントからは、Wi-Fi、RF、スペクトラム データがコントローラに提供されません。すべての CleanAir システム機能は、AP がこのモードになっていて、クライアントが実行されていない間、一時停止状態になります。このモードは、リモートトラブルシューティングのみを対象としています。Spectrum Expert のアクティブな接続は最大で 3 つまで可能です。

CleanAir の制約事項

- 監視モードのアクセス ポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは Radio Resource Management (RRM) 計画から除外され、隣接アクセス ポイントのリストに含まれません。IDR クラスタリングは、コントローラがネットワーク内の隣接アクセス ポイントを検出する機能に依存しています。複数のアクセス ポイントから関係する干渉デバイスを検出する機能を使用できるのは、監視モードのアクセス ポイント間に限られます。
- Spectrum Expert (SE) の接続機能は、ローカル、FlexConnect、ブリッジ、および監視の各モードでサポートされています。アクセス ポイントは、Spectrum Expert に現在のチャンネルに関するスペクトラム情報だけを提供します。ローカル、FlexConnect、およびブリッジの各モードでは、スペクトラム データは現在アクティブなチャンネル（複数可）に対して有効です。また監視モードでは、共通の監視対象チャンネルリストを使用できます。アクセス ポイントは AQ（電波品質）レポートと IDR（干渉デバイスレポート）をコントローラに送り続け、現在のモードに応じて通常の処理を実行します。スニファおよび不正検出のアクセス

ポイントモードは、CleanAir のスペクトラムモニタリングのすべてのタイプと互換性はありません。

- ローカルモードアクセス ポイント 5 つに対して監視モードアクセス ポイント 1 つという比率をお勧めします。これは、最適なカバレッジのためにネットワーク設計および専門ガイドンスによって異なる場合があります。
- SE Connect モードでは、Cisco 2500 シリーズの Cisco WLC の物理ポートにアクセス ポイントを直接接続しないでください。
- Spectrum Expert (Windows XP ラップトップクライアント) と AP 間では ping が可能である必要があります。不可能な場合は正しく動作しません。



第 144 章

Cisco CleanAir の設定

- [コントローラでの Cisco CleanAir の設定, 1073 ページ](#)
- [アクセスポイントに対する Cisco CleanAir の設定, 1080 ページ](#)

コントローラでの Cisco CleanAir の設定

Cisco ワイヤレス LAN コントローラでの Cisco CleanAir の設定 (GUI)

- ステップ 1** [Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [CleanAir] の順に選択して、[802.11a (または 802.11b) > CleanAir] ページを開きます。
- ステップ 2** [CleanAir] チェックボックスをオンにして、802.11a/n または 802.11b/g/n ネットワークで Cisco CleanAir の機能を有効にします。Cisco WLC がスペクトラム干渉を検出しないようにするには、これをオフにします。デフォルトでは、この値は選択されていません。
- ステップ 3** [Report Interferers] チェックボックスをオンにして、Cisco CleanAir システムで検出した干渉源をレポートできるようにします。Cisco WLC が干渉源をレポートしないようにするには、これをオフにします。デフォルト値はオンです。
- (注) [Report Interferers] が無効の場合は、デバイスセキュリティアラーム、イベント駆動型 RRM、および Persistent Device Avoidance (PDA) アルゴリズムは機能しません。
- ステップ 4** CleanAir で検出できる持続性デバイスに関する情報を伝播できるようにするには、[Persistent Device Propagation] チェックボックスを選択します。永続的デバイスの伝搬を有効にすると、同じ Cisco WLC に接続されている隣接アクセスポイントに永続的デバイスの情報を伝搬させることができます。永続型の干渉源は、検出されない場合でも、常に存在し、WLAN の動作に干渉します。
- ステップ 5** Cisco CleanAir システムによって検出およびレポートされる必要のある干渉源が [Interferences to Detect] ボックスに表示され、検出される必要のない干渉源は [Interferences to Ignore] ボックスに表示されるようにします。[>] および [<] ボタンを使用して、これらの 2 つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が検出されます。選択できる干渉源の候補には、次のものがあります。
- [Bluetooth Paging Inquiry] : Bluetooth の検出 (802.11b/g/n のみ)

- [Bluetooth Sco Acl] : Bluetooth リンク (802.11b/g/n のみ)
- [Generic DECT] : Digital Enhanced Cordless Communication (DECT) デジタル コードレス電話
- [Generic TDD] : 時分割複信 (TDD) トランスミッタ
- [Generic Waveform] : 連続トランスミッタ
- [Jammer] : 電波妨害デバイス
- [Microwave] : 電子レンジ (802.11b/g/n のみ)
- [Canopy] : Canopy ブリッジ デバイス
- [Spectrum 802.11 FH] : 802.11 周波数ホッピング デバイス (802.11b/g/n のみ)
- [Spectrum 802.11 inverted] : スペクトラム反転 Wi-Fi 信号を使用するデバイス
- [Spectrum 802.11 non std channel] : 非標準の Wi-Fi チャンネルを使用するデバイス
- [Spectrum 802.11 SuperG] : 802.11 SuperAG デバイス
- [Spectrum 802.15.4] : 802.15.4 デバイス (802.11b/g/n のみ)
- [Video Camera] : アナログ ビデオ カメラ
- [WiMAX Fixed] : WiMAX 固定デバイス (802.11a/n/ac のみ)
- [WiMAX Mobile] : WiMAX モバイルデバイス (802.11a/n/ac のみ)
- [XBox] : Microsoft Xbox (802.11b/g/n のみ)

(注) Cisco WLC にアソシエートされているアクセス ポイントは、[Interferences to Detect] ボックスに表示されている干渉源に関する干渉レポートだけを送信します。この機能によって、対象としない干渉源のほか、ネットワークにフラッディングを発生させたり、Cisco WLC や Prime Infrastructure にパフォーマンスの問題を引き起こす可能性のある干渉源をフィルタで除去することができます。フィルタリングによって、システムが通常のパフォーマンスレベルに戻ることができます。

ステップ 6 Cisco CleanAir のアラームを次のように設定します。

- a) [Enable AQI (Air Quality Index) Trap] チェックボックスを選択して、電波品質アラームのトリガーを有効にします。この機能が無効にするには、このボックスを選択解除します。デフォルト値はオンです。
- b) ステップ a で [Enable AQI Trap] チェックボックスを選択した場合は、電波品質アラームをトリガーするしきい値を指定するために、1 ~ 100 (両端の値を含む) の値を [AQI Alarm Threshold] テキストボックスに入力します。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 35 です。
- c) [AQI Alarm Threshold (1 to 100)] に任意の値を設定します。電波品質がしきい値に達した場合にアラームが生成されます。デフォルトは 35 です。有効な範囲は 1 ~ 100 です。
- d) [Enable trap for Unclassified Interferences] チェックボックスを選択して、[AQI Alarm Threshold] で指定した重大度しきい値を超える未分類の干渉が検出されたときに AQI アラームが発生するようにします。未分類の干渉とは、検出されたものの、識別可能な干渉のタイプに該当しないものです。

- e) [Threshold for Unclassified category trap (1 to 99)] に値を入力します。1～99 の範囲で値を入力します。デフォルト値は20です。これは未分類の干渉のカテゴリに対する重大度の指標となるしきい値です。
- f) [Enable Interference Type Trap] チェックボックスをオンにして、指定したデバイス タイプが Cisco WLC によって検出されたときに干渉源アラームをトリガーするようにします。この機能を無効にするには、このボックスをオフにします。デフォルト値はオンです。
- g) 干渉アラームをトリガーする必要がある干渉源が [Trap on These Types] ボックスに表示され、干渉アラームをトリガーする必要のない干渉源は [Do Not Trap on These Types] ボックスに表示されるようにします。[>]および[<] ボタンを使用して、これらの2つのボックス間で干渉源を移動します。デフォルトでは、すべての干渉源が干渉アラームを生成します。
たとえば、Cisco WLC が電波妨害デバイスを検出したときにアラームを送信するようにするには、[Enable Interference Type Trap] チェックボックスをオンにして、電波妨害デバイスを [Trap on These Types] ボックスに移動させます。

ステップ 7 [Apply] をクリックします。

ステップ 8 Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、イベント駆動型無線リソース管理 (RRM) の実行をトリガーするよう設定します。

- a) [EDRRM] フィールドを見て、Event Driven RRM (EDRRM) の現在の状態を確認します。これが有効である場合は、[Sensitivity Threshold] フィールドを見て、イベント駆動型 RRM が起動されるしきい値レベルを確認します。
- b) イベント駆動型 RRM の現在の状態や感度のレベルを変更する場合は、[Change Settings] をクリックします。[802.11a (または 802.11b) > RRM > Dynamic Channel Assignment (DCA)] ページが表示されます。
- c) [EDRRM] チェックボックスを選択して、アクセスポイントがあるレベルの干渉を検出した場合に RRM の実行がトリガーされるようにします。この機能を無効にするには選択解除します。デフォルト値はオンです。
- d) ステップ c で [EDRRM] チェックボックスを選択した場合は、[Sensitivity Threshold] ドロップダウン リストから [Low]、[Medium]、[High]、または [Custom] を選択して、RRM をトリガーするしきい値を指定します。アクセスポイントの干渉がしきい値レベルを上回ると、RRM はローカルの動的チャネル割り当て (DCA) の実行を開始し、ネットワークのパフォーマンスを改善するために可能な場合は影響を受けるアクセスポイント無線のチャンネルを変更します。[Low] は、環境の変更に対する感度を下げることが表すのに対して、[High] は、感度を上げることが表します
EDRRM の感度のしきい値に [Custom] を選択した場合は、[Custom Sensitivity Threshold] フィールドにしきい値を設定する必要があります。デフォルトの感度は35です。
EDRRM AQ のしきい値は、感度が [Low] の場合は35、[Medium] の場合は50、[High] の場合は60です。
- e) [Apply] をクリックします。

ステップ 9 [Save Configuration] をクリックします。

Cisco ワイヤレス LAN コントローラでの Cisco CleanAir の設定 (CLI)

ステップ 1 次のコマンドを入力して、802.11 ネットワークで Cisco CleanAir 機能を設定します。

```
config {802.11a | 802.11b} cleanair {enable | disable} all
```

この機能を無効にすると、Cisco WLC はスペクトル データをまったく受信しなくなります。デフォルト値はイネーブルです。

ステップ 2 ネットワーク上のすべての関連するアクセス ポイントの CleanAir を有効にします。

```
config {802.11a cleanair enable network
```

メッシュ アクセス ポイントの 5 GHz 無線で、CleanAir を有効にできます。

ステップ 3 次のコマンドを入力して、干渉検出を設定し、Cisco CleanAir システムで検出する必要がある干渉源を指定します。

```
config {802.11a | 802.11b} cleanair device {enable | disable} type
```

ここで、*type* には次のいずれかを選択します。

- **802.11-fh** : 802.11 周波数ホッピング デバイス (802.11b/g/n のみ)
- **802.11-inv** : スペクトラム反転 Wi-Fi 信号を使用するデバイス
- **802.11-nonstd** : 非標準の Wi-Fi チャンネルを使用するデバイス
- **802.15.4** : 802.15.4 デバイス (802.11b/g/n のみ)
- **all** : すべての干渉デバイス タイプ (これがデフォルト値です)
- **bt-discovery** : Bluetooth の検出 (802.11b/g/n のみ)
- **bt-link** : Bluetooth リンク (802.11b/g/n のみ)
- **canopy** : Canopy デバイス
- **cont-tx** : 連続トランスミッタ
- **dect-like** : Digital Enhanced Cordless Communication (DECT) デジタル コードレス電話
- **jammer** : 電波妨害デバイス
- **mw-oven** : 電子レンジ (802.11b/g/n のみ)
- **superag** : 802.11 SuperAG デバイス
- **tdd-tx** : 時分割複信 (TDD) トランスミッタ
- **video camera** : アナログ ビデオ カメラ
- **wimax-fixed** : WiMAX 固定デバイス
- **wimax-mobile** : WiMAX モバイル デバイス
- **xbox** : Microsoft Xbox (802.11b/g/n のみ)

(注) Cisco WLC にアソシエートされているアクセス ポイントは、このコマンドで指定された干渉の種類についてのみ干渉レポートを送信します。この機能によって、ネットワークにフラグディングを発生させたり、Cisco WLC や Prim Infrastructure にパフォーマンスの問題を引き起こす可能性のある干渉源をフィルタで除去することができます。フィルタリングによって、システムが通常のパフォーマンス レベルに戻ることができます。

ステップ 4 次のコマンドを入力して、電波品質アラームのトリガーを設定します。

```
config {802.11a | 802.11b} cleanair alarm air-quality {enable | disable}
```

デフォルト値はイネーブルです。

ステップ 5 次のコマンドを入力して、電波品質アラームをトリガーするしきい値を指定します。

```
config {802.11a | 802.11b} cleanair alarm air-quality {enable | disable}config {802.11a | 802.11b} cleanair alarm air-quality threshold threshold
```

threshold の値は、1 ~ 100 (両端の値を含む) です。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 35 です。

ステップ 6 次のコマンドを入力して、干渉源アラームのトリガーを有効にします。

```
config {802.11a | 802.11b} cleanair alarm device {enable | disable}
```

デフォルト値はイネーブルです。

ステップ 7 次のコマンドを入力して、アラームをトリガーする干渉源を指定します。

```
config {802.11a | 802.11b} cleanair alarm device type {enable | disable}ここで、type には次のいずれかを選択します。
```

- **802.11-fh** : 802.11 周波数ホッピング デバイス (802.11b/g/n のみ)
- **802.11-inv** : スペクトラム反転 Wi-Fi 信号を使用するデバイス
- **802.11-nonstd** : 非標準の Wi-Fi チャンネルを使用するデバイス
- **802.15.4** : 802.15.4 デバイス (802.11b/g/n のみ)
- **all** : すべての干渉デバイス タイプ (これがデフォルト値です)
- **bt-discovery** : Bluetooth の検出 (802.11b/g/n のみ)
- **bt-link** : Bluetooth リンク (802.11b/g/n のみ)
- **canopy** : Canopy デバイス
- **cont-tx** : 連続トランスミッタ
- **dect-like** : Digital Enhanced Cordless Communication (DECT) デジタル コードレス電話
- **jammer** : 電波妨害デバイス
- **mw-oven** : 電子レンジ (802.11b/g/n のみ)
- **superag** : 802.11 SuperAG デバイス
- **tdd-tx** : 時分割複信 (TDD) トランスミッタ
- **video camera** : アナログ ビデオ カメラ

- **wimax-fixed** : WiMAX 固定デバイス
- **wimax-mobile** : WiMAX モバイル デバイス
- **xbox** : Microsoft Xbox (802.11b/g/n のみ)

ステップ 8 次のコマンドを入力して、未分類のデバイスに対する電波品質アラームのトリガーを設定します。
config {802.11a | 802.11b} cleanair alarm unclassified {enable | disable}

ステップ 9 次のコマンドを入力して、未分類のデバイスに対して電波品質アラームをトリガーするしきい値を指定します。

config {802.11a | 802.11b} cleanair alarm unclassified threshold *threshold*

threshold の値は、1～99 バイト（両端の値を含む）です。電波品質がしきい値レベルを下回ると、アラームが生成されます。値 1 は最低の電波品質を表し、100 は最高を表します。デフォルト値は 35 です。

ステップ 10 次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、イベント駆動型無線リソース管理 (RRM) の実行がトリガーされるよう設定します。

config advanced {802.11a | 802.11b} channel cleanair-event {enable | disable} : スペクトルイベント駆動型 RRM を有効または無効にします。デフォルト値はディセーブルです。

config advanced {802.11a | 802.11b} channel cleanair-event sensitivity {low | medium | high | custom} : RRM をトリガーするしきい値を指定します。アクセス ポイントに対してしきい値レベルを上回るレベルの干渉が発生すると、RRM によってローカルの動的チャンネル割り当て (DCA) の実行が開始され、可能であればネットワークのパフォーマンスが向上するように、影響を受けているアクセスポイント無線のチャンネルが変更されます。low は、この環境内で変更が行われる感度を下げることを表し、high はこの感度を上げることを表します。感度の値に custom を設定して、任意のレベルを選択することもできます。デフォルトは medium です。

config advanced {802.11a | 802.11b} channel cleanair-event sensitivity threshold *thresholdvalue* : 限界感度を custom に設定する場合は、カスタムしきい値を設定する必要があります。デフォルトは 35 です。

ステップ 11 次のコマンドを入力して、永続的デバイスの伝搬を有効にします。

config advanced {802.11a | 802.11b} channel pda-prop {enable | disable}

ステップ 12 次のコマンドを入力して、変更を保存します。

save config

ステップ 13 次のコマンドを入力して、802.11a/n または 802.11b/g/n ネットワークに対する Cisco CleanAir の設定を確認します。

show {802.11a | 802.11b} cleanair config

以下に類似した情報が表示されます。

```
(Cisco Controller) >show 802.11a cleanair config

Clean Air Solution..... Disabled
Air Quality Settings:
  Air Quality Reporting..... Enabled
  Air Quality Reporting Period (min)..... 15
  Air Quality Alarms..... Enabled
    Air Quality Alarm Threshold..... 35
    Unclassified Interference..... Disabled
    Unclassified Severity Threshold..... 20
```

```

Interference Device Settings:
  Interference Device Reporting..... Enabled
Interference Device Types:
  TDD Transmitter..... Enabled
  Jammer..... Enabled
  Continuous Transmitter..... Enabled
  DECT-like Phone..... Enabled
  Video Camera..... Enabled
  WiFi Inverted..... Enabled
  WiFi Invalid Channel..... Enabled
  SuperAG..... Enabled
  Canopy..... Enabled
  WiMax Mobile..... Enabled
  WiMax Fixed..... Enabled
Interference Device Alarms..... Enabled
  Interference Device Types Triggering Alarms:
    TDD Transmitter..... Disabled
    Jammer..... Enabled
    Continuous Transmitter..... Disabled
    DECT-like Phone..... Disabled
    Video Camera..... Disabled
    WiFi Inverted..... Enabled
    WiFi Invalid Channel..... Enabled
    SuperAG..... Disabled
    Canopy..... Disabled
    WiMax Mobile..... Disabled
    WiMax Fixed..... Disabled
Additional Clean Air Settings:
  CleanAir ED-RRM State..... Disabled
  CleanAir ED-RRM Sensitivity..... Medium
  CleanAir ED-RRM Custom Threshold..... 50
  CleanAir Persistent Devices state..... Disabled
  CleanAir Persistent Device Propagation..... Enabled

```

ステップ 14 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対するスペクトル イベント駆動型 RRM の設定を確認します。

```
show advanced {802.11a | 802.11b} channel
```

以下に類似した情報が表示されます。

```

Automatic Channel Assignment
  Channel Assignment Mode..... AUTO
  Channel Update Interval..... 600 seconds [startup]
  Anchor time (Hour of the day)..... 0
  Channel Update Contribution..... SNI
  CleanAir Event-driven RRM option..... Enabled
  CleanAir Event-driven RRM sensitivity..... Medium

```

アクセスポイントに対する Cisco CleanAir の設定

アクセスポイントに対する Cisco CleanAir の設定 (GUI)

ステップ 1 [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] の順に選択して、[802.11a/n/ac (または 802.11b/g/n) Radios] ページを開きます。

ステップ 2 カーソルを目的のアクセスポイントの青いドロップダウン矢印の上に置いて [Configure] をクリックします。[802.11a/n/ac (または 802.11b/g/n) Cisco APs > Configure] ページが表示されます。
[CleanAir Capable] フィールドには、このアクセスポイントが CleanAir の機能に対応しているかどうかが表示されます。対応している場合は、次の手順に進み、このアクセスポイントに対して CleanAir を有効または無効にします。アクセスポイントが CleanAir の機能に対応していない場合は、このアクセスポイントに対して CleanAir を有効にすることはできません。

(注) デフォルトでは、Cisco CleanAir の機能は無線に対して有効になっていません。

ステップ 3 [CleanAir Status] ドロップダウンリストから [Enable] を選択して、このアクセスポイントに対して Cisco CleanAir の機能を有効にします。このアクセスポイントで CleanAir の機能を無効にするには、[Disable] を選択します。デフォルト値は [Enable] です。この設定は、このアクセスポイントに対するグローバルな CleanAir の設定より優先します。

[Number of Spectrum Expert Connections] テキストボックスには、このアクセスポイント無線に現在接続している Spectrum Expert アプリケーションの数が表示されます。アクティブな接続は最大で 3 つまで可能です。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

ステップ 6 [Back] をクリックして、[802.11a/n/ac (または 802.11b/g/n) Radios] ページに戻ります。

ステップ 7 [802.11a/n/ac (または 802.11b/g/n) Radios] ページの [CleanAir Status] テキストボックスを見て、各アクセスポイント無線の Cisco CleanAir のステータスを確認します。

Cisco CleanAir のステータスは次のいずれかになります。

- [UP] : アクセスポイント無線に対するスペクトラムセンサーが現在正常に動作中です (エラーコード 0)。
- [DOWN] : アクセスポイント無線に対するスペクトラムセンサーは、エラーが発生したために現在動作していません。最も可能性の高いエラーの原因は、アクセスポイント無線が無効になっていることです (エラーコード 8)。このエラーを修正するには、無線を有効にしてください。
- [ERROR] : アクセスポイント無線に対するスペクトラムセンサーがクラッシュしており (エラーコード 128)、この無線に対する CleanAir のモニタリングが機能していません。このエラーが発生した場合は、アクセスポイントをリブートしてください。エラーが引き続き発生する場合は、この無線に対して Cisco CleanAir の機能を無効にすることもできます。
- [N/A] : このアクセスポイント無線は Cisco CleanAir の機能に対応していません。

- (注) フィルタを作成して、Cisco CleanAir の特定のステータス (UP、DOWN、ERROR、N/A など) を持つアクセスポイント無線だけを表示する [802.11a/n/ac Radios] ページや [802.11b/g/n Radios] ページを作成することもできます。この機能は、アクセスポイント無線のリストが複数ページに渡るために一目ですべてを確認できない場合に特に役立ちます。フィルタを作成するには、[Change Filter] をクリックして [Search AP] ダイアログボックスを開き、[CleanAir Status] チェックボックスを1つ以上選択して、[Find] をクリックします。検索基準に一致するアクセスポイント無線のみが [802.11a/n/ac Radios] ページまたは [802.11b/g/n Radios] ページに表示されます。また、ページ上部の [Current Filter] パラメータには、リストの作成に使用したフィルタが表示されます (たとえば、CleanAir Status: UP)。

アクセスポイントに対する Cisco CleanAir の設定 (CLI)

- ステップ 1** 次のコマンドを入力して、特定のアクセスポイントに Cisco CleanAir の機能を設定します。
config {802.11a | 802.11b} cleanair {enable | disable} Cisco_AP
- ステップ 2** 次のコマンドを入力して、変更を保存します。
save config
- ステップ 3** 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークにある特定のアクセスポイントの Cisco CleanAir の設定を確認します。
show ap config {802.11a | 802.11b} Cisco_AP
- 以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 0
Cisco AP Name..... CISCO_AP3500
...
Spectrum Management Information
  Spectrum Management Capable..... Yes
  Spectrum Management Admin State..... Enabled
  Spectrum Management Operation State..... Up
  Rapid Update Mode..... Disabled
  Spectrum Expert connection..... Disabled
  Spectrum Sensor State..... Configured (Error code = 0)
```

- (注) スペクトル管理機能の状態とスペクトラムセンサーの状態に関する考えられるエラーコードについての説明は、[アクセスポイントに対する Cisco CleanAir の設定 \(GUI\)](#)、(1080 ページ) のステップ 7 を参照してください。



第 145 章

干渉デバイスのモニタリング

- [干渉デバイスをモニタリングするための前提条件](#), 1083 ページ
- [干渉デバイスのモニタリング \(GUI\)](#), 1083 ページ
- [干渉デバイスのモニタリング \(CLI\)](#), 1085 ページ
- [永続的デバイスのモニタリング \(GUI\)](#), 1086 ページ
- [永続的デバイスのモニタリング \(CLI\)](#), 1086 ページ
- [無線帯域の電波品質のモニタリング](#), 1087 ページ

干渉デバイスをモニタリングするための前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

干渉デバイスのモニタリング (GUI)

ステップ 1 [Monitor] > [Cisco CleanAir] > [802.11a/n] または [802.11b/g/n] > [Interference Devices] を選択して、[CleanAir > Interference Devices] ページを開きます。

このページには、次の情報が表示されます。

- [AP Name] : 干渉デバイスが検出されたアクセス ポイントの名前。
- [Radio Slot #] : 無線が取り付けられているスロット。
- [Interferer Type] : 干渉源のタイプ。
- [Affected Channel] : デバイスから影響を受けているチャネル。
- [Detected Time] : 干渉が検出された時刻。
- [Severity] : 干渉デバイスの重大度の指標。

- [Duty Cycle (%)] : 干渉デバイスが動作している間の時間の割合。
- [RSSI] : アクセス ポイントの受信信号強度表示 (RSSI) 。
- [DevID] : 一意に識別できる干渉デバイスのデバイス識別番号。
- [ClusterID] : デバイスのタイプを一意に識別できるクラスタ識別番号。

ステップ 2 ある基準に基づいて干渉デバイスに関する情報を表示するには、[Change Filter] をクリックします。

ステップ 3 フィルタを削除して、アクセス ポイントのリスト全体を表示するには、[Clear Filter] をクリックします。次に示すパラメータに基づいて干渉デバイスのリストを表示するフィルタを作成することができます。

- [Cluster ID] : クラスタ ID に基づいてフィルタリングを行うには、このチェックボックスをオンにして、このフィールドの隣にあるテキスト ボックスにクラスタ ID を入力します。
- [APName] : アクセス ポイントの名前に基づいてフィルタリングを行うには、このチェックボックスをオンにして、このフィールドの隣にあるテキスト ボックスにアクセス ポイントの名前を入力します。
- [Interferer Type] : 干渉デバイスのタイプに基づいてフィルタリングを行うには、このチェックボックスをオンにして、オプションから干渉デバイスを選択します。

次のいずれかの干渉デバイスを選択します。

- BT Link
- MW Oven
- 802.11 FH
- BT Discovery
- TDD Transmit
- Jammer
- Continuous TX
- DECT Phone
- Video Camera
- 802.15.4
- WiFi Inverted
- WiFi Inv. Ch
- SuperAG
- Canopy
- XBox
- WiMax Mobile
- WiMax Fixed
- WiFi ACI

- Unclassified
- Activity Channels
- Severity
- Duty Cycle (%)
- RSSI

ステップ 4 [Find] をクリックします。
現在選択されているフィルタ パラメータは、[Current Filter] フィールドに表示されます。

干渉デバイスのモニタリング (CLI)

この項では、802.11a/n または 802.11b/g/n の無線帯域に対する干渉デバイスのモニタリングに使用するコマンドについて説明します。

アクセスポイントによる干渉源の検出

802.11a/n/ac または 802.11b/g/n 無線帯域の特定のアクセスポイントによって検出されたすべての干渉源の情報を表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair device ap Cisco_AP
```

CleanAir 対応のアクセスポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラムセンサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。ダウンしたデバイスは、スペクトラムデータベースから適正に削除されます。ある特定のデバイスに対する干渉源検出がすべてレポートされる場合は、クラスタ ID を長期間にわたって有効とし、デバイス検出が増大しないようにします。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth 対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAir では、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされるようにします。この処理によってユーザレコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

デバイスのタイプによる干渉源の検出

802.11a/n/ac または 802.11b/g/n 無線帯域について、特定のデバイス タイプのすべての干渉源の情報を表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair device type type
```

永続的干渉源の検出

802.11a/n/ac または 802.11b/g/n 無線帯域にある特定のアクセス ポイントに対する永続的干渉源の一覧を表示するには、次のコマンドを入力します。

```
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```

永続的デバイスのモニタリング (GUI)

Cisco WLC の GUI を使用して特定のアクセス ポイントで永続的デバイスをモニタするには、次の手順を実行します。

[Wireless] > [Access Points] > [Radios] > [802.11a/n] または [802.11b/g/n] の順に選択して [802.11a/n/ac (または 802.11b/g/n) Radios] ページを開きます。/ac カーソルを目的のアクセス ポイントの青いドロップダウン矢印の上に置いて [Detail] をクリックします。[802.11a/n/ac (または 802.11b/g/n) AP Interfaces > Detail] ページが表示されます。

このページには、アクセスポイントの詳細と、このアクセスポイントによって検出された永続的デバイスのリストが表示されます。永続的デバイスの詳細は、[Persistent Devices] セクションの下に表示されます。

それぞれの永続的デバイスについて、次の情報が表示されます。

- [Class Type] : 永続的デバイスの分類タイプ。
- [Channel] : このデバイスが影響を与えているチャンネル。
- [DC(%)] : 永続的デバイスのデューティ サイクル (パーセンテージ)。
- [RSSI(dBm)] : 永続的デバイスの RSSI インジケータ。
- [Last Seen Time] : このデバイスが最後にアクティブになったときのタイムスタンプ。

永続的デバイスのモニタリング (CLI)

CLI を使用して永続的デバイスの一覧を表示するには、次のコマンドを入力します。

```
show ap auto-rf {802.11a | 802.11b} ap_name
```

以下に類似した情報が表示されます。

```
Number Of Slots..... 2
AP Name..... AP_1142_MAP
MAC Address..... c4:7d:4f:3a:35:38
```

```

Slot ID..... 1
Radio Type..... RADIO_TYPE_80211a
Sub-band Type..... All
Noise Information
. . . . .
Power Level..... 1
  RTS/CTS Threshold..... 2347
  Fragmentation Threshold..... 2346
  Antenna Pattern..... 0

Persistent Interference Devices
Class Type          Channel  DC (%)  RSSI (dBm)  Last Update Time
-----
Video Camera        149     100    -34         Tue Nov  8 10:06:25 2011

```

それぞれの永続的デバイスについて、次の情報が表示されます。

- [Class Type] : 永続的デバイスの分類タイプ。
- [Channel] : このデバイスが影響を与えているチャンネル。
- [DC(%)] : 永続的デバイスのデューティ サイクル (パーセンテージ)。
- [RSSI(dBm)] : 永続的デバイスの RSSI インジケータ。
- [Last Seen Time] : このデバイスが最後にアクティブになったときのタイムスタンプ。

無線帯域の電波品質のモニタリング

この項では、Cisco WLC の GUI と CLI の両方を使用して、802.11a/n/ac および 802.11b/g/n 無線帯域の電波品質をモニタする方法について説明します。

無線帯域の電波品質のモニタリング (GUI)

[Monitor] > [Cisco CleanAir] > [802.11a/n/ac] または [802.11b/g/n] > [Air Quality Report] を選択して、[CleanAir > Air Quality Report] ページを開きます。

このページには、802.11a/n/ac と 802.11b/g/n の両方の無線帯域の電波品質が表示されます。特に、次の情報が表示されます。

- [AP Name] : 802.11a/n/ac または 802.11b/g/n 無線帯域において、電波品質が最悪と報告されているアクセス ポイントの名前。
- [Radio Slot] : 無線が取り付けられているスロットの番号。
- [Channel] : 電波品質をモニタしている無線チャンネル。
- [Minimum AQ] : この無線チャンネルの最低電波品質。
- [Average AQ] : この無線チャンネルの平均電波品質。
- [Interferer] : 802.11a/n/ac または 802.11b/g/n 無線帯域で無線によって検出された干渉源の数。
- [DFS] : 動的周波数選択。DFS が有効かどうかを表します。

無線帯域の電波品質のモニタリング (CLI)

この項では、802.11a/n/ac または 802.11b/g/n の無線帯域の電波品質のモニタに使用できるコマンドについて説明します。

電波品質のサマリーの表示

802.11a/n/ac または 802.11b/g/n 無線帯域の電波品質のサマリーを表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair air-quality summary
```

ある無線帯域のすべてのアクセスポイントの電波品質の表示

802.11a/n/ac または 802.11b/g/n のアクセスポイントとその電波品質の情報を表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair air-quality
```

ある無線帯域のアクセスポイントの電波品質の表示

802.11a/n/ac または 802.11b/g/n 無線帯域にある特定のアクセスポイントの電波品質に関する情報を表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair air-quality Cisco_AP
```

無線帯域の電波品質 (ワースト ケース) のモニタリング (GUI)

ステップ 1 [Monitor] > [Cisco CleanAir] > [Worst Air-Quality] を選択して、[CleanAir > Worst Air Quality Report] ページを開きます。

このページには、802.11a/n/ac と 802.11b/g/n の両方の無線帯域の電波品質が表示されます。特に、次の情報が表示されます。

- [APName] : 802.11 無線帯域において、電波品質が最悪と報告されているアクセスポイントの名前。
- [Channel Number] : 電波品質が最悪と報告された無線チャネル。
- [Minimum Air Quality Index(1 to 100)] : この無線チャネルの最低電波品質。電波品質の指標 (AQI) の値は、100 が最高で、1 が最悪です。
- [Average Air Quality Index(1 to 100)] : この無線チャネルの平均電波品質。電波品質の指標 (AQI) の値は、100 が最高で、1 が最悪です。
- [Interference Device Count] : 802.11 無線帯域で無線によって検出された干渉源の数。

ステップ 2 特定のアクセスポイント無線に対する永続的干渉源の一覧を確認するには、次の手順を実行します。

- a) [Wireless] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] の順に選択して、[802.11a/n/ac (または 802.11b/g/n) Radios] ページを開きます。
- b) カーソルを目的のアクセスポイント無線の青いドロップダウン矢印の上に置いて [CleanAir-RRM] をクリックします。[802.11a/n/ac (または 802.11b/g/n) Cisco APs > Access Point Name > Persistent Devices] ページが表示されます。このページには、このアクセスポイント無線によって検出された干渉源のデバイスタイプが一覧されます。また、干渉が検出されたチャネル、干渉がアクティブだった時間のパーセンテージ (デューティ サイクル)、干渉源の受信信号強度 (RSSI)、および干渉が最後に検出された日付と時刻も表示されます。

無線帯域の電波品質 (ワースト ケース) のモニタリング (CLI)

この項では、802.11 無線帯域の電波品質のモニタに使用できるコマンドについて説明します。

電波品質のサマリーの表示 (CLI)

802.11a/n/ac または 802.11b/g/n 無線帯域の電波品質のサマリーを表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair air-quality summary
```

ある無線帯域におけるすべてのアクセスポイントの中で最も悪い電波品質に関する情報の表示 (CLI)

802.11a/n/ac または 802.11b/g/n のアクセスポイントとその電波品質 (ワースト ケース) 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 {802.11a | 802.11b} cleanair air-quality worst
```

ある無線帯域のアクセスポイントの電波品質の表示 (CLI)

次のコマンドを入力して、802.11 無線帯域の特定のアクセスポイントに関する電波品質情報を表示します。

```
show {802.11a | 802.11b} cleanair air-quality Cisco_AP
```

デバイスタイプごとのアクセスポイントの電波品質の表示 (CLI)

- 802.11a/n/ac または 802.11b/g/n 無線帯域の特定のアクセスポイントによって検出されたすべての干渉源の情報を表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair device ap Cisco_AP
```

- 802.11a/n または 802.11b/g/n 無線帯域について、特定のデバイスタイプのすべての干渉源の情報を表示するには、次のコマンドを入力します。

```
show {802.11a | 802.11b} cleanair device type type
```

ここで、*type* には次のいずれかを選択します。

- **802.11-fh** : 802.11 周波数ホッピング デバイス (802.11b/g/n のみ)
- **802.11-inv** : スペクトラム反転 Wi-Fi 信号を使用するデバイス
- **802.11-nonstd** : 非標準の Wi-Fi チャンネルを使用するデバイス
- **802.15.4** : 802.15.4 デバイス (802.11b/g/n のみ)
- **all** : すべての干渉デバイス タイプ (これがデフォルト値です)
- **bt-discovery** : Bluetooth の検出 (802.11b/g/n のみ)
- **bt-link** : Bluetooth リンク (802.11b/g/n のみ)
- **canopy** : Canopy ブリッジ デバイス
- **cont-tx** : 連続トランスミッタ
- **dect-like** : Digital Enhanced Cordless Communication (DECT) デジタル コードレス電話
- **jammer** : 電波妨害デバイス
- **mw-oven** : 電子レンジ (802.11b/g/n のみ)
- **superag** : 802.11 SuperAG デバイス
- **tdd-tx** : 時分割複信 (TDD) トランスミッタ
- **video camera** : アナログ ビデオ カメラ
- **wimax-fixed** : WiMAX 固定デバイス
- **wimax-mobile** : WiMAX モバイル デバイス
- **xbox** : Microsoft Xbox (802.11b/g/n のみ)

永続的干渉源の検出 (CLI)

802.11a/n/ac または 802.11b/g/n 無線帯域にある特定のアクセス ポイントに対する永続的干渉源の一覧を表示するには、次のコマンドを入力します。

```
show ap auto-rf {802.11a | 802.11b} Cisco_AP
```




第 146 章

Spectrum Expert の接続の設定

- [Spectrum Expert 接続について](#), 1091 ページ
- [Spectrum Expert の設定 \(GUI\)](#), 1091 ページ

Spectrum Expert 接続について

スペクトラム アナライザから提供されるような RF 分析プロットの作成に使用できる詳細なスペクトラム データを入手するには、Cisco CleanAir 対応のアクセス ポイントを、Spectrum Expert アプリケーションを実行している Microsoft Windows XP または Vista の PC (*Spectrum Expert* コンソールと呼ばれる) に直接接続するよう設定します。Spectrum Expert との接続は、Prime Infrastructure から半自動的に開始することも、Cisco WLC から手動で開始することもできます。この項では、後者の方法について説明します。

Spectrum Expert の設定 (GUI)

はじめる前に

Spectrum Expert コンソールとアクセス ポイントとの間に接続を確立する前に、IP アドレスのルーティングが正しく設定され、途中にあるすべてのファイアウォールでネットワーク スペクトラム インターフェイス (NSI) ポートが開かれていることを確認します。

- ステップ 1** Spectrum Expert コンソールに接続するアクセス ポイントで、Cisco CleanAir 機能が有効になっていることを確認します。
- ステップ 2** Cisco WLC GUI または CLI を使用してアクセス ポイントを SE-Connect モードに設定します。
(注) SE-Connect モードは、1 つの無線だけでなく、そのアクセス ポイント全体に対して設定されません。しかし、Spectrum Expert コンソールが接続するのは一度に 1 つの無線です。

Cisco WLC GUI を使用している場合は、次の手順に従ってください。

- a) [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

- b) 対象のアクセスポイントの名前を選択して、[All APs > Details for] ページを開きます。
 - c) [AP Mode] ドロップダウンリストから [SE-Connect] を選択します。このモードは、Cisco CleanAir 機能にサポートできるアクセスポイントでのみ使用できます。SE-Connect モードが使用可能なオプションとして表示されるには、アクセスポイントに有効状態のスペクトラム対応無線が少なくとも 1 つ以上ある必要があります。
 - d) [Apply] をクリックして、変更を確定します。
 - e) アクセスポイントをリポートするように求められたら、[OK] をクリックします。
- CLI を使用している場合は、次の手順に従ってください。

- a) 次のコマンドを入力して、アクセスポイントに SE-Connect モードを設定します。
`config ap mode se-connect Cisco_AP`
 - b) アクセスポイントをリポートするように求められたら、「Y」と入力します。
 - c) 次のコマンドを入力して、アクセスポイントの SE-Connect の設定状況を確認します。
`show ap config {802.11a | 802.11b} Cisco_AP`
- 以下に類似した情報が表示されます。

```
Cisco AP Identifier..... 0
Cisco AP Name..... CISCO_AP3500
...
Spectrum Management Information
  Spectrum Management Capable..... Yes
  Spectrum Management Admin State..... Enabled
  Spectrum Management Operation State..... Up
  Rapid Update Mode..... Disabled
  Spectrum Expert connection..... Enabled
  Spectrum Sensor State..... Configured (Error code = 0)
```

ステップ 3 Windows PC で、次の URL から Cisco Software Center にアクセスします。
<http://www.cisco.com/cisco/software/navigator.html>

ステップ 4 [Product] > [Wireless] > [Cisco Spectrum Intelligence] > [Cisco Spectrum Expert] > [Cisco Spectrum Expert Wi-Fi] の順にクリックし、Spectrum Expert 4.0 の実行可能ファイル (*.exe) をダウンロードします。

ステップ 5 PC で Spectrum Expert アプリケーションを実行します。

ステップ 6 [Connect to Sensor] ダイアログボックスが表示されたら、アクセスポイントの IP アドレスを入力し、アクセスポイントの無線を選択し、認証のために 16 バイトのネットワーク スペクトラム インターフェイス (NSI) キーを入力します。Spectrum Expert アプリケーションによって、NSI プロトコルを使用して、アクセスポイントへの TCP/IP による直接接続が開かれます。

- (注) アクセスポイントは、2.4 GHz の周波数をポート 37540 で、5 GHz の周波数をポート 37550 でリスニングする TCP サーバである必要があります。これらのポートは、Spectrum Expert アプリケーションが NSI プロトコルを使用してアクセスポイントに接続するために、開かれている必要があります。
- (注) Cisco WLC GUI では、NSI キーは [All APs > Details for] ページにある [Network Spectrum Interface Key] フィールド ([Port Number] フィールドの下) に表示されます。Cisco WLC CLI から NSI キーを表示するには、`show ap config {802.11a | 802.11b} Cisco_AP` コマンドを入力します。

SE-Connect モードのアクセス ポイントが Cisco WLC に join すると、アクセス ポイントから Spectrum Capabilities 通知メッセージが送信され、Cisco WLC は Spectrum Configuration Request で応答します。この要求には 16 バイトのランダム NSI キーが含まれます。このキーは NSI 認証で使用するために Cisco WLC で作成されたものです。Cisco WLC はアクセス ポイントごとにキーを 1 つ作成し、アクセス ポイントはこのキーをリブートするまで保存します。

(注) Spectrum Expert コンソール接続は、アクセス ポイントの無線ごとに最大 3 つまで確立できます。Cisco WLC GUI の [802.11a/n/ac (または 802.11b/g/n) Cisco APs > Configure] ページにある [Number of Spectrum Expert Connections] テキスト ボックスには、現在アクセス ポイント無線に接続されている Spectrum Expert アプリケーションの数が表示されます。

- ステップ 7** Spectrum Expert アプリケーションの右下隅にある [Slave Remote Sensor] テキスト ボックスを選択して、Spectrum Expert コンソールがアクセス ポイントに接続されていることを確認します。デバイスが 2 台接続されている場合は、このテキスト ボックスにアクセス ポイントの IP アドレスが表示されます。
- ステップ 8** Spectrum Expert アプリケーションを使用して、アクセス ポイントからのスペクトラム データを表示および分析します。
-



第 **IX** 部

FlexConnect の設定

- [FlexConnect の設定, 1097 ページ](#)
- [FlexConnect ACL の設定, 1123 ページ](#)
- [FlexConnect グループの設定, 1129 ページ](#)
- [FlexConnect の AAA Override の設定, 1143 ページ](#)
- [FlexConnect アクセスポイントに対する FlexConnect AP のアップグレードの設定, 1149 ページ](#)



第 147 章

FlexConnect の設定

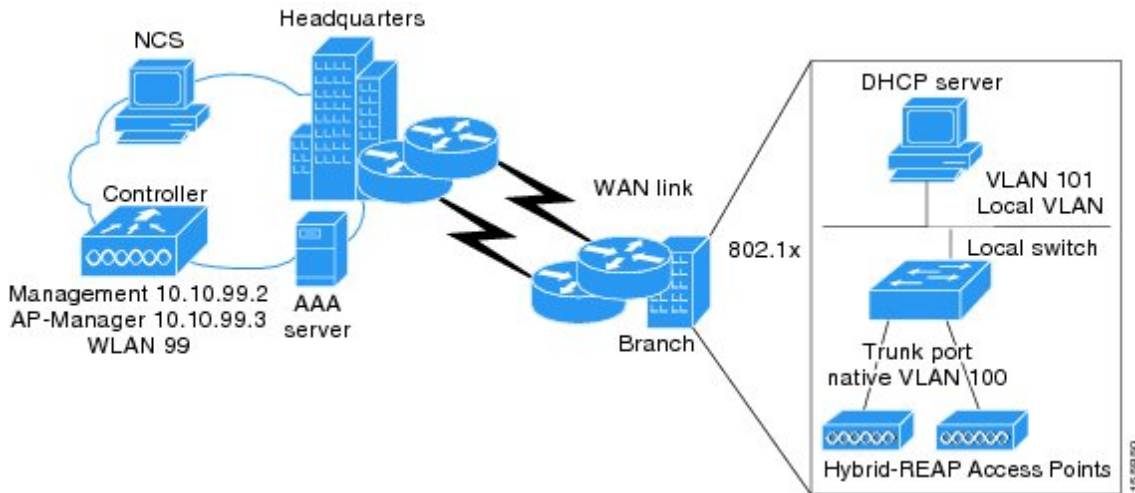
- [FlexConnect について, 1097 ページ](#)
- [FlexConnect の制約事項, 1104 ページ](#)
- [FlexConnect の設定, 1106 ページ](#)
- [FlexConnect イーサネットフォールバックの設定, 1120 ページ](#)

FlexConnect について

FlexConnect（以前は、ハイブリッドリモートエッジアクセスポイントまたは H-REAP と呼ばれていました）は、ブランチオフィスとリモートオフィスに導入されるワイヤレスソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスから Wide Area Network（WAN; ワイドエリアネットワーク）経由で、支社またはリモートオフィスのアクセスポイントを設定および制御できるようになります。FlexConnect アクセスポイントは、コントローラへの接続を失ったとき、クライアントデータトラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。接続モードで、FlexConnect アクセスポイントは、ローカル認証も実行できます。

次の図に、FlexConnect の一般的な導入を示します。

図 71 : FlexConnect の導入



コントローラ ソフトウェアでは、FlexConnect アクセス ポイントに対する耐障害性をより強化した方法が提供されています。以前のリリースでは、コントローラから解除されるたびに、FlexConnect アクセス ポイントはスタンドアロン モードに移行します。中央でスイッチされるクライアントのアソシエーションは解除されます。ただし、FlexConnect アクセス ポイントはローカルにスイッチされたクライアントに引き続き対応します。FlexConnect アクセス ポイントがコントローラ（またはスタンバイ コントローラ）に再 join すると、すべてのクライアントが接続解除され、再度認証されます。この機能は強化されており、クライアントと FlexConnect アクセス ポイント間の接続はそのまま保持され、クライアントによるシームレスな接続が実現します。この機能は、アクセス ポイントとコントローラの設定が同じである場合にだけ使用できます。

中央で認証されたクライアントは再認証されます。

セッションタイムアウトおよび再認証は、アクセス ポイントがコントローラへの接続を確立したときに実行されます。

クライアント接続が確立された後に、コントローラはクライアントの元の属性を復元しません。クライアントのユーザ名、現在のレートとサポートされているレート、およびリッスン間隔値は、セッション タイマーが切れた後でのみデフォルト値にリセットされます。

FlexConnect アクセス ポイントは、1 ロケーションにつき何台でも展開できます。複数の FlexConnect グループを 1 つのロケーションで定義できます。

コントローラはユニキャスト パケットまたはマルチキャスト パケットの形式でアクセス ポイントにマルチキャスト パケットを送信できます。FlexConnect モードで、アクセス ポイントはユニキャスト形式でのみマルチキャスト パケットを受信できます。

FlexConnect アクセス ポイントは、1 対 1 のネットワーク アドレス変換 (NAT) 設定をサポートします。また、真のマルチキャストを除くすべての機能に対して、ポート アドレス変換 (PAT) をサポートします。NAT 境界を越えるマルチキャストもサポートされます (ユニキャスト オプションを使用して設定されている場合)。FlexConnect アクセス ポイントは、中央でスイッチされる

すべての WLAN に対して真のマルチキャストが動作するときを除き、多対 1 の NAT/PAT 境界もサポートします。



- (注) NAT と PAT は FlexConnect アクセス ポイントではサポートされていますが、対応するコントローラではサポートされていません。シスコは、NAT/PAT 境界の背後にコントローラを置く構成はサポートしません。

アクセスポイントで、これらのセキュリティタイプがローカルにアクセス可能である場合、VPN および PPTP は、ローカルにスイッチされるトラフィックに対してサポートされます。

FlexConnect アクセス ポイントは複数の SSID をサポートします。

ワーク グループブリッジおよびユニバーサルワークグループブリッジは、ローカルにスイッチされるクライアントの FlexConnect アクセス ポイントでサポートされます。

FlexConnect は、IPv4 の動作と同様にトラフィックをローカル VLAN にブリッジすることによって、IPv6 クライアントをサポートしています。FlexConnect は、最大 100 のアクセス ポイントのグループに対するクライアント モビリティをサポートしています。

現在の FlexConnect 設定で、コントローラとアクセスポイント間のリンクが動作を停止した場合、FlexConnect AP はスタンドアロン モードになります。

AP がローカルから FlexConnect にモードを変更する場合、AP はリブートする必要があります。リブートによって支店の導入全体に遅延が発生します。FlexConnect AP の導入期間の短縮のために、モードが変更されると、コントローラは AP への `spam_reset_AP` メッセージの送信を停止します。AP については、モード変更ペイロードを受信すると、`lwapp_reap_start()` コマンドを実行します。このアクションによって REAP モジュールが開始され、AP モードは FlexConnect に変更されます。

AP がコントローラに設定更新要求を送信すると、FlexConnect パラメータが設定されます。AP とコントローラ間の接続は維持されます。アソシエーション解除は行われません。



- (注) ローカルから FlexConnect へのモード変更は導入期間の短縮に対してサポートされています。他のモード変更の場合、AP はリブートする必要があります。AP サブモードでのワイヤレス侵入防御システム (wIPS) への変更の場合、リブートは必要ありません。その他のサブモード設定では、AP のリブートが必要です。

FlexConnect 認証プロセス

アクセスポイントは、ブート時にコントローラを検索します。コントローラが見つかったら、そのコントローラに join し、最新のソフトウェアイメージと設定をコントローラからダウンロードして、無線を初期化します。ダウンロードした設定は不揮発性メモリに保存されて、スタンドアロンモードで使用されます。



- (注) 最新のコントローラソフトウェアのダウンロード後に、アクセスポイントをリブートしたら、アクセスポイントを FlexConnect モードへ変換する必要があります。これは、GUI または CLI を使用して行えます。

FlexConnect アクセスポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- アクセスポイントの IP アドレスが DHCP サーバから割り当て済みの場合は、通常の CAPWAP または LWAPP ディスカバリ プロセスを介してコントローラを検出します。



- (注) OTAP は、6.0.196 以降のコードを使用するコントローラではサポートされなくなりました。

- アクセスポイントに固定 IP アドレスが割り当てられている場合は、DHCP オプション 43 以外の方法のディスカバリ プロセスを使用してコントローラを検出します。アクセスポイントがレイヤ 3 ブロードキャストでコントローラを検出できない場合は、DNS 解決を使用することをお勧めします。DNS を使用すれば、固定 IP アドレスを持ち DNS サーバを認識しているアクセスポイントは、最低 1 つのコントローラを見つけることができます。
- CAPWAP と LWAPP のどちらのディスカバリ メカニズムも使用できないリモートネットワークにあるコントローラを検出できるようにするには、プライミングを使用してください。この方法を使用すると、アクセスポイントの接続先のコントローラを（アクセスポイントの CLI により）指定できます。



- (注) アクセスポイントがコントローラを検索する方法の詳細については、コントローラ導入ガイド (<http://www.cisco.com/en/US/docs/wireless/technology/controller/deployment/guide/dep.html>) を参照してください。

FlexConnect アクセスポイントがコントローラに到達できる時（接続モードと呼ばれます）、コントローラはクライアント認証を支援します。FlexConnect アクセスポイントがコントローラにアクセスできないとき、アクセスポイントはスタンドアロンモードに入り、独自にクライアントを認証します。



- (注) アクセスポイント上の LED は、デバイスが異なる FlexConnect モードに入るときに変化します。LED パターンの情報については、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。

クライアントが FlexConnect アクセスポイントにアソシエートするとき、アクセスポイントではすべての認証メッセージをコントローラに送信し、WLAN 設定に応じて、クライアントデータパケットをローカルにスイッチする（ローカルスイッチング）か、コントローラに送信（中央ス

スイッチング) します。クライアント認証 (オープン、共有、EAP、Web 認証、および NAC) とデータパケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- 中央認証、中央スイッチング：コントローラがクライアント認証を処理し、すべてのクライアントデータはコントローラにトンネルを通じて戻されます。この状態は、接続済みモードの場合にだけ有効です。
- 中央認証、ローカルスイッチング：コントローラがクライアント認証を処理し、FlexConnect アクセスポイントがデータパケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードと共にコンフィギュレーションコマンドを送信し、FlexConnect アクセスポイントに対して、ローカルにデータパケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。
- ローカル認証、ローカルスイッチング：FlexConnect アクセスポイントがクライアント認証を処理し、クライアントデータパケットをローカルにスイッチします。この状態はスタンダロンモードおよび接続済みモードの場合に有効です。

接続済みモードでは、アクセスポイントは、ローカルで認証されたクライアントに関する最小限の情報をコントローラに提供します。次の情報はコントローラでは使用できません。

- ポリシータイプ
- アクセス VLAN
- VLAN 名
- サポートされるレート
- 暗号化の暗号

ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位 (MTU) が 500 バイトを下回らない、最小帯域幅が 128 kbps のリモートオフィス設定を維持できない場合に役立ちます。ローカル認証で、認証機能はアクセスポイント自体に存在します。ローカル認証は、ブランチオフィスの遅延要件を短縮できます。



(注) ローカル認証は、ローカルスイッチングモードの FlexConnect アクセスポイントの WLAN 上のみで有効にできます。

ローカル認証に関する注意事項は、次のとおりです。

- ゲスト認証は、FlexConnect ローカル認証を有効にした WLAN で実行できません。
- コントローラ上でのローカル RADIUS はサポートされていません。
- クライアントが認証されたら、ローミングはグループ内のコントローラおよび他の FlexConnect アクセスポイントがクライアント情報に更新された後でのみサポートされます。
- 接続モードのローカル認証には、WLAN 設定が必要です。



(注) FlexConnect アクセス ポイントに接続している、ローカルにスイッチされたクライアントが IP アドレスを更新し、また join する場合に、クライアントは実行状態のまま残ります。これらのクライアントはコントローラによって再認証されません。

- 認証ダウン、スイッチダウン：この状態になると、WLAN は既存クライアントのアソシエーションを解除し、ビーコン要求とプローブ要求の送信を停止します。この状態はスタンドアロン モードおよび接続済みモードの両方の場合に有効です。
- 認証ダウン、ローカル スイッチング：WLAN は新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロン モードでのみ有効です。

FlexConnect アクセス ポイントがスタンドアロン モードになると、オープン、共通、WPA-PSK、または WPA2-PSK の認証用に設定された WLAN は、「ローカル認証、ローカル スイッチング」状態になり、新しいクライアント認証を続行します。コントローラ ソフトウェア リリース 4.2 以降のリリースでは、これは 802.1X、WPA-802.1X、WPA2-802.1X、または CCKM 用に設定された WLAN でも正しい設定です。ただし、これらの認証タイプでは外部の RADIUS サーバが設定されている必要があります。FlexConnect アクセス ポイントでローカル RADIUS サーバを設定して、スタンドアロン モードで、またはローカル認証と組み合わせて 802.1X をサポートすることもできます。

その他の WLAN は、「認証停止、スイッチング停止」状態（WLAN が中央スイッチング用に設定されている場合）または「認証停止、ローカル スイッチング」状態（WLAN がローカルスイッチング用に設定されている場合）のいずれかになります。

FlexConnect アクセス ポイントがスタンドアロン モードではなく、コントローラに接続されている場合は、コントローラはプライマリ RADIUS サーバを使用します。コントローラがプライマリ RADIUS サーバにアクセスする順序は、[RADIUS Authentication Servers] ページまたは **config radius auth add** CLI コマンドで指定されたとおりとなります（WLAN に対して別のサーバ順序が指定されている場合を除く）。ただし、802.1X EAP 認証を使用する場合は、クライアントを認証するために、スタンドアロン モードの FlexConnect アクセス ポイント用のバックアップ RADIUS サーバが必要となります。



(注) コントローラはバックアップ RADIUS サーバを使用しません。コントローラはローカル認証モードでバックアップ RADIUS サーバを使用します。

バックアップ RADIUS サーバは、個々のスタンドアロン モード FlexConnect アクセス ポイントに対して設定することも（コントローラの CLI を使用）、スタンドアロン モード FlexConnect アクセス ポイントのグループに対して設定することも（GUI または CLI を使用）できます。個々のアクセス ポイントに対して設定されたバックアップ サーバは、FlexConnect に対するバックアップ RADIUS サーバ設定よりも優先されます。

FlexConnect アクセス ポイントがスタンダロン モードに入ると、中央スイッチング WLAN 上にあるすべてのクライアントのアソシエートが解除されます。Web 認証 WLAN の場合は、既存クライアントのアソシエートは解除されませんが、アソシエートされているクライアントの数がゼロ (0) に達すると、FlexConnect アクセス ポイントからのビーコン応答の送信が停止します。また、Web 認証 WLAN にアソシエートしようとする新しいクライアントにアソシエート解除メッセージが送信されます。ネットワーク アクセス制御 (NAC) や Web 認証 (ゲスト アクセス) などのコントローラに依存するアクティビティは無効になり、アクセス ポイントは侵入検知システム (IDS) レポートをコントローラに送信しません。さらに、ほとんどの無線リソース管理 (RRM) 機能 (ネイバーディスカバリ、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバリストの使用、不正阻止および検出) は無効化されます。ただし、FlexConnect アクセス ポイントは、スタンダロン モードで動的周波数選択をサポートします。

Web 認証がリモート サイトで FlexConnect のアクセス ポイントに使用されると、クライアントはリモート ローカルサブネットから IP アドレスを取得します。最初の URL 要求を解決するため、DNS がサブネットのデフォルト ゲートウェイを介してアクセスできます。コントローラが DNS クエリーの応答パケットを代行受信およびリダイレクトするには、これらのパケットは CAPWAP 接続を介してデータセンターでコントローラにアクセスする必要があります。Web 認証プロセス中、FlexConnect のアクセス ポイントは DNS と DHCP メッセージのみを許可します。つまり、アクセス ポイントは、クライアントの Web 認証が完了するまで DNS 応答メッセージをコントローラに転送します。クライアントの Web 認証が完了すると、すべてのトラフィックがローカルでスイッチされます。



(注)

コントローラが NAC に対して設定されている場合、クライアントはアクセス ポイントが接続モードにある場合にのみアソシエートできます。NAC が有効化されているときは、正常に動作しない VLAN (または隔離 VLAN) を作成してください。この VLAN に割り当てられたクライアントのデータトラフィックがコントローラを経由するようにするためです。これは、WLAN がローカルスイッチングを行うように設定されている場合でも必要です。クライアントが隔離 VLAN に割り当てられると、そのクライアントのデータパケットはすべて中央でスイッチングされます。隔離 VLAN の作成の詳細については、「動的インターフェイスの設定」の項を参照してください。NAC アウトオブバンドサポートの設定の詳細については、「NAC アウトオブバンド統合の設定」の項を参照してください。

FlexConnect アクセス ポイントがスタンダロン モードになると、次のようになります。

- アクセス ポイントは、ARP 経由でデフォルトゲートウェイに到達できるかどうかを確認します。その場合、アクセス ポイントはコントローラへの到達を試行し続けます。

アクセス ポイントが ARP を確立できない場合は、次のことが起こります。

- アクセス ポイントは 5 回の検出を試行し、それでもコントローラを検出できない場合は、新しい DHCP IP を取得するために、イーサネットインターフェイス上で DHCP を更新しようとします。
- アクセス ポイントが、5 回再試行して失敗した場合、インターフェイスの IP アドレスを再度更新します。これは 3 回試行されます。

- 3回の試行が失敗した場合、アクセスポイントは固定IPに戻ってリブートします（アクセスポイントが固定IPを使用して設定されている場合のみ）。
- リブートの実行により、アクセスポイントの不明なエラーの可能性が排除されます。

アクセスポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエーション解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

FlexConnect の制約事項

- 設定変更をローカルにスイッチされる WLAN に適用すると、アクセスポイントが無線のリセットすることによって、関連付けら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ます（変更された WLAN に関連付けられていないクライアントも含む）。ただし、この動作は変更された WLAN が中央でスイッチされる場合は発生しません。メンテナンス時にも設定変更を実行することをお勧めします。
- 固定 IP アドレスまたは DHCP アドレスを持つ FlexConnect アクセスポイントを展開することができます。DHCP の場合、DHCP サーバはローカルに使用可能であり、ブート時にアクセスポイントの IP アドレスを提供する必要があります。
- FlexConnect は最大で 4 つの断片化されたパケット、または最低 500 バイトの最大伝送単位 (MTU) WAN リンクをサポートします。
- アクセスポイントとコントローラ間のラウンドトリップ遅延が 300 ミリ秒 (ms) を超えてはなりません。また、CAPWAP コントロールパケットは他のすべてのトラフィックよりも優先される必要があります。300 ミリ秒のラウンドトリップ遅延を実現できない場合は、アクセスポイントを設定してローカル認証を実行できます。
- クライアント接続は、アクセスポイントがスタンダアロンモードから接続モードに移行するときに RUN 状態になっている、ローカルにスイッチされたクライアントに対してのみ復元されます。アクセスポイントがスタンダアロンモードから接続モードに移行した後、アクセスポイントの無線もリセットされます。
- コントローラの設定は、アクセスポイントがスタンダアロンモードになった時点と、アクセスポイントが接続済みモードに戻った時点の間で同じである必要があります。同様に、アクセスポイントがセカンダリコントローラまたはバックアップコントローラにフォールバックする場合、プライマリコントローラとセカンダリコントローラまたはバックアップコントローラの設定は同じである必要があります。
- 新規に接続したアクセスポイントは、FlexConnect モードでブートできません。
- CCKM 高速ローミングを FlexConnect アクセスポイントで使用するには、FlexConnect グループを設定する必要があります。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカルスイッチングを行うように設定されている WLAN での使用はサポートされていません。

- FlexConnect アクセスポイントのプライマリ コントローラとセカンダリ コントローラの設定が同一であることが必要です。設定が異なると、アクセスポイントはその設定を失い、特定の機能（WLAN の無効化、VLAN、静的チャンネル番号など）が正しく動作しないことがあります。さらに、FlexConnect アクセスポイントの SSID とそのインデックス番号が、両方のコントローラで同一であることを確認してください。
- 2500 シリーズ コントローラに FlexConnect モードのアクセスポイントを直接接続しないでください。
- アクセスポイントで設定された syslog サーバと組み合わせて、FlexConnect アクセスポイントを設定する場合、アクセスポイントがリロードされ、1 以外のネイティブ VLAN になった後、初期化時に、アクセスポイントからの syslog パケットで VLAN ID 1 のタグが付けられているものはほとんどありません。これは既知の問題です。
- MAC フィルタリングは、スタンドアロンモードの FlexConnect アクセスポイントではサポートされていません。ただし、MAC フィルタリングは、接続モードの FlexConnect アクセスポイントでのローカルスイッチングと中央認証はサポートされています。また、FlexConnect アクセスポイントを持つローカルにスイッチされる WLAN の Open SSID、MAC フィルタリングおよび RADIUS NAC は、MAC が ISE でチェックされる有効な設定です。
- FlexConnect で、IPv6 ACL、ネイバー ディスカバリ キャッシュ、および IPv6 NDP パケットの DHCPv6 スヌーピングはサポートされていません。
- FlexConnect では、クライアントの詳細を示すページにどの IPv6 クライアントのアドレスも表示されません。
- ローカルにスイッチされた WLAN を使用した FlexConnect アクセスポイントでは、IP ソースガードを実行したり、ARP スプーフィングを防止したりすることができません。中央でスイッチされた WLAN では、ワイヤレスコントローラは IP ソースガードおよび ARP スプーフィングを実行します。
- ローカル スwitching を使用する FlexConnect AP における ARP スプーフィング攻撃を防ぐために、ARP インスペクションを使用することを推奨します。
- Flexconnect AP の WLAN でローカル スwitching を有効にすると、AP はローカル スwitching を実行します。ただし、ローカルモードの AP に対しては、中央スウィッチングが実行されます。
- FlexConnect スタンドアロンモードの Wi-Fi Protected Access バージョン 2 (WPA2)、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Advanced Encryption Standard (AES) のみがサポートされます。
- FlexConnect スタンドアロンモードの Wi-Fi Protected Access (WPA)、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Temporal Key Integrity Protocol (TKIP) のみがサポートされます。
- TKIP による WPA2 および AES による WPA は、スタンドアロンモード、接続モードのローカル認証、および接続モードの CCKM 高速ローミングではサポートされません。
- AVC は FlexConnect ローカル スwitch モードの AP ではサポートされません。

FlexConnect の設定



(注) 設定作業は、リストされている順序で実行する必要があります。

リモート サイトでのスイッチの設定

ステップ 1 FlexConnect を有効にするアクセス ポイントを、スイッチ上のトランクまたはアクセス ポートに接続します。

(注) この手順に示す設定例では、FlexConnect アクセス ポイントはスイッチ上のトランク ポートに接続されます。

ステップ 2 この手順の設定例を参照して、スイッチが FlexConnect アクセス ポイントをサポートするように設定します。

この設定例では、FlexConnect アクセス ポイントは、トランク インターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。このアクセス ポイントは、このネイティブ VLAN 上での IP 接続を必要とします。リモートサイトのローカルサーバとリソースは、VLAN 101 上にあります。DHCP プールがスイッチの両 VLAN のローカル スイッチ内に作成されます。最初の DHCP プール（ネイティブ）は FlexConnect アクセス ポイントにより使用され、2 つ目の DHCP プール（ローカルスイッチング）は、クライアントがローカルでスイッチングされる WLAN にアソシエートする場合、クライアントにより使用されます。設定例の太字のテキストは、これらの設定を示します。

ローカル スイッチの設定例は次のとおりです。

```
ip dhcp pool NATIVE
  network 209.165.200.224 255.255.255.224
  default-router 209.165.200.225
  dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
  network 209.165.201.224 255.255.255.224
  default-router 209.165.201.225
  dns-server 192.168.100.167
!
interface FastEthernet1/0/1
  description Uplink port
  no switchport
  ip address 209.165.202.225 255.255.255.224
!
interface FastEthernet1/0/2
  description the Access Point port
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 100
  switchport trunk allowed vlan 101
  switchport mode trunk
```



```

!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
end
!

```

FlexConnect に対するコントローラの設定

次の 2 つの環境で FlexConnect のコントローラを設定できます。

- 中央でスイッチされる WLAN
- ローカルでスイッチされる WLAN

FlexConnect のコントローラの設定には、中央でスイッチされる WLAN とローカルにスイッチされる WLAN を作成する操作が含まれます。次の表に、3 つの WLAN の例を示します。

表 28 : WLAN の例

| WLAN | セキュリティ | 認証 | スイッチング | インターフェイスマッピング (VLAN) |
|---------------------|-----------------|------|--------|------------------------------|
| employee | WPA1+WPA2 | 中央 | 中央 | management (中央でスイッチされる VLAN) |
| employee-local | WPA1+WPA2 (PSK) | ローカル | ローカル | 101 (ローカルにスイッチされる VLAN) |
| guest-central | Web 認証 | 中央 | 中央 | management (中央でスイッチされる VLAN) |
| employee-local-auth | WPA1+WPA2 | ローカル | ローカル | 101 (ローカルにスイッチされる VLAN) |

FlexConnect に対するコントローラの設定（ゲスト アクセスに使用される中央でスイッチされた WLAN の場合）

はじめる前に

ゲスト ユーザ アカウントが作成されている必要があります。ゲスト ユーザ アカウントの作成方法の詳細については、『Cisco Wireless LAN Controller System Management Guide』を参照してください。

-
- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** ドロップダウン リストから [Create New] を選択し、[Go] をクリックして [WLANs > New] ページを開きます。
- ステップ 3** [Type] ドロップダウン リストから、[WLAN] を選択します。
- ステップ 4** [Profile Name] テキスト ボックスに、`guest-central` を入力します。
- ステップ 5** [WLAN SSID] テキスト ボックスに、`guest-central` を入力します。
- ステップ 6** [WLAN ID] ドロップダウン リストから、WLAN の ID を選択します。
- ステップ 7** [Apply] をクリックします。[WLANs > Edit] ページが表示されます。
- ステップ 8** [General] タブで、[Status] チェックボックスをオンにして WLAN を有効にします。
- ステップ 9** [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [None] を選択します。
- ステップ 10** [Security > Layer 3] タブで次の手順を実行します。
- [Layer 3 Security] ドロップダウン リストから [None] を選択します。
 - [Web Policy] チェックボックスをオンにします。
 - [Authentication] を選択します。
- (注)
- 外部 Web サーバを使用する場合は、WLAN 上でそのサーバに対する事前認証アクセス コントロール リスト (ACL) を設定し、[Layer 3] タブでこの ACL を WLAN 事前認証 ACL として選択する必要があります。
- ステップ 11** [Apply] をクリックします。
- ステップ 12** [Save Configuration] をクリックします。
-

FlexConnect に対するコントローラの設定 (GUI)

- ステップ 1** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2** ドロップダウン リストから [Create New] を選択し、[Go] をクリックして [WLANs > New] ページを開きます。
- ステップ 3** [Type] ドロップダウン リストから、[WLAN] を選択します。
- ステップ 4** [Profile Name] テキスト ボックスに、WLAN の一意のプロファイル名を入力します。
- ステップ 5** [WLAN SSID] テキスト ボックスに、WLAN の名前を入力します。
- ステップ 6** [WLAN ID] ドロップダウン リストから、この WLAN の ID 番号を選択します。
- ステップ 7** [Apply] をクリックします。
[WLANs > Edit] ページが表示されます。
- ステップ 8** 中央でスイッチされる WLAN とローカルにスイッチされる WLAN の両方で FlexConnect のコントローラを設定できます。
中央でスイッチされる WLAN で FlexConnect のコントローラを設定するには、次の手順を実行します。
- [General] タブで、[Status] チェックボックスをオンにして WLAN を有効にします。
 - NAC を有効にし、隔離 VLAN を作成してから、この WLAN に使用する場合は、[General] タブの [Interface/Interface Group(G)] ドロップダウン リストからインターフェイスを選択します。
 - [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択し、必要に応じて WPA+WPA2 パラメータを設定します。
- ローカルでスイッチされる WLAN で FlexConnect のコントローラを設定するには、次の手順を実行します。
- [General] タブで、[Status] チェックボックスをオンにして WLAN を有効にします。
 - NAC を有効にし、隔離 VLAN を作成してから、この WLAN に使用する場合は、[General] タブの [Interface/Interface Group(G)] ドロップダウン リストからインターフェイスを選択します。
 - [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [WPA+WPA2] を選択し、必要に応じて [WPA+WPA2] パラメータを設定します。
 - [Advanced] タブで、次の手順を実行します。
 - [FlexConnect Local Switching] チェックボックスをオンまたはオフにして、または FlexConnect モードの AP に関連付けられているクライアントデータのローカル スイッチングを有効または無効にします。

(注) 次に、この機能に関するガイドラインおよび制限事項を示します。

- ローカル スイッチングを有効化すると、この WLAN をアドバタイズするすべての FlexConnect アクセス ポイントは、データ パケットを（コントローラへトンネリングする代わりに）ローカルにスイッチできます。
 - FlexConnect ローカル スイッチングが有効のときは、デフォルトではコントローラはクライアントの IP アドレスを認識するために有効になります。ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。コントローラがクライアントの IP アドレスを認識できるまで待たなくてもクライアント接続を維持できるように、クライアント IP アドレス認識機能を無効にしてください。このオプションを無効にできるのは、FlexConnect ローカル スイッチングを行うように設定されているときだけです。FlexConnect 中央スイッチングを行う場合は、無効にすることはできません。
 - FlexConnect アクセス ポイントの場合、FlexConnect ローカルスイッチングに対して設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとしてアクセス ポイントで継承されます。このマッピングは SSID ごと、FlexConnect アクセス ポイントごとに変更できます。FlexConnect 以外のアクセス ポイントでは、すべてのトラフィックがトンネルを通じてコントローラに戻され、VLAN タギングは各 WLAN のインターフェイス マッピングによって決定されます。
- [FlexConnect Local Auth] チェックボックスをオンまたはオフにして、WLAN のローカル認証を有効または無効にします。
 - [Learn Client IP Address] チェックボックスをオンまたはオフにして、クライアントの IP アドレスの学習を有効または無効にします。
 - [VLAN based Central Switching] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上での AAA Override VLAN に基づく中央スイッチングを有効または無効にします。

(注) これらは、この機能の注意事項および制限事項です。

- オーバーライドされたインターフェイス上でのマルチキャストはサポートされていません。
 - この機能は、WLAN がローカルでスイッチされる WLAN 単位でのみ使用できません。
 - IPv6 ACL、CAC、NAC、および IPv6 はサポートされていません。
 - IPv4 ACL は、VLAN に基づく中央スイッチング有効な場合にのみサポートされ、無線 LAN 上の中央スイッチングのクライアントにのみ適用できます。
 - この機能は、ローカルでスイッチされる WLAN の FlexConnect モードの AP に適用できます。
 - この機能は、ローカル モードの AP には適用できません。
 - この機能は、中央でスイッチされる WLAN の FlexConnect モードの AP ではサポートされません。
 - この機能は、中央認証だけでサポートされます。
 - この機能は、Web 認証セキュリティクライアント上ではサポートされません。
 - ローカル スイッチング クライアントのレイヤ 3 ローミングはサポートされません。
- [Central DHCP Processing] チェックボックスをオンまたはオフにして、機能を有効または無効にします。この機能を有効にすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。
 - [Override DNS] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN に割り当てられたインターフェイス上での DNS サーバアドレスのオーバーライドを有効または無効にします。中央でスイッチされる WLAN 上で DNS をオーバーライドすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
 - [NAT-PAT] チェックボックスをオンまたはオフにして、ローカルでスイッチされる WLAN 上でのネットワーク アドレス変換 (NAT) およびポートアドレス変換 (PAT) を有効または無効にします。NAT および PAT を有効にするには、[Central DHCP Processing] を有効にする必要があります。
 - [Central Assoc] チェックボックスをオンまたはオフにして、Cisco WLC のクライアント再アソシエーションとセキュリティ キー キャッシュを有効または無効にします。AP 機能の PMIPv6 MAG では、高速ローミングをサポートするために、AP が大規模に展開されている Cisco WLC でクライアント再アソシエーションが中央で処理される必要があります。
- ローカル認証での中央アソシエーションの設定は、WLAN でサポートされません。PMIPv6 トンネルのセットアップ後、PMIPv6 クライアントからのすべてのデータトラフィックは、総称ルーティングカプセル化 (GRE) トンネルでローカルモビリティアンカー (LMA) に転送されます。AP と Cisco WLC の間の接続が失われた場合、既存の PMIPv6 クライアントのデータトラフィック

クは AP とクライアントの間の接続が失われるまで引き続き送受信されます。この状態では、新しいクライアントアソシエーションが受け入れられず、AP は WLAN へのビーコンまたはプローブ応答を送信しません。

ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

FlexConnect に対するコントローラの設定 (CLI)

- **config wlan flexconnect local-switching wlan_id enable** : ローカル スイッチングを行うように WLAN を設定します。



(注) FlexConnect ローカル スイッチングが有効のときは、デフォルトではコントローラはクライアント IP アドレスを認識できるまで待機します。ただし、クライアントが Fortress レイヤ 2 暗号化を使用するように設定されている場合は、コントローラがそのクライアント IP アドレスを知ることができないので、コントローラはクライアントの接続を定期的に切断します。コントローラがクライアントの IP アドレスを認識できるまで待たなくてもクライアント接続を維持できるように、**config wlan flexconnect learn-ipaddr wlan_id disable** コマンドを使用して、クライアント IP アドレス認識機能を無効にします。この機能を無効にできるのは、FlexConnect ローカル スイッチングを行うように設定されているときだけです。FlexConnect 中央スイッチングを行う場合は、無効にすることはできません。この機能を有効にするには、**config wlan flexconnect learn-ipaddr wlan_id enable** コマンドを入力します。



(注) WLAN がローカルにスイッチされる場合 (LS)、**config wlan flexconnect learn-ipaddr wlan-id {enable | disable}** コマンドを使用する必要があります。WLAN が中央でスイッチされる場合 (CS)、**config wlan learn-ipaddr-cswlan wlan-id {enable | disable}** コマンドを使用する必要があります。

- **config wlan flexconnect local-switching wlan_id {enable | disable}** : 中央スイッチングを行うように WLAN を設定します。
- **config wlan flexconnect vlan-central-switching wlan_id {enable | disable}** : ローカルでスイッチされる WLAN 上での AAA Override VLAN に基づく中央スイッチングを設定します。次に、この機能に関するガイドラインおよび制限事項を示します。
 - オーバーライドされたインターフェイス上でのマルチキャストはサポートされていません。

- この機能は、WLAN がローカルでスイッチされる WLAN 単位でのみ使用できます。
- IPv6 ACL、CAC、NAC、および IPv6 はサポートされていません。
- IPv4 ACL は、VLAN に基づく中央スイッチング有効な場合にのみサポートされ、無線 LAN 上の中央スイッチングのクライアントにのみ適用できます。
- この機能は、ローカルでスイッチされる WLAN の FlexConnect モードの AP に適用できます。
- この機能は、ローカル モードの AP には適用できません。
- この機能は、中央でスイッチされる WLAN の FlexConnect モードの AP ではサポートされません。
- この機能は、中央認証だけでサポートされます。
- この機能は、Web 認証セキュリティクライアント上ではサポートされません。
- ローカル スイッチング クライアントのレイヤ 3 ローミングはサポートされません。

- **config wlan flexconnect central-assoc wlan-id {enable | disable}** : Cisco WLC のクライアント再アソシエーションとセキュリティ キー キャッシュを設定します。AP 機能の PMIPv6 MAG では、高速ローミングをサポートするために、AP が大規模に展開されている Cisco WLC でクライアント再アソシエーションが中央で処理される必要があります。

デフォルトでは、Cisco WLC のクライアント再アソシエーションとセキュリティキーキャッシュは無効の状態です。

ローカル認証での中央アソシエーションの設定は、WLAN でサポートされません。PMIPv6 トンネルのセットアップ後、PMIPv6 クライアントからのすべてのデータトラフィックは、総称ルーティングカプセル化 (GRE) トンネルでローカルモビリティアンカー (LMA) に転送されます。AP と Cisco WLC の間の接続が失われた場合、既存の PMIPv6 クライアントのデータトラフィックは AP とクライアントの間の接続が失われるまで引き続き送受信されます。この状態では、新しいクライアントアソシエーションが受け入れられず、AP は WLAN へのビーコンまたはプローブ応答を送信しません。

FlexConnect の情報を取得するには、次のコマンドを使用します。

- **show ap config general Cisco_AP** : VLAN 設定を表示します。
- **show wlan wlan_id** : WLAN がローカルと中央のどちらでスイッチされるかを表示します。
- **show client detail client_mac** : クライアントがローカルと中央のどちらでスイッチされるかを表示します。

次のコマンドを使用して、デバッグ情報を取得します。

- **debug flexconnect aaa {event | error} {enable | disable}** : FlexConnect のバックアップ RADIUS サーバのイベントまたはエラーのデバッグを有効または無効にします。
- **debug flexconnect cckm {enable | disable}** : グループのデバッグを有効または無効にします。

- **debug flexconnect {enable | disable}**— : FlexConnect グループのデバッグを有効または無効にします。
- **debug pem state {enable | disable}** : Policy Manager ステート マシンのデバッグを有効または無効にします。
- **debug pem events {enable | disable}** : Policy Manager イベントのデバッグを有効または無効にします。

FlexConnect のアクセス ポイントの設定

FlexConnect のアクセス ポイントの設定 (GUI)

アクセス ポイントが物理的にネットワークに追加されていることを確認します。

-
- ステップ 1** [Wireless] を選択して、[All APs] ページを開きます。
- ステップ 2** 目的のアクセス ポイントの名前をクリックします。 [All APs > Details] ページが表示されます。
- ステップ 3** [AP Mode] ドロップダウンリストから [FlexConnect] を選択して、このアクセス ポイントの FlexConnect を有効にします。
- (注) [Inventory] タブの最後のパラメータは、そのアクセス ポイントを FlexConnect に対して設定できるかどうかを示します。
- ステップ 4** [Apply] をクリックして変更を適用し、アクセス ポイントをリポートします。
- ステップ 5** [FlexConnect] タブを選択して、[All APs > Details for] (FlexConnect) ページを開きます。アクセス ポイントが FlexConnect グループに属する場合、グループの名前は [FlexConnect Name] テキストボックスに表示されます。
- ステップ 6** WLAN VLAN マッピングを設定するには、ドロップダウン リストから次のオプションを選択します。
- Make AP Specific
 - Remove AP Specific
- ステップ 7** [VLAN Support] チェックボックスをオンにし、[Native VLAN ID] テキストボックスにリモートネットワーク上のネイティブ VLAN の番号 (100 など) を入力します。
- (注) デフォルトで、VLAN は FlexConnect アクセス ポイント上では有効化されていません。 FlexConnect を有効にすると、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。この設定はアクセス ポイントで保存され、join response が成功した後に受信されます。デフォルトでは、ネイティブ VLAN は 1 です。VLAN が有効化されているドメインの FlexConnect アクセス ポイントごとに、ネイティブ VLAN を 1 つ設定する必要があります。そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。

(注) アップグレードまたはダウングレード後、アクセスポイントに VLAN マッピングを保持するには、アクセスポイントの join は準備されたコントローラに制限されている必要があります。つまり、他の方法で使用可能であるはずの、異なる設定の他のコントローラは見つからないということです。同様に、アクセスポイントが join する時点で、異なる VLAN マッピングが設定されているコントローラを通過する場合、アクセスポイントでの VLAN マッピングが一致しない場合があります。

ステップ 8 [Apply] をクリックします。イーサネットポートがリセットされる間、アクセスポイントは一時的にコントローラへの接続を失います。

ステップ 9 同じアクセスポイントの名前をクリックしてから、[FlexConnect] タブをクリックします。

ステップ 10 [VLAN Mappings] をクリックして [All APs > アクセスポイント名 > VLAN Mappings] ページを開きます。

ステップ 11 ローカルスイッチングが行われるときにクライアントの IP アドレス取得元となる VLAN の番号（この例では VLAN 101）を [VLAN ID] テキストボックスに入力します。

ステップ 12 Web 認証 ACL を設定するには、次の手順を実行します。

a) [External WebAuthentication ACLs] リンクをクリックして、[ACL mappings] ページを開きます。[ACL Mappings] ページには、WLAN ACL マッピングおよび Web ポリシー ACL の詳細が一覧表示されます。

b) [WLAN Id] ボックスに、WLAN ID を入力します。

c) [WebAuth ACL] ドロップダウンリストから、FlexConnect ACL を選択します。

(注) FlexConnect ACL を作成するには、[FlexConnect Groups] > [FlexConnect ACLs] を選択し、[New] をクリックし、FlexConnect ACL 名を入力し、[Apply] をクリックします。

d) [Add] をクリックします。

e) [Apply] をクリックします。

ステップ 13 ローカルスプリット ACL を設定するには、次の手順を実行します。

a) [Local Split ACLs] リンクをクリックして、[ACL Mappings] ページを開きます。

b) [WLAN Id] ボックスに、WLAN ID を入力します。

c) [Local-Split ACL] ドロップダウンリストから、FlexConnect ACL を選択します。

(注) FlexConnect ACL を作成するには、[FlexConnect Groups] > [FlexConnect ACLs] を選択し、[New] をクリックし、FlexConnect ACL 名を入力し、[Apply] をクリックします。

中央でスイッチされる WLAN に関連付けられた WAN リンクに接続するクライアントが、ローカルサイトに存在するデバイスに一部のトラフィックを送信する必要がある場合、クライアントは、CAPWAP 経由でトラフィックをコントローラに送信し、CAPWAP 経由または帯域外の接続を使用して、ローカルサイトに同じトラフィックを戻す必要があります。このプロセスは不必要に WAN リンク帯域幅を消費します。この問題を回避するには、パケットの内容に基づいたクライアントによる送信トラフィックの分類を可能にする、スプリットトンネリング機能を使用できます。一致するパケットはローカルでスイッチされ、残りのトラフィックは中央でスイッチされます。ローカルサイトに存在するデバイスの IP アドレスと一致するクライアントによって送信されるトラフィックを、ローカルでスイッチされるトラフィックとして分類し、残りのトラフィックを中央でスイッチされるトラフィックとして分類できます。

AP 上でのローカルスプリットトンネリングを設定するには、WLAN 上で必要な DHCP が有効になっていることを確認します。これにより、スプリット WLAN に関連付けられるクライアントが DHCP を実行することが確保されます。

(注) ローカル スプリット トンネリングは、Cisco 1500 シリーズ、Cisco 1130、Cisco 1240 アクセス ポイントではサポートされないため、固定 IP アドレスを持つクライアントに対して機能しません。

d) [Add] をクリックします。

ステップ 14 中央での DHCP 処理を設定するには、次の手順を実行します。

a) [WLAN Id] ボックスに、中央 DHCP をマッピングする WLAN ID を入力します。

b) [Central DHCP] チェックボックスをオンまたはオフにして、マッピングに対する中央 DHCP を有効または無効にします。

c) [Override DNS] チェックボックスをオンまたはオフにして、マッピングに対する DNS のオーバーライドを有効または無効にします。

d) [NAT-PAT] チェックボックスをオンまたはオフにして、マッピングに対するネットワーク アドレス変換およびポートアドレス変換を有効または無効にします。

e) [Add] をクリックして、中央 DHCP と WLAN のマッピングを追加します。

ステップ 15 ローカルでスイッチされる WLAN を WebAuth ACL にマッピングするには、次の手順を実行します。

a) [WLAN Id] ボックスに、WLAN ID を入力します。

b) [WebAuth ACL] ドロップダウンリストから、FlexConnect ACL を選択します。

(注) FlexConnect ACL を作成するには、[FlexConnect Groups] > [FlexConnect ACLs] を選択し、[New] をクリックし、FlexConnect ACL 名を入力し、[Apply] をクリックします。

c) [Add] をクリックします。

(注) AP に固有の FlexConnect ACL のプライオリティは、最も高くなります。WLAN に固有の FlexConnect ACL のプライオリティは、最も低くなります。

ステップ 16 [WebPolicy ACL] ドロップダウンリストから FlexConnect ACL を選択し、[Add] をクリックして、FlexConnect ACL を Web ポリシーとして設定します。

(注) アクセス ポイントに固有の最大 16 の Web ポリシー ACL を設定できます。

ステップ 17 [Apply] をクリックします。

ステップ 18 [Save Configuration] をクリックします。

(注) リモート サイトで、FlexConnect に対して設定が必要なその他すべてのアクセス ポイントについて、この手順を繰り返します。

FlexConnect のアクセス ポイントの設定 (CLI)

- **config ap mode flexconnect Cisco_AP** : このアクセス ポイントに対して FlexConnect を有効にします。
- **config ap flexconnect radius auth set {primary | secondary} ip_address auth_port secret Cisco_AP** : 特定の FlexConnect アクセス ポイントに対してプライマリまたはセカンダリの RADIUS サーバを設定します。



(注) スタンドアロン モードでは、Session Timeout RADIUS 属性のみがサポートされています。その他のすべての属性や RADIUS アカウンティングはサポートされていません。



(注) FlexConnect アクセスポイントに対して設定されている RADIUS サーバを削除するには、**config ap flexconnect radius auth delete {primary | secondary} Cisco_AP** コマンドを入力します。

- **config ap flexconnect vlan wlan wlan_id vlan-id Cisco_AP** : VLAN ID をこの FlexConnect アクセスポイントに割り当てることができます。デフォルトでは、アクセスポイントは WLAN にアソシエートされている VLAN ID を継承します。
- **config ap flexconnect vlan {enable | disable} Cisco_AP** : この FlexConnect アクセスポイントに対して VLAN タギングを有効化または無効化します。デフォルトでは、VLAN タギングは無効化されていません。VLAN タギングが FlexConnect アクセスポイント上で有効化されると、ローカルスイッチングを行うように設定された WLAN は、コントローラで割り当てられた VLAN を継承します。
- **config ap flexconnect vlan native vlan-id Cisco_AP** : この FlexConnect アクセスポイントに対するネイティブ VLAN を設定できます。デフォルトでは、ネイティブ VLAN として設定されている VLAN はありません。(VLAN タギングが有効化されているとき) FlexConnect アクセスポイントごとにネイティブ VLAN を 1 つ設定する必要があります。アクセスポイントが接続されているスイッチポートに、対応するネイティブ VLAN も設定されていることを確認します。FlexConnect アクセスポイントのネイティブ VLAN 設定と、アップストリームスイッチポートのネイティブ VLAN が一致しない場合は、アクセスポイントとコントローラとの間でパケットを送受信することはできません。



(注) アップグレードまたはダウングレード後、アクセスポイントに VLAN マッピングを保存するには、アクセスポイントの join を準備されたコントローラに制限する必要があります。他の方法で使用可能であるはずの、異なる設定の他のコントローラは見つかりません。同様に、アクセスポイントが join する時点で、異なる VLAN マッピングが設定されているコントローラを通過する場合、アクセスポイントでの VLAN マッピングが一致しない場合があります。

- 次のコマンドを入力して、FlexConnect モードのアクセスポイントの WLAN に Web 認証または Web パススルー ACL のマッピングを設定します。

config ap flexconnect web-auth wlan wlan_id cisco_ap acl_name {enable | disable}



(注) APに固有のFlexConnect ACLのプライオリティは、最も高くなります。WLANに固有のFlexConnect ACLのプライオリティは、最も低くなります。

- 次のコマンドを入力して、FlexConnect モードの AP 上で ポリシー ACL を設定します。
config ap flexconnect policy acl {add | delete} acl_name cisco_ap



(注) アクセス ポイントに固有の最大 16 の ポリシー ACL を設定できます。

- AP ごとにローカル スプリット トンネリングを設定するには、次のコマンドを入力します。
config ap local-split {enable | disable} wlan-id acl acl-name ap-name
- 次のコマンドを入力して、WLAN ごとに AP 上で中央 DHCP を設定します。
config ap flexconnect central-dhcp wlan-id ap-name {enable override dns | disable | delete}



(注) ゲートウェイの Gratuitous ARP はアクセス ポイントによってクライアントに送信され、これにより、中央サイトから IP アドレスを取得します。これは、アクセス ポイントによってゲートウェイにプロキシ設定を行うために実行されます。

FlexConnect アクセス ポイントで次のコマンドを使用して、ステータス情報を取得します。

- **show lwapp reap status** : FlexConnect アクセス ポイントのステータス (connected または standalone) を表示します。
- **show capwap reap association** : このアクセス ポイントにアソシエートされているクライアントのリストと各クライアントの SSID を表示します。

FlexConnect アクセス ポイントで次のコマンドを使用して、デバッグ情報を取得します。

- **debug capwap reap** : 一般的な FlexConnect アクティビティを表示します。
- **debug capwap reap mgmt** : クライアント認証とアソシエーションのメッセージを表示します。
- **debug capwap reap load** : FlexConnect アクセス ポイントがスタンドアロン モードでブートされるときに役立つ、ペイロード アクティビティを表示します。
- **debug dot11 mgmt interface** : 802.11 管理インターフェイス イベントを表示します。
- **debug dot11 mgmt msg** : 802.11 管理メッセージを表示します。
- **debug dot11 mgmt ssid** : SSID 管理イベントを示します。
- **debug dot11 mgmt state-machine** : 802.11 ステート マシンを表示します。

- `debug dot11 mgmt station` : クライアント イベントを表示します。

WLAN 上のローカル認証用のアクセス ポイントの設定 (GUI)

-
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 WLAN の ID をクリックします。[WLANs > Edit] ページが表示されます。
- ステップ 3 [Advanced] タブをクリックして、[WLANs > Edit (WLAN Name)] ページを開きます。
- ステップ 4 [FlexConnect Local Switching] チェックボックスをオンにして、FlexConnect ローカル スイッチングを有効にします。
- ステップ 5 [FlexConnect Local Auth] チェックボックスをオンにして、FlexConnect ローカル認証を有効にします。
 注意 2500 シリーズ コントローラに FlexConnect モードのアクセス ポイントを直接接続しないでください。
- ステップ 6 [Apply] をクリックして、変更を確定します。
-

WLAN 上のローカル認証用のアクセス ポイントの設定 (CLI)

はじめる前に

開始する前に、アクセス ポイントについてローカル認証を有効にしたい WLAN で、有効なローカル スイッチングがある必要があります。WLAN 上のローカル スイッチングを有効にする手順については、「[FlexConnect に対するコントローラの設定 \(CLI\)](#)」の項を参照してください。

- `config wlan flexconnect ap-auth wlan_id {enable | disable}` : WLAN 上でローカル認証を有効または無効にするようにアクセス ポイントを設定します。



注意 FlexConnect モードのアクセス ポイントを直接 Cisco 2500 シリーズ コントローラに接続しないでください。

- `show wlan wlan-id` : WLAN の設定を表示します。ローカル認証が有効になっている場合は、次の情報が表示されます。

```

: : :
: : :
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
Auto Anchor..... Disabled
FlexConnect Local Switching..... Enabled
FlexConnect Local Authentication..... Enabled
FlexConnect Learn IP Address..... Enabled
Client MFP..... Optional
Tkip MIC Countermeasure Hold-down Timer..... 60
Call Snooping..... Disabled
Roamed Call Re-Anchor Policy..... Disabled

```

...

クライアント デバイスの WLAN への接続

FlexConnect に対するコントローラの設定で作成した WLAN にクライアント デバイスを接続するためのプロファイルを作成するには、次の手順に従ってください。

シナリオ例 (表 28 : WLAN の例を参照) では、クライアントに 3 つのプロファイルがあります。

- 1 「employee」 WLAN に接続するには、WPA/WPA2 と PEAP-MSCHAPV2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、クライアントはコントローラの管理 VLAN から IP アドレスを取得します。
- 2 「local-employee」 WLAN に接続するには、WPA/WPA2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、クライアントはローカルスイッチの VLAN 101 から IP アドレスを取得します。
- 3 「guest-central」 WLAN に接続するには、オープン認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、クライアントはアクセスポイントへのネットワーク ローカル上の VLAN 101 から IP アドレスを取得します。クライアントが接続すると、ローカルユーザは、Web ブラウザに任意の HTTP アドレスを入力できます。ユーザは、Web 認証プロセスを完了するために、自動的にコントローラへダイレクトされます。Web ログインページが表示されると、ユーザはユーザ名とパスワードを入力します。

クライアントのデータトラフィックがローカルと中央のどちらでスイッチングされているかを調べるには、コントローラの GUI で [Monitor] > [Clients] を選択し、目的のクライアントの [Detail] リンクをクリックして、[AP Properties] の下の [Data Switching] パラメータを確認します。

FlexConnect イーサネット フォールバックの設定

FlexConnect イーサネット フォールバックについて

イーサネットリンクが機能しないときに無線をシャットダウンするように AP を設定できます。イーサネットリンクが使用可能状態に戻った場合、無線を使用可能状態に戻すように AP を設定できます。この機能は、接続されている AP に依存しない、またはスタンドアロンモードです。無線がシャットダウンすると、AP は WLAN をブロードキャストしないため、クライアントは最初のアソシエーションおよびローミングで AP に接続することができません。

イーサネットインターフェイスのフラッピングから無線への影響を防ぐために、設定可能な遅延タイマーが用意されています。

FlexConnect イーサネット フォールバックの制約事項

- FlexConnect イーサネット フォールバックの設定はグローバル レベルで、すべて FlexConnect AP に適用できます。ただし、この機能は Cisco AP1130、AP1240、および AP1150 には適用されません。
- FlexConnect イーサネット フォールバック機能は、Cisco AP1520、AP1550 などの複数のポートが使用されている AP には適用されません。
- イーサネット インターフェイスで設定するキャリア遅延は、ヒステリシスに基づいてインターフェイスをシャットダウンおよびリロードします。したがって、設定する遅延が、イーサネットおよび 802.11 インターフェイスがシャットダウンおよびリロードされる前の実際の遅延とは異なる場合があります。

FlexConnect イーサネット フォールバックの設定 (GUI)

-
- ステップ 1** [Wireless] > [Access Points] > [Global Configuration] を選択します。
[Global Configuration] ページが表示されます。
- ステップ 2** [FlexConnect Ethernet Fallback] 領域で、[Radio Interface Shutdown] チェックボックスをオンまたはオフにします。
- ステップ 3** [Radio Interface Shutdown] チェックボックスをオンにした場合は、AP 無線インターフェイスがシャットダウンするまでの遅延またはイーサネット インターフェイス ダウンタイムを秒単位で入力します。デフォルトの遅延は 0 秒です。
(注) [Radio Interface Shutdown] チェックボックスをオンにした場合にのみ遅延を入力できます。
- ステップ 4** [FlexConnect Ethernet Fallback] 領域で、[FlexConnect Arp-Cache] チェックボックスを選択して、FlexConnect AP のローカルにスイッチされる WLAN でプロキシ ARP を追加します。
- ステップ 5** [Apply] をクリックします。
- ステップ 6** [Save Configuration] をクリックします。
-

FlexConnect イーサネット フォールバックの設定 (CLI)

-
- ステップ 1** 次のコマンドを入力して、無線インターフェイスを設定します。
config flexconnect fallback-radio-shut {disable | enable delay *time-in-seconds*}
- ステップ 2** 次のコマンドを入力して、FlexConnect イーサネット フォールバック機能設定のステータスを確認します。
show flexconnect summary
-



FlexConnect ACL の設定

- [アクセス コントロール リストについて](#), 1123 ページ
- [FlexConnect ACL の制限](#), 1124 ページ
- [FlexConnect ACL の設定 \(GUI\)](#), 1125 ページ
- [FlexConnect ACL の設定 \(CLI\)](#), 1127 ページ
- [FlexConnect ACL の表示およびデバッグ \(CLI\)](#), 1128 ページ

アクセス コントロール リストについて

アクセスコントロールリスト (ACL) は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです (たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます)。ACL を使用すると、ネットワーク トラフィックのアクセス制御を行えます。コントローラで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、または WLAN に適用できます。ACL を使用すると、ワイヤレスクライアントで送受信されるデータ トラフィックやコントローラの CPU へのデータ トラフィックを制御できます。FlexConnect アクセス ポイント上で ACL を設定して、ローカルにスイッチされるアクセス ポイント上のデータ トラフィックの効率的な使用およびアクセス制御を実現できます。

FlexConnect ACL は、入力と出力の両方のモードのアクセス ポイントで VLAN インターフェイスに適用できます。

アクセス ポイントの既存のインターフェイスを ACL にマッピングできます。インターフェイスは、FlexConnect アクセス ポイントで WLAN-VLAN マッピングを設定することによって作成できます。

FlexConnect ACL は、VLAN サポートが FlexConnect アクセス ポイントで有効になっている場合のみ、アクセス ポイントの VLAN に適用できます。

FlexConnect ACL の制限

- FlexConnect ACL は FlexConnect のアクセス ポイントにのみ適用できます。設定は、AP および VLAN ごとに適用されます。
- コントローラ上に最大 512 の ACL を設定できます。
- コントローラに設定されている非 FlexConnect ACL は FlexConnect AP には適用できません。
- FlexConnect ACL では、ルールごとの方向はサポートされていません。通常の ACL とは異なり、Flexconnect ACL では方向を持たせて設定することはできません。ACL 全体を入力または出力としてインターフェイスに適用する必要があります。
- 最大で 512 の FlexConnect ACL を定義することができ、各 ACL に最大 64 のルール（またはフィルタ）を設定できます。各ルールには、ルールの処理に影響を与えるパラメータがあります。パケットがルールに関連するすべてのパラメータに一致すると、そのルールに関連するアクション設定がパケットに適用されます。
- ネットワークの ACL は、Control and Provisioning of Wireless Access Points (CAPWAP) が Lightweight Access Point Protocol (LWAPP) で使用されているものとは異なるポートを使用するため、変更を必要とする場合があります。
- すべての ACL で、最後のルールとして暗黙の *deny all* ルールが適用されます。パケットがどのルールとも一致しない場合、対応するアクセス ポイントによってドロップされます。
- WLAN-VLAN マッピングを使用して AP で作成された VLAN の ACL マッピングは、AP ベースごとでのみ実行する必要があります。VLAN は AAA Override の FlexConnect グループで作成できます。これらの VLAN に WLAN のマッピングはありません。
- FlexConnect グループで作成された VLAN の ACL は、FlexConnect グループのみでマッピングする必要があります。同じ VLAN が、対応する AP および FlexConnect グループにある場合、AP VLAN が優先されます。つまり、ACL が AP にマッピングされていない場合、FlexConnect グループの VLAN にマッピングされていても VLAN には ACL がないということです。
- AAA クライアントの ACL のサポート
 - AAA がクライアント ACL を送信する前に、ACL が FlexConnect グループまたは AP で作成されることを確認してください。ACL は、クライアントが AP に関連付けられるときに AP に動的にダウンロードされることはありません。
 - 最大 96 の ACL を AP で設定できます。各 ACL には最大 64 のルールを設定できます。
 - FlexConnect ACL には方向がありません。ACL 全体が入力または出力として適用されます。
 - AAA によって返される ACL は、クライアントの 802.11 側の入力と出力の両方に適用されます。

FlexConnect ACL の設定 (GUI)

ステップ 1 [Security] > [Access Control Lists] > [FlexConnect Access Control Lists] を選択します。
[FlexConnect ACL] ページが表示されます。

このページには、コントローラ上で設定したすべての FlexConnect ACL が一覧表示されます。このページには、対応するコントローラで作成した FlexConnect ACL も表示されます。ACL を削除するには、該当する ACL 名の横にある青のドロップダウン矢印の上にカーソルを移動し、[Remove] を選択します。

ステップ 2 [New] をクリックして、新しい ACL を追加します。
[Access Control Lists > New] ページが表示されます。

ステップ 3 [Access Control List Name] テキストボックスに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。
[Access Control Lists > Edit] ページが表示されたら、[Add New Rule] をクリックします。
[Access Control Lists > Rules > New] ページが表示されます。

ステップ 6 この ACL のルールを次のように設定します。

a) コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] テキストボックスで、値 (1 ~ 64) を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

(注) ルール 1 ~ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が自動的に調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b) [Source] ドロップダウンリストから次のオプションのいずれかを選択して、この ACL を適用するパケットの送信元を指定します。

- [Any] : 任意の送信元 (これはデフォルト値です)。
- [IP Address] : 特定の送信元。このオプションを選択する場合は、該当するテキストボックスに送信元の IP アドレスとネットマスクを入力します。

c) [Destination] ドロップダウンリストから次のオプションのいずれかを選択して、この ACL を適用するパケットの宛先を指定します。

- [Any] : 任意の宛先 (これはデフォルト値です)。
- [IP Address] : 特定の宛先。このオプションを選択する場合は、テキストボックスに宛先の IP アドレスとネットマスクを入力します。

d) [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。使用できるプロトコル オプションは、次のとおりです。

- [Any] : 任意のプロトコル (これは、デフォルト値です)。
- TCP
- UDP
- [ICMP] : インターネット制御メッセージプロトコル
- [ESP] : IP カプセル化セキュリティ ペイロード
- [AH] : 認証ヘッダー
- [GRE] : Generic Routing Encapsulation
- [IP-in-IP] : IP-in-IP パケットを許可または拒否します
- [Eth Over IP] : Ethernet-over-Internet プロトコル
- [OSPF] : Open Shortest Path First
- [Other] : その他の Internet Assigned Numbers Authority (IANA) プロトコル

(注) [Other] を選択する場合は、[Protocol] テキスト ボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルのリストは IANA Web サイトで確認できます。

コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット (アドレス解決プロトコル (ARP) パケットなど) は指定できません。

[TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つの追加のパラメータが表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポートオプションは、ネットワークスタックとのデータ送受信をするアプリケーションによって使用されます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。

e) [DSCP] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point (DSCP) 値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダーテキストボックスです。

- [Any] : 任意の DSCP (これは、デフォルト値です)
- [Specific] : [DSCP] テキスト ボックスに入力する、0 ~ 63 の特定の DSCP

f) [Action] ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。

g) [Apply] をクリックします。

[Access Control Lists > Edit] ページが表示され、この ACL のルールが示されます。

h) この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 7 [Save Configuration] をクリックします。

FlexConnect ACL の設定 (CLI)

- **config flexconnect acl create name** : FlexConnect アクセス ポイントの ACL を作成します。 name は、最大 32 文字の IPv4 ACL 名にする必要があります。
- **config flexconnect acl delete name** : FlexConnect ACL を削除します。
- **config flexconnect acl rule action acl-name rule-index {permit |deny}** : ACL を許可または拒否します。
- **config flexconnect acl rule add acl-name rule-index** : ACL ルールを追加します。
- **config flexconnect acl rule change index acl-name old-index new-index** : ACL ルールのインデックス値を変更します。
- **config flexconnect acl rule delete name** : ACL ルールを削除します。
- **config flexconnect acl rule dscp acl-name rule-index {0-63 | any}** : ルール インデックスの DiffServ コード ポイント (DSCP) 値を指定します。 DSCP は、インターネット上のサービスの質を定義するのに使用できる IP ヘッダーです。 0 ~ 63 の値または値 **any** を入力します。 デフォルト値は **any** です。
- **config flexconnect acl rule protocol acl-name rule-index {0-255 | any}** : ルール インデックスを ACL ルールに割り当てます。 0 ~ 255 の値または「any」を指定します。 デフォルトは「any」です。
- **config flexconnect acl rule destination address acl-name rule-index ipv4-addr subnet-mask** : ルールの宛先 IP アドレス、ネットマスク、およびポート範囲を設定します。
- **config flexconnect acl rule destination port range acl-name rule-index start-port end-port** : ルールの宛先ポート範囲を設定します。
- **config flexconnect acl rule source address acl-name rule-index ipv4-addr subnet-mask** : ルールの送信元 IP アドレスおよびネットマスクを設定します。
- **config flexconnect acl apply acl-name** : FlexConnect アクセス ポイントに ACL を適用します。
- **config flexconnect acl rule swap acl-name index-1 index-2** : 2 つのルールのインデックス値を入れ替えます。
- **config ap flexconnect vlan add acl vlan-id ingress-aclname egress-acl-name ap-name** : FlexConnect アクセス ポイントに VLAN を追加します。
- **config flexconnect acl rule source port range acl-name rule-index start-port end-port** : ルールの送信元ポート範囲を設定します。

FlexConnect ACL の表示およびデバッグ (CLI)

- **show flexconnect acl summary** : ACL の要約を表示します。
- **show client detail <mac-address>** : [FlexConnect ACL Applied Status] および [IPv4 ACL Applied Status] を表示します。 IPv4 ACL 名フィールドに、ローカル/中央スイッチングに基づいてクライアントに適用される ACL が表示されます。
- **show flexconnect acl detailed acl-name** : ACL の詳細情報を表示します。
- **debug flexconnect acl {enable | disable}** : FlexConnect ACL のデバッグを有効または無効にします。
- **debug capwap reap** : CAPWAP のデバッグを有効にします。



第 149 章

FlexConnect グループの設定

- [FlexConnect グループについて, 1129 ページ](#)
- [FlexConnect グループの設定, 1133 ページ](#)
- [FlexConnect グループの VLAN-ACL マッピングの設定, 1138 ページ](#)
- [FlexConnect グループの WLAN-VLAN マッピングの設定, 1139 ページ](#)

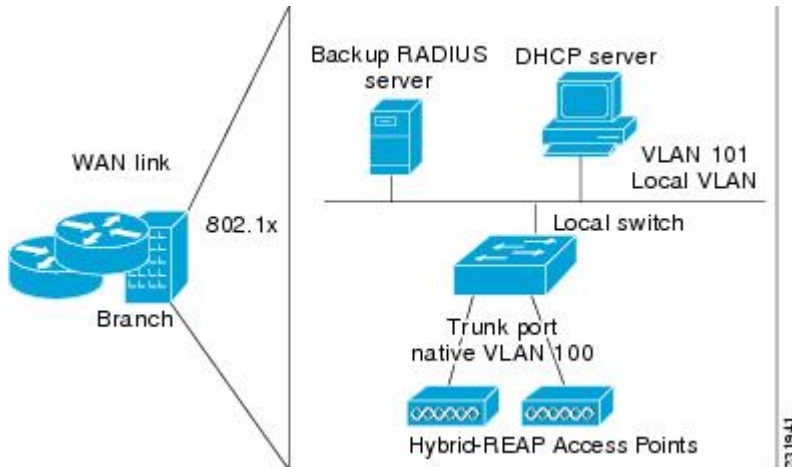
FlexConnect グループについて

お使いの FlexConnect アクセス ポイントをまとめて管理するために、FlexConnect グループを作成して、特定のアクセス ポイントをそれらのグループに割り当てることができます。

グループ内のすべての FlexConnect アクセス ポイントは、同じバックアップ RADIUS サーバ、CCKM、およびローカル認証の設定情報を共有します。この機能は、リモートオフィス内や建物のフロア上に複数の FlexConnect アクセス ポイントがあり、それらすべてを一度に設定する場合に役立ちます。たとえば、FlexConnect に対してバックアップ RADIUS サーバを 1 つ設定しておけば、個々のアクセス ポイント上で同じサーバを設定する必要はありません。

次の図は、ブランチ オフィスでのバックアップ RADIUS サーバを使用した FlexConnect の一般的な導入です。

図 72 : FlexConnect グループの導入



FlexConnect グループおよびバックアップ RADIUS サーバ

スタンドアロンモードの FlexConnect アクセス ポイントがバックアップ RADIUS サーバに対して完全な 802.1X 認証を実行できるように、コントローラを設定することができます。プライマリバックアップ RADIUS サーバを設定することも、プライマリとセカンダリの両方のバックアップ RADIUS サーバを設定することもできます。FlexConnect アクセス ポイントが 2 つのモード、スタンドアロンまたは接続の場合に、これらのサーバを使用することができます。

FlexConnect グループおよび CCKM

FlexConnect グループは、FlexConnect アクセス ポイントと共に使用する CCKM 高速ローミングが必要となります。CCKM 高速ローミングは、ワイヤレス クライアントを別のアクセス ポイントにローミングする際に簡単かつ安全にキー交換できるように、完全な EAP 認証が実行されたマスターキーの派生キーをキャッシュすることにより実現します。この機能により、クライアントをあるアクセス ポイントから別のアクセス ポイントへローミングする際に、完全な RADIUS EAP 認証を実行する必要がなくなります。FlexConnect アクセス ポイントでは、アソシエートする可能性のあるすべてのクライアントに対する CCKM キャッシュ情報を取得する必要があります。それにより、CCKM キャッシュ情報をコントローラに送り返さずに、すばやく処理できます。たとえば、300 台のアクセス ポイントを持つコントローラと、アソシエートする可能性のある 100 台のクライアントがある場合、100 台すべてのクライアントに対して CCKM キャッシュを送信することは現実的ではありません。少数のアクセス ポイントから成る FlexConnect を作成すれば（たとえば、同じリモートオフィス内の 4 つのアクセス ポイントのグループを作成）、クライアントはその 4 つのアクセス ポイント間でのみローミングします。CCKM キャッシュがその 4 つのアクセス ポイント間で配布されるのは、クライアントがアクセス ポイントの 1 つにアソシエートするときだけとなります。



- (注) FlexConnect アクセス ポイントと FlexConnect 以外のアクセス ポイントとの間の CCKM 高速ローミングはサポートされていません。

FlexConnect グループおよび Opportunistic Key Caching

7.0.116.0 リリースから、FlexConnect グループによって、Opportunistic Key Caching (OKC) はクライアントの高速ローミングを可能にします。OKC は、同じ FlexConnect グループにあるアクセスポイントの PMK キャッシングを使用して高速ローミングを容易にします。

この機能により、クライアントをある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際に、完全な認証を実行する必要がなくなります。クライアントが 1 つの FlexConnect 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たびに、FlexConnect グループアクセスポイントはキャッシュされた PMK を使用して PMKID を計算します。

FlexConnect アクセスポイントで PMK キャッシュ エントリを参照するには、**show capwap reap pmk** コマンドを使用します。この機能は、Cisco FlexConnect アクセスポイントでサポートされています。



- (注) WPA2/802.1x 認証中に PMK が生成される場合、FlexConnect アクセスポイントは接続モードになっている必要があります。

OKC または CCKM に対して FlexConnect グループを使用する場合、PMK キャッシュは、同じ FlexConnect グループの一部で同じコントローラにアソシエートされているアクセスポイント間でのみ共有されます。アクセスポイントが同じ FlexConnect グループにあっても、同じモビリティグループの一部である別のコントローラにアソシエートされている場合、PMK キャッシュは更新されず、CCKM ローミングは失敗します。

FlexConnect グループおよびローカル認証

スタンドアロンモードの FlexConnect アクセスポイントが最大 100 人の静的に設定されたユーザに対して LEAP、EAP-FAST、PEAP、または EAP-TLS 認証を実行できるように、コントローラを設定できます。コントローラは、各 FlexConnect アクセスポイントがコントローラに join したときに、ユーザ名とパスワードの静的リストをその FlexConnect アクセスポイントに送信します。グループ内の各アクセスポイントは、そのアクセスポイントにアソシエートされたクライアントのみを認証します。

この機能が適しているのは、企業が自律アクセスポイントネットワークから Lightweight FlexConnect アクセスポイントネットワークに移行するときに、大きなユーザデータベースを保持したくない場合、または自律アクセスポイントの持つ RADIUS サーバ機能の代わりとなる別のハードウェアデバイスを追加したくない場合です。



(注) AP ローカル認証が有効な場合、LEAP、EAP-FAST、PEAP、または EAP-TLS 認証を設定できません。

AP がクライアントに証明書を送信しなければならないため、AP に証明書をプロビジョニングする必要があります。コントローラにベンダー デバイス証明書およびベンダー CA 証明書をダウンロードします。コントローラは AP にこれらの証明書を送ります。コントローラにベンダー デバイス証明書およびベンダー CA 証明書を設定しない場合、FlexConnect グループに関連する AP は、多くの無線クライアントが認識しない可能性のあるコントローラの自己署名証明書をダウンロードします。

EAP-TLS を使用すると、クライアントのルート CA が AP のルート CA と異なる場合、AP はクライアント証明書を認識および受理しません。企業の公開キー インフラストラクチャ (PKI) を使用する場合、コントローラが FlexConnect グループの AP に証明書を渡せるように、コントローラにベンダー デバイス証明書およびベンダー CA 証明書をダウンロードする必要があります。クライアントと AP の共通ルート CA を使用しないと、EAP-TLS はローカル AP で失敗します。AP は外部 CA を検査することができず、クライアントの証明書検証のために自身の CA チェーンを利用します。

ローカル証明書および CA 証明書のための AP のスペースは約 7 KB です。つまり短いチェーンのみが適応します。長いチェーンまたは複数のチェーンはサポートされません。



(注) この機能は、FlexConnect バックアップ RADIUS サーバ機能とともに使用できます。FlexConnect がバックアップ RADIUS サーバとローカル認証の両方で設定されている場合、FlexConnect アクセス ポイントは、まずプライマリ バックアップ RADIUS サーバの認証を試行します。その後、セカンダリ バックアップ RADIUS サーバを試行し (プライマリに接続できない場合)、最後に FlexConnect アクセス ポイント自身の認証を試行します (プライマリとセカンダリの両方に接続できない場合)。

FlexConnect グループの数およびアクセス ポイントのサポートは、使用しているプラットフォームによって異なります。次の設定を行えます。

- Cisco 5500 シリーズ コントローラに対して、グループごとに最大 100 の FlexConnect グループおよび最大 25 台のアクセス ポイント。
- 7.2 リリースの Cisco Flex 7500 シリーズ コントローラに対して、グループごとに最大 1000 の FlexConnect グループおよび最大 50 台のアクセス ポイント。
- 7.3 リリースの Cisco Flex 7500 および Cisco 8500 シリーズ コントローラに対して、グループごとに最大 2000 の FlexConnect グループおよび最大 100 台のアクセス ポイント。
- 残りのプラットフォームに対して、グループごとに最大 20 の FlexConnect グループおよび最大 25 台のアクセス ポイント。

FlexConnect グループの設定

FlexConnect グループの設定 (GUI)

- ステップ 1** [Wireless] > [FlexConnect Groups] を選択して、[FlexConnect Groups] ページを開きます。このページでは、これまでに作成されたすべての FlexConnect グループが表示されます。
- (注) 既存のグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて [Remove] を選択します。
- ステップ 2** [New] をクリックして、新しい FlexConnect グループを作成します。
- ステップ 3** [FlexConnect Groups > New] ページで、[Group Name] テキスト ボックスに新しいグループの名前を入力します。最大 32 文字の英数字を入力できます。
- ステップ 4** [Apply] をクリックします。新しいグループが [FlexConnect Groups] ページに表示されます。
- ステップ 5** グループのプロパティを編集するには、目的のグループの名前をクリックします。[FlexConnect Groups > Edit] ページが表示されます。
- ステップ 6** プライマリ RADIUS サーバをこのグループに対して設定する場合 (たとえば、アクセスポイントが 802.1X 認証を使用する場合) は、[Primary RADIUS Server] ドロップダウン リストから目的のサーバを選択します。それ以外の場合は、そのテキスト ボックスの設定をデフォルト値の [None] のままにします。
- ステップ 7** セカンダリ RADIUS サーバをこのグループに対して設定する場合は、[Secondary RADIUS Server] ドロップダウン リストからサーバを選択します。それ以外の場合は、そのフィールドの設定をデフォルト値の [None] のままにします。
- ステップ 8** 次の手順に従って、FlexConnect グループに RADIUS サーバを設定します。
- RADIUS サーバの IP アドレスを入力します。
 - プライマリまたはセカンダリとしてサーバタイプを選択します。
 - 共有の秘密を入力して、RADIUS サーバにログインし、確認用の入力を行います。
 - ポート番号を入力します。
 - [Add] をクリックします。
- ステップ 9** アクセス ポイントをグループに追加するには、[Add AP] をクリックします。追加のフィールドが、ページの [Add AP] の下に表示されます。
- ステップ 10** 次のいずれかの作業を実行します。
- このコントローラに接続されているアクセス ポイントを選択するには、[Select APs from Current Controller] チェックボックスをオンにして、[AP Name] ドロップダウン リストからアクセス ポイントの名前を選択します。
- (注) このコントローラ上のアクセス ポイントを選択すると、不一致が起らないように、アクセス ポイントの MAC アドレスが自動的に [Ethernet MAC] テキスト ボックスに入力されます。

- 別のコントローラに接続されているアクセスポイントを選択するには、[Select APs from Current Controller] チェックボックスをオフのままにして、そのアクセスポイントのMACアドレスを [Ethernet MAC] テキストボックスに入力します。

(注) 同じグループ内の FlexConnect アクセスポイントがそれぞれ別のコントローラに接続されている場合は、すべてのコントローラが同じモビリティグループに属している必要があります。

ステップ 11 [Add] をクリックして、アクセスポイントをこの FlexConnect グループに追加します。アクセスポイントの MAC アドレス、名前、およびステータスがページ下部に表示されます。

(注) アクセスポイントを削除するには、そのアクセスポイントの青いドロップダウンの矢印の上にカーソルを置いて [Remove] を選択します。

ステップ 12 [Apply] をクリックします。

ステップ 13 次のように、FlexConnect グループのローカル認証を有効にします。

- [Primary RADIUS Server] パラメータと [Secondary RADIUS Server] パラメータが [None] に設定されていることを確認します。
 - [Enable AP Local Authentication] チェックボックスをオンにして、この FlexConnect グループに対してローカル認証を有効にします。デフォルト値はオフです。
 - [Apply] をクリックします。
 - [Local Authentication] タブを選択して、[FlexConnect > Edit (Local Authentication > Local Users)] ページを開きます。
 - LEAP、EAP-FAST、PEAP、または EAP-TLS を使用して認証できるクライアントを追加するには、次のいずれかを実行します。
 - [Upload CSV File] チェックボックスをオンにして、カンマ区切り値 (CSV) ファイルをアップロードします。[Browse] ボタンをクリックすると、ユーザ名とパスワードを含む CSV ファイル (ファイルの各行は、username, password の形式になっている必要があります) を参照し、[Add] をクリックすると、CSV ファイルをアップロードします。クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。
 - クライアントを個別に追加するには、クライアントのユーザ名を [User Name] テキストボックスに入力し、クライアントのパスワードを [Password] テキストボックスと [Confirm Password] テキストボックスに入力します。[Add] をクリックすると、サポートされるローカルユーザのリストにこのクライアントが追加されます。クライアントの名前が、ページ左側の「User Name」という見出しの下に表示されます。
- (注) 最大 100 個のクライアントを追加できません。
- [Apply] をクリックします。
 - [Protocols] タブを選択して、[FlexConnect > Edit (Local Authentication > Protocols)] ページを開きます。
 - FlexConnect アクセスポイントが LEAP を使用してクライアントを認証できるようにするには、[Enable LEAP Authentication] チェックボックスをオンにします。
 - EAP-FAST を使用しているクライアントを FlexConnect アクセスポイントで認証できるようにするには、[Enable EAP-FAST Authentication] チェックボックスをオンにします。デフォルト値はオフです。
 - FlexConnect アクセスポイントが PEAP 認証を使用してクライアントを認証できるようにするには、[Enable PEAP Authentication] チェックボックスをオンにします。

AP ローカル認証が有効な場合にのみ、PEAP 認証を設定できます。

- m) EAP-TLS を使用しているクライアントを FlexConnect アクセスポイントで認証できるようにするには、[Enable EAP TLS Authentication] チェックボックスをオンにします。
AP ローカル認証が有効な場合にのみ、EAP-TLS 認証を設定できます。
EAP-TLS 認証を有効にすると、アクセスポイントに EAP ルートとデバイスの証明書をダウンロードできるようになります。ダウンロードしない場合は、[EAP TLS Certificate download] チェックボックスを選択解除することができます。
- n) Protected Access Credential (PAC) をプロビジョニングする方法に応じて、次のいずれかを実行します。
- 手動の PAC プロビジョニングを使用するには、[Server Key] テキストボックスと [Confirm Server Key] テキストボックスに、PAC の暗号化と復号化に使用するサーバキーを入力します。キーは 32 桁の 16 進数文字である必要があります。
 - PAC プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにするには、[Enable Auto Key Generation] チェックボックスをオンにします。
- o) [Authority ID] テキストボックスに、EAP-FAST サーバの Authority ID を入力します。識別子は 32 桁の 16 進数文字である必要があります。
- p) [Authority Info] テキストボックスに、EAP-FAST サーバの Authority ID をテキスト形式で入力します。32 桁までの 16 進数文字を入力できます。
- q) PAC タイムアウト値を指定するには、[PAC Timeout] チェックボックスをオンにして、PAC がテキストボックスに表示される秒数を入力します。デフォルトではオフになっています。入力できる有効な範囲は 2 ~ 4095 秒です。
- r) [Apply] をクリックします。

ステップ 14 [WLAN-ACL mapping] タブでは、次のことを実行できます。

- a) [Web Auth ACL Mapping] の下で、WLAN ID を入力し、[WebAuth ACL] を選択し、[Add] をクリックして、Web 認証 ACL と WLAN をマッピングします。
- b) [Local Split ACL Mapping] の下で、WLAN ID を入力し、[Local Split ACL] を選択し、[Add] をクリックして、ローカルスプリット ACL を WLAN にマッピングします。
- (注) ローカルスプリットトンネリングには、最大 16 の WLAN と ACL の組み合わせを設定できます。ローカルスプリットトンネリングは、静的 IP アドレスを使用するクライアントには機能しません。

ステップ 15 [Central DHCP] タブでは、次のことを実行できます。

- a) [WLAN Id] ボックスに、中央 DHCP をマッピングする WLAN ID を入力します。
- b) [Central DHCP] チェックボックスをオンまたはオフにして、マッピングに対する中央 DHCP を有効または無効にします。
- c) [Override DNS] チェックボックスをオンまたはオフにして、マッピングに対する DNS のオーバーライドを有効または無効にします。
- d) [NAT-PAT] チェックボックスをオンまたはオフにして、マッピングに対するネットワークアドレス変換およびポートアドレス変換を有効または無効にします。

- e) [Add] をクリックして、中央 DHCP と WLAN のマッピングを追加します。

ステップ 16 [Save Configuration] をクリックします。

ステップ 17 さらに FlexConnect を追加する場合は、この手順を繰り返します。

- (注) 個々のアクセス ポイントが FlexConnect グループに属しているかどうかを確認するには、次の順に選択します。[FlexConnect] タブで [Wireless] > [Access Points] > [All APs] > 目的のアクセス ポイントの名前。アクセス ポイントが FlexConnect に属する場合、グループの名前は [FlexConnect Name] テキスト ボックスに表示されます。

FlexConnect グループの設定 (CLI)

ステップ 1 次のコマンドを入力して、FlexConnect グループを追加または削除します。

```
config flexconnect group group_name {add | delete}
```

ステップ 2 次のコマンドを入力して、FlexConnect グループのプライマリ RADIUS サーバまたはセカンダリ RADIUS サーバを設定します。

```
config flexconnect group group_name radius server auth {add | delete} {primary | secondary} server_index
```

ステップ 3 次のコマンドを入力して、FlexConnect グループのプライマリ RADIUS サーバまたはセカンダリ RADIUS サーバを設定します。

```
config flexconnect group group-name radius server auth {{add {primary | secondary} ip-addr auth-port secret} | {delete {primary | secondary}}}
```

ステップ 4 次のコマンドを入力して、FlexConnect グループにアクセス ポイントを追加します。

```
config flexconnect group_name ap {add | delete} ap_mac
```

ステップ 5 次のように、FlexConnect のローカル認証を設定します。

- a) FlexConnect グループにプライマリおよびセカンダリの RADIUS サーバが設定されていないことを確認します。

- b) この FlexConnect グループのローカル認証を有効または無効にするには、次のコマンドを入力します。

```
config flexconnect group group_name radius ap {enable | disable}
```

- c) 次のコマンドを入力して、LEAP、EAP-FAST、PEAP、または EAP-TLS を使用して認証するクライアントのユーザ名とパスワードを入力します。

```
config flexconnect group group_name radius ap user add username password password
```

- (注) 最大 100 個のクライアントを追加できます。

- d) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが LEAP を使用して認証できるかどうかを指定します。

```
config flexconnect group group_name radius ap leap {enable | disable}
```

- e) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが EAP-FAST を使用して認証できるかどうかを指定します。

config flexconnect group group_name radius ap eap-fast {enable | disable}

- f) AP に EAP ルートおよびデバイス証明書をダウンロードするには、次のコマンドを入力します。

config flexconnect group group_name radius ap eap-cert download

- g) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが EAP-TLS を使用してクライアントを認証できるかどうかを指定します。

config flexconnect group group_name radius ap eap-tls {enable | disable}

- h) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが PEAP を使用してクライアントを認証できるかどうかを指定します。

config flexconnect group group_name radius ap peap {enable | disable}

- i) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが PEAP を使用して認証できるかどうかを指定します。

config flexconnect group group_name radius ap peap {enable | disable}

- j) 次のコマンドを入力して、FlexConnect アクセス ポイント グループが EAP-TLS を使用して認証できるかどうかを指定します。

config flexconnect group group_name radius ap eap-tls {enable | disable}

- k) 次のコマンドを入力して、EAP ルートおよびデバイス証明書をダウンロードします。

config flexconnect group group_name radius ap eap-cert download

- l) PAC をプロビジョニングする方法に応じて、次のいずれかのコマンドを入力します。

- **config flexconnect group group_name radius ap server-key key** : PAC の暗号化と暗号解除に使用するサーバ キーを指定します。キーは 32 桁の 16 進数文字である必要があります。

- **config flexconnect group group_name radius ap server-key auto** : PAC プロビジョニング中に、PAC を持たないクライアントに PAC を自動的に送信できるようにします。

- m) EAP-FAST サーバの Authority ID を指定するには、次のコマンドを入力します。

config flexconnect group group_name radius ap authority id id

id は 32 桁の 16 進数文字です。

- n) EAP-FAST サーバの Authority ID をテキスト形式で指定するには、次のコマンドを入力します。

config flexconnect group group_name radius ap authority info info

info は 32 桁までの 16 進数文字です。

- o) PAC が表示される秒数を指定するには、次のコマンドを入力します。

config flexconnect group group_name radius ap pac-timeout timeout

timeout に指定できるのは、2 ~ 4095 秒の範囲内の値または 0 です。0 がデフォルト値です。この値を指定すると、PAC はタイムアウトしなくなります。

- ステップ 6** 次のコマンドを入力して、FlexConnect グループ 上に ポリシー ACL を設定します。

config flexconnect group group-name policy acl {add | delete} acl-name

- ステップ 7** 次のコマンドを入力して、FlexConnect グループごとにローカル スプリット トンネリングを設定します。

config flexconnect group group_name local-split wlan wlan-id acl acl-name flexconnect-group-name {enable | disable}

- ステップ 8** ローカルにスイッチされるクライアントに対して、上書きされたインターフェイスの L2 ブロードキャストドメイン間のマルチキャスト/ブロードキャストを設定するには、次のコマンドを入力します。
config flexconnect group *group_name* multicast overridden-interface {enable | disable}
- ステップ 9** 次のコマンドを入力して、WLAN ごとに中央 DHCP を設定します。
config flexconnect group *group_name* central-dhcp *wlan-id* {enable override dns | disable | delete}
- ステップ 10** 次のコマンドを入力して、FlexConnect グループにポリシー ACL を設定します。
config flexconnect group *group_name* policy acl {add | delete} *acl-name*
- ステップ 11** 次のコマンドを入力して、FlexConnect グループに Web 認証 ACL を設定します。
config flexconnect group *group_name* web-auth wlan *wlan-id* acl *acl-name* {enable | disable}
- ステップ 12** 次のコマンドを入力して、FlexConnect グループに WLAN-VLAN マッピングを設定します。
config flexconnect group *group_name* wlan-vlan wlan *wlan-id* {add | delete} vlan *vlan-id*
- ステップ 13** グループの効率的なアップグレードを設定するには、次のコマンドを入力します。
config flexconnect group *group_name* predownload {enable | disable | master | slave} *ap-name* retry-count *maximum retry count* *ap-name* *ap-name*
- ステップ 14** 次のコマンドを入力して、変更を保存します。
save config
- ステップ 15** 次のコマンドを入力して、FlexConnect グループの最新のリストを表示します。
show flexconnect group summary
- ステップ 16** 次のコマンドを入力して、特定の FlexConnect グループの詳細を表示します。
show flexconnect group detail *group_name*
-

FlexConnect グループの VLAN-ACL マッピングの設定

FlexConnect グループの VLAN-ACL マッピングの設定 (GUI)

- ステップ 1** [Wireless] > [FlexConnect Groups] を選択します。
[FlexConnect Groups] ページが表示されます。このページに、コントローラにアソシエータされているアクセスポイントが一覧表示されます。
- ステップ 2** VLAN-ACL マッピングを設定する FlexConnect グループの [Group Name] リンクをクリックします。
- ステップ 3** [VLAN-ACL Mapping] タブをクリックします。
その FlexConnect グループの [VLAN-ACL Mapping] ページが表示されます。

- ステップ 4 [VLAN ID] テキスト ボックスにネイティブ VLAN ID を入力します。
- ステップ 5 [Ingress ACL] ドロップダウン リストから、[Ingress ACL] を選択します。
- ステップ 6 [Egress ACL] ドロップダウン リストから、出力 ACL を選択します。
- ステップ 7 [Add] をクリックして、FlexConnect グループにこのマッピングを追加します。
VLAN ID は、必要な ACL とともにマッピングされます。マッピングを削除するには、青のドロップダウン 矢印の上にカーソルを移動し、[Remove] を選択します。

FlexConnect グループの VLAN-ACL マッピングの設定 (CLI)

- 次のコマンドを入力して、VLAN を FlexConnect グループに追加し、入力 ACL と出力 ACL をマッピングします。

```
config flexconnect group group-name vlan add vlan-id acl ingress-acl egress acl
```

VLAN-ACL マッピングの表示 (CLI)

- 次のコマンドを入力して、FlexConnect グループの詳細を表示します。
show flexconnect group detail group-name
- 次のコマンドを入力して、アクセス ポイントの VLAN-ACL マッピングを表示します。
show ap config general ap-name

FlexConnect グループの WLAN-VLAN マッピングの設定

FlexConnect グループの WLAN-VLAN マッピングの設定 (GUI)

次に注意事項を示します。

- 個々の AP 設定は、FlexConnect グループおよびグローバル WLAN の設定よりも優先されません。FlexConnect グループ設定は、グローバル WLAN 設定よりも優先されます。
- AP レベル設定はフラッシュに保存され、WLAN および FlexConnect グループの設定は RAM に保存されます。
- AP は、異なるコントローラ間を移動する場合に、個々の VLAN マッピングを保持することができます。ただし、FlexConnect グループおよびグローバルのマッピングは新しいコントローラの設定になります。WLAN SSID が 2 台のコントローラ間で異なる場合、WLAN-VLAN マッピングは適用されません。
- ダウンストリームトラフィックでは、VLAN ACL が最初に適用されてからクライアント ACL が適用されます。アップストリームトラフィックでは、クライアント ACL が最初に適用されてから VLAN ACL が適用されます。

- 802.1X 認証時に ACL が AP に存在する必要があります。ACL が AP がない場合、クライアントは、802.1X 認証に成功しても AP によって認証を拒否される場合があります。

| AP 上の ACL の有無 | AAA から送信された ACL 名 | 802.1X 認証の結果 |
|---------------|-------------------|--------------------|
| No | No | 認証済み、ACL 適用なし |
| No | Yes | 認証拒否 |
| Yes | No | 認証済み、ACL 適用なし |
| Yes | Yes | 認証済み、クライアント ACL 適用 |

- クライアント認証後に、ACL 名が RADIUS サーバ上で変更された場合、クライアントは、再び最初から認証を実行して正しいクライアント ACL を取得する必要があります。
- FlexConnect グループの WLAN-VLAN マッピングは Cisco AP の 1131 および 1242 でサポートされません。

はじめる前に

WLAN がローカルにスイッチされることを確認します。設定は、WLAN が AP でブロードキャストされる場合にのみ AP に適用されます。

-
- ステップ 1 [Wireless] > [FlexConnect Groups] を選択します。
- ステップ 2 グループ名をクリックします。
[FlexConnect Groups > Edit] ページが表示されます。
- ステップ 3 [WLAN VLAN Mapping] タブをクリックします。
- ステップ 4 WLAN ID と VLAN ID を入力し、[Add] をクリックします。
マッピングは同じタブに表示されます。
- ステップ 5 [Apply] をクリックします。
- ステップ 6 [Save Configuration] をクリックします。
-

FlexConnect グループの WLAN-VLAN マッピングの設定 (CLI)

はじめる前に

WLAN がローカルにスイッチされることを確認します。設定は、WLAN が AP でブロードキャストされる場合にのみ AP に適用されます。

- 次のコマンドを入力して、FlexConnect グループに WLAN-VLAN マッピングを設定します。
config flexconnect group group-name wlan-vlan wlan wlan-id {add | delete} vlan vlan-id



第 150 章

FlexConnect の AAA Override の設定

- [認証、許可、アカウントिंग オーバーライドについて](#), 1143 ページ
- [FlexConnect の AAA Override に関する制約事項](#), 1145 ページ
- [アクセス ポイント上の FlexConnect に対する AAA Override の設定 \(GUI\)](#), 1146 ページ
- [アクセス ポイント上の FlexConnect に対する VLAN Override の設定 \(CLI\)](#), 1147 ページ

認証、許可、アカウントिंग オーバーライドについて

WLAN の [Allow Authentication, Authorization, Accounting (AAA) Override] オプションでは認証用に WLAN を設定することができます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、QoS、および ACL を適用できます。

FlexConnect アクセス ポイントに対する AAA Override は、ローカルにスイッチされたクライアントへダイナミック VLAN の割り当てを提供します。また、FlexConnect の AAA Override は、上書きされたクライアントの高速ローミング (Opportunistic Key Caching : OKC/Cisco Centralized Key management : CCKM) をサポートします。

FlexConnect に対する VLAN Override は、中央で認証されたクライアントとローカルで認証されたクライアントの両方に適用されます。VLAN は、FlexConnect グループで設定することができます。

AP の VLAN が WLAN-VLAN を使用して設定されている場合、対応する ACL の AP 設定が適用されます。FlexConnect グループを使用して VLAN を設定する場合、FlexConnect グループで設定された対応する ACL が適用されます。FlexConnect グループと AP で同じ VLAN を設定する場合、ACL を使用した AP 設定が優先されます。WLAN-VLAN マッピングからの新しい VLAN 用のスロットがない場合、設定されている最新の FlexConnect グループ VLAN が置き換えられます。

AAA から戻された VLAN が AP 上に存在しない場合、クライアントは WLAN に設定されたデフォルト VLAN にフォールバックされます。

AAA Override を設定する前に、アクセス ポイントで VLAN が作成されている必要があります。これらの VLAN は、アクセス ポイントの既存の WLAN-VLAN マッピングを使用するか、または FlexConnect グループ VLAN-ACL マッピングを使用して作成できます。

IPv6 ACL に対する AAA オーバーライド

Cisco Identity Services Engine (ISE) または ACS のように、中央集中型 AAA サーバを介した中央集中型のアクセス制御をサポートするために、AAA Override 属性を使用してクライアントごとに IPv6 ACL を提供できます。この機能を使用するには、IPv6 ACL をコントローラに設定し、AAA Override 機能を有効にして WLAN を有効にする必要があります。IPv6 ACL の AAA 属性は IPv4 ベースの ACL をプロビジョニングするために使用される *Airespace-ACL-Name* 属性に似た *Airespace-IPv6-ACL-Name* です。AAA 属性が返すコンテンツは、コントローラで設定された IPv6 ACL の名前に一致する文字列になるはずですが。

AP とコントローラの双方向レート制限の AAA Override

FlexConnect AP の AAA Override が、QoS レベルや帯域幅コントラクトを、Web 認証済み WLAN と 802.1X 認証済み WLAN の両方のローカルにスイッチされるトラフィックに対して動的に割り当てるようにできます。アップストリームとダウンストリームの両方のパラメータが、対応する AP に送信されます。

次の表に、二方向レート制限の実装の例を示します。

表 29: 双方向レート制限の実装

| アップストリーム/
ダウンストリーム | ローカル モード | FlexConnect 中央ス
イッチング | FlexConnect ローカ
ル スイッチング | FlexConnect スタン
ドアロン |
|---------------------------|----------|--------------------------|-----------------------------|-------------------------|
| クライアントごと
のダウンストリー
ム | コントローラ | コントローラ | AP | AP |
| クライアントごと
のアップストリー
ム | AP | AP | AP | AP |

次の表には、ローカルおよび FlexConnect 中央スイッチングの優先順位の例が示されています。

表 30: レート制限パラメータ

| AAA | AAA の QoS プロファイル | WLAN | WLAN の QoS プ
ロファイル | クライアントに
適用される |
|----------|------------------|----------|-----------------------|------------------|
| 100 Kbps | 200 Kbps | 300 Kbps | 400 Kbps | 100 Kbps |
| ○ | — | — | — | 200 Kbps |
| ○ | ○ | — | — | 300 Kbps |
| ○ | ○ | ○ | — | 400 Kbps |
| ○ | ○ | ○ | ○ | 無制限 |

FlexConnect の AAA Override に関する制約事項

- AAA Override を設定する前に、VLAN をアクセス ポイントで作成する必要があります。これらの VLAN は、アクセス ポイントの既存の WLAN-VLAN マッピングを使用するか、または FlexConnect グループ VLAN-ACL マッピングを使用して作成できます。
- 常に、AP には最大 16 の VLAN があります。まず、VLAN は AP 設定 (WLAN-VLAN) に従って選択され、残りの VLAN は FlexConnect グループで設定または表示されている順序で FlexConnect グループからプッシュされます。VLAN スロットがフルの場合、エラーメッセージが表示されます。
- ローカルにスイッチされるクライアントの AAA は、VLAN Override のみをサポートします。
- ダイナミック VLAN の割り当ては、Access Control Server (ACS) のコントローラの Web 認証ではサポートされていません。
- AP およびコントローラの双方向レート制限の AAA Override は、次の 802.11n の非メッシュ アクセス ポイントのすべてでサポートされます。

- 1040
- 1140
- 1250
- 1260
- 1600
- 2600
- 3500
- 3600

この機能は、メッシュおよびレガシーの AP プラットフォームでサポートされていません。

- 1130
 - 1240
 - 1520
 - 1550
- 双方向レート制限の場合
 - 双方向レート制限がない場合、AAA Override は実行されません。
 - 対応する WLAN の QoS プロファイルが Silver であっても、クライアントの QoS プロファイルは Platinum に設定できます。AP では、クライアントが音声キューにパケットを送信できます。ただし、セッション開始プロトコル (SIP) スヌーピングを WLAN 上で無効にして、SIP クライアントのトラフィックが音声キューに送信されないようにする必要があります。

- ISE サーバがサポートされています。
- アップストリーム レート制限パラメータは、AAA Override のダウンストリームパラメータと同様です。
- ローカル認証はサポートされていません。

アクセスポイント上の FlexConnect に対する AAA Override の設定 (GUI)

ステップ 1 [Wireless] > [All] > [APs] を選択します。
[All APs] ページが表示されます。このページに、コントローラにアソシエータされているアクセスポイントが一覧表示されます。

ステップ 2 対応する AP 名をクリックします。

ステップ 3 [FlexConnect] タブをクリックします。

ステップ 4 [Native VLAN ID] の値を入力します。

ステップ 5 [VLAN Mappings] ボタンをクリックして、[AP VLANs] マッピングを設定します。
次のようなパラメータが表示されます。

- [AP Name] : アクセスポイント名。
- [Base Radio MAC] : AP のベース無線。
- [WLAN-SSID-VLAN ID Mapping] : コントローラで設定された各 WLAN に対して、対応する SSID および VLAN ID が表示されます。WLAN の VLAN ID 列を編集して WLAN-VLAN ID マッピングを変更します。
- [Centrally Switched WLANs] : 中央でスイッチされる WLAN が設定されている場合、WLAN-VLAN マッピングが一覧表示されます。
- [AP Level VLAN ACL Mapping] : 次のパラメータを使用できます。
 - [VLAN ID] : VLAN ID。
 - [Ingress ACL] : VLAN に対応する入力 ACL。
 - [Egress ACL] : VLAN に対応する出力 ACL。

各 ACL タイプのドロップダウンリストからマッピングを選択して、入力 ACL および出力 ACL マッピングを変更します。

- [Group Level VLAN ACL Mapping] : 次のグループレベルの VLAN ACL マッピングパラメータが使用できます。
 - [VLAN ID] : VLAN ID。
 - [Ingress ACL] : この VLAN に対する入力 ACL。

° [Egress ACL] : この VLAN に対する出力 ACL。

ステップ 6 [Apply] をクリックします。

アクセス ポイント上の FlexConnect に対する VLAN Override の設定 (CLI)

FlexConnect アクセス ポイントの VLAN Override を設定するには、次のコマンドを使用します。

```
config ap flexconnect vlan add vlan-id acl ingress-acl egress-acl ap_name
```




第 151 章

FlexConnect アクセスポイントに対する FlexConnect AP のアップグレードの設定

- [FlexConnect AP のアップグレードについて, 1149 ページ](#)
- [FlexConnect アクセスポイントに対する FlexConnect AP アップグレードに関する制約事項, 1150 ページ](#)
- [FlexConnect AP のアップグレードの設定 \(GUI\) , 1150 ページ](#)
- [FlexConnect AP のアップグレードの設定 \(CLI\) , 1151 ページ](#)

FlexConnect AP のアップグレードについて

通常、AP のイメージをアップグレードする際に、プリイメージダウンロード機能を使用して、AP がクライアントに対応できない時間を短縮することができます。一方、アクセスポイントはアップグレード中、クライアントに対応できないため、ダウンしている時間も増加します。プリイメージダウンロード機能は、このダウンしている時間を短縮するために使用することができます。ただし、ブランチオフィスセットアップの場合、アップグレードイメージは引き続き WAN リンクを介して、各アクセスポイントにダウンロードされるので、より大きな遅延が発生します。

より効率的な方法は、FlexConnect AP のアップグレード機能を使用することです。この機能が有効になっている場合、まずローカルネットワーク内の各モデルの 1 つのアクセスポイントは、WAN リンクを介してアップグレードイメージをダウンロードします。これはマスター/スレーブモデルやクライアント/サーバモデルと同じように動作します。このアクセスポイントは、次に類似したモデルの残りのアクセスポイントのマスターになります。残りのアクセスポイントは、次にアップグレードイメージをマスターアクセスポイントから、ローカルネットワークを介してプリイメージダウンロード機能を使用してダウンロードします。これにより、WAN の遅延時間が短縮されます。

FlexConnect アクセスポイントに対する FlexConnect AP アップグレードに関する制約事項

- ネットワークのプライマリ コントローラおよびセカンダリ コントローラは、プライマリ イメージおよびバックアップ イメージの設定と同じにする必要があります。
- FlexConnect グループが設定されている場合、そのグループ内のすべてのアクセス ポイントは、同じサブネット内にあるか、NAT を介してアクセスできる必要があります。

FlexConnect AP のアップグレードの設定 (GUI)

-
- ステップ 1** [Wireless] > [FlexConnect Groups] を選択します。
[FlexConnect Groups] ページが表示されます。このページに、コントローラで設定された FlexConnect グループが一覧表示されます。
- ステップ 2** イメージアップグレードを設定する [Group Name] リンクをクリックします。
- ステップ 3** [Image Upgrade] タブをクリックします。
- ステップ 4** [FlexConnect AP Upgrade] チェックボックスをオンにして、FlexConnect AP のアップグレードを有効にします。
- ステップ 5** 前の手順で FlexConnect AP のアップグレードを有効にした場合、次のパラメータを有効にする必要があります。
- [Slave Maximum Retry Count] : アップグレード イメージのダウンロードについて、スレーブ アクセスポイントがマスターアクセスポイントに接続するように試すべき試行回数。設定された再試行の間にイメージダウンロードが行われない場合、イメージはWANを介してアップグレードされます。
 - [Upgrade Image] : アップグレードイメージを選択します。オプションは、[Primary]、[Backup]、および [Abort] です。
 - [FlexConnect Upgrade] をクリックして、アップグレードします。
- ステップ 6** [AP Name] ドロップダウンリストから、[Add Master] をクリックしてマスターアクセスポイントを追加します。
アクセスポイントを選択して、FlexConnect グループのマスターアクセスポイントを手動で割り当てることができます。
- ステップ 7** [Apply] をクリックします。
-

FlexConnect AP のアップグレードの設定 (CLI)

- **config flexconnect group *group-name* predownload {enable | disable}** : FlexConnect AP のアップグレードを有効または無効にします。
- **config flexconnect group *group-name* predownload master *ap-name*** : あるアクセス ポイントをマスター アクセス ポイントとして手動で割り当てます。
- **config flexconnect group *group-name* predownload slave *retry-count* *ap-name*** : アクセスポイントをスレーブ アクセス ポイントとして再試行回数とともに設定します。
- **config flexconnect group *group-name* predownload start** : FlexConnect グループのアクセス ポイントでイメージ ダウンロードを開始します。
- **config ap image predownload {abort | primary | backup}** : プリイメーリアップグレードでダウンロードする必要があるイメージ タイプを割り当てます。
- **show flexconnect group *group-name*** : FlexConnect グループ設定の概要を表示します。
- **show ap image all** : アクセス ポイント上のイメージの詳細を表示します。



第 **X** 部

モビリティ グループの設定

- [モビリティ グループの設定, 1155 ページ](#)
- [モビリティ グループの統計の表示, 1171 ページ](#)
- [自動アンカー モビリティの設定, 1175 ページ](#)
- [WLAN モビリティ セキュリティの値の検証, 1181 ページ](#)
- [シンメトリック モビリティ トンネリングの使用, 1183 ページ](#)
- [モビリティ ping テストの実行, 1185 ページ](#)
- [固定 IP アドレスを持つクライアントのダイナミック アンカーの設定, 1187 ページ](#)
- [外部マッピングの設定, 1191 ページ](#)
- [プロキシ モバイル IPv6 の設定, 1193 ページ](#)
- [新しいモビリティの設定, 1201 ページ](#)



第 152 章

モビリティ グループの設定

- [モビリティについて, 1155 ページ](#)
- [モビリティ グループについて, 1159 ページ](#)
- [モビリティ グループを設定するための前提条件, 1163 ページ](#)
- [モビリティ グループの設定 \(GUI\) , 1165 ページ](#)
- [モビリティ グループの設定 \(CLI\) , 1167 ページ](#)

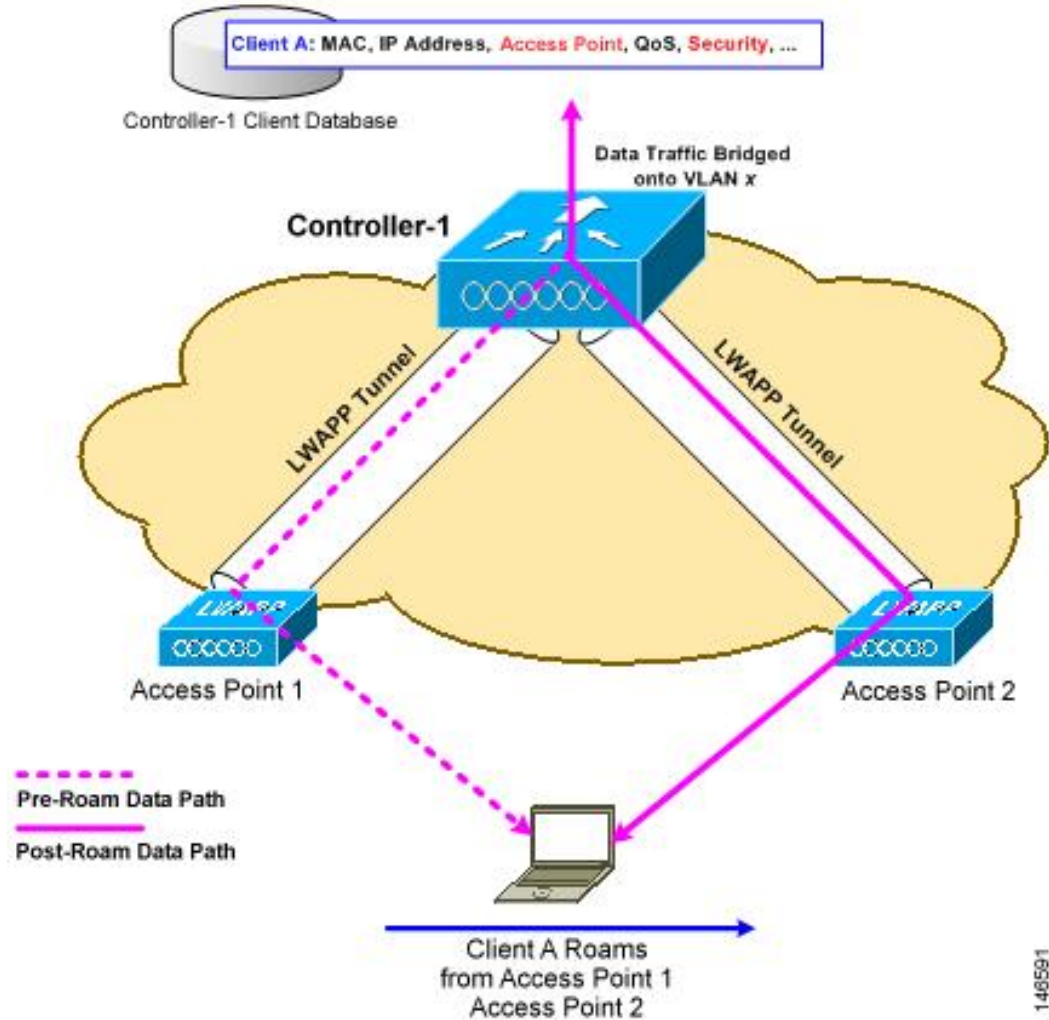
モビリティについて

モビリティ（ローミング）は、できるだけ遅れることなく、確実かつスムーズに、あるアクセスポイントから別のアクセスポイントへアソシエーションを維持する無線 LAN クライアントの機能です。この項では、コントローラが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレスクライアントがアクセスポイントにアソシエートして認証すると、アクセスポイントのコントローラは、クライアントデータベースにそのクライアントに対するエントリを設定します。このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティコンテキストおよびアソシエーション、Quality of Service (QoS) コンテキスト、WLAN、およびアソシエートされたアクセスポイントが含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレスクライアントで送受信されるトラフィックを管理します。

この図には、2つのアクセスポイントが同一のコントローラに join されている場合の両アクセスポイント間における無線クライアントローミングの様子が示されています。

図 73: コントローラ内ローミング

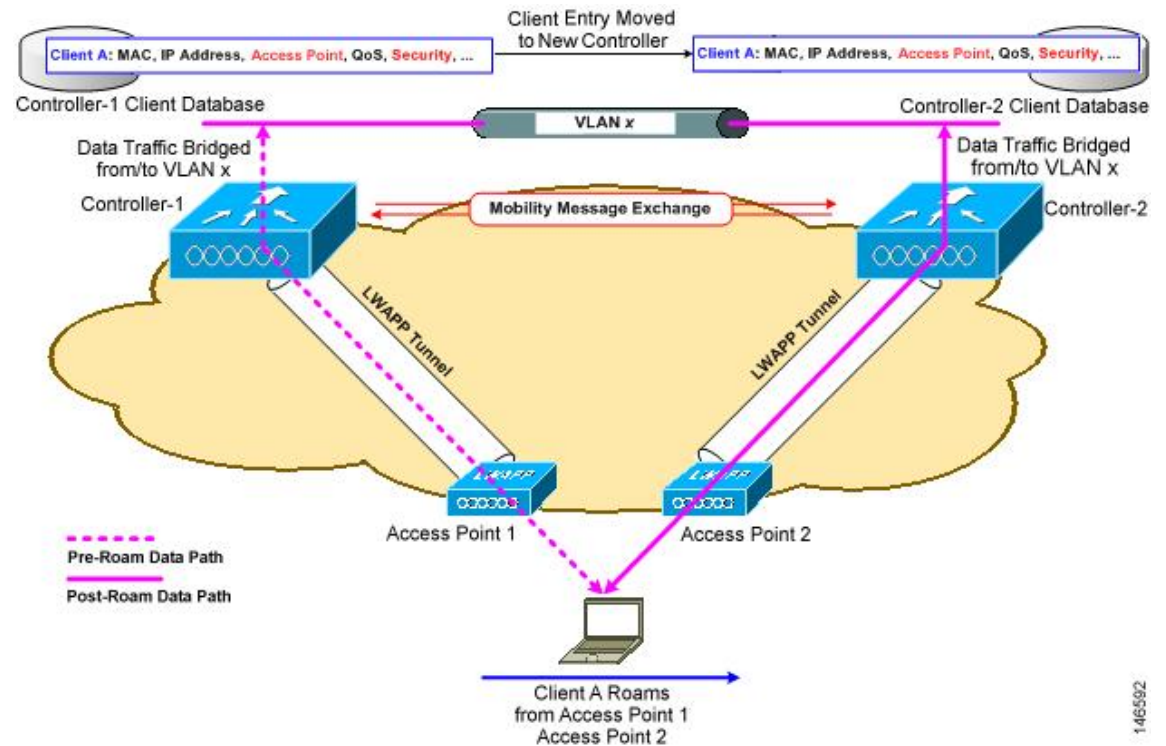


ワイヤレスクライアントがそのアソシエーションをあるアクセスポイントから別のアクセスポイントへ移動する場合、コントローラはクライアントのデータベースを新たにアソシエートするアクセスポイントでアップデートするだけです。必要に応じて、新たなセキュリティコンテキストとアソシエーションも確立されます。

しかし、クライアントが1つのコントローラに join されたアクセスポイントから別のコントローラに join されたアクセスポイントにローミングする際には、プロセスはより複雑になります。また、同一のサブネット上でこれらのコントローラが動作しているかどうかによっても異なります。

次の図に、コントローラの無線 LAN インターフェイスが同じ IP サブネット上に存在する場合に発生するコントローラ間ローミングを示します。

図 74: コントローラ間ローミング



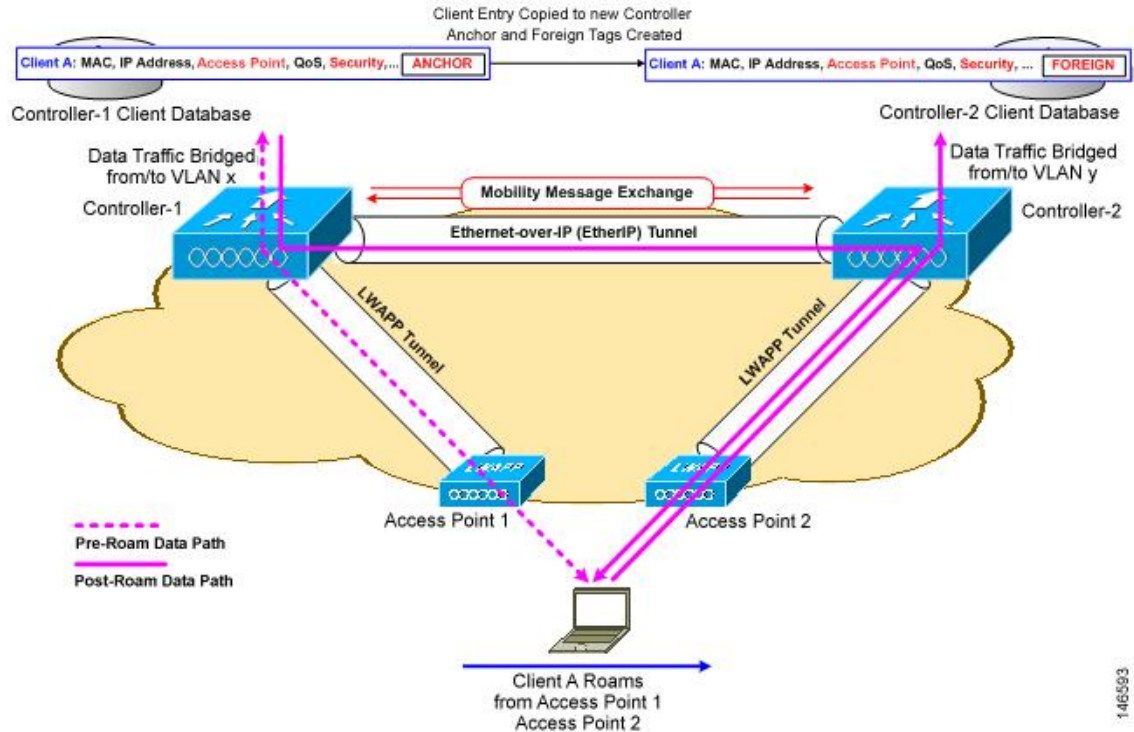
クライアントが新たなコントローラに join されたアクセスポイントへアソシエートする場合、新たなコントローラはモビリティメッセージを元のコントローラと交換し、クライアントのデータベースエントリは新たなコントローラに移動されます。新たなセキュリティコンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベースエントリは新たなアクセスポイントに対してアップデートされます。このプロセスは、ユーザには透過的に行われます。



(注) 802.1X/Wi-Fi Protected Access (WPA) セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

次の図は、コントローラの無線 LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを表したものです。

図 75: サブネット間ローミング



サブネット間ローミングは、コントローラがクライアントのローミングに関するモビリティメッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベースエントリを新しいコントローラに移動するのではなく、元のコントローラのクライアントデータベース内で該当クライアントに「アンカー」エントリのマークが付けられます。このデータベースエントリが新しいコントローラのクライアントデータベースにコピーされ、新しいコントローラ内で「外部」エントリのマークが付けられます。ローミングはワイヤレスクライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカーと外部の両コントローラの WLAN に同一のネットワークアクセス権限を設定し、ソーススペースのルーティングやソーススペースのファイアウォールを設定しないでおく必要があります。そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

コントローラと ACS を使用して設定されたスタティック固定で動的に VLAN および QoS を割り当てるように AAA オーバーライドが有効になっている場合、外部コントローラはレイヤ 2 の認証 (802.1x) の後に権限 VLAN を使用してアンカー コントローラを更新します。レイヤ 3 RADIUS 認証の場合、認証の RADIUS 要求は、アンカー コントローラによって送信されます。

モビリティは、MAC フィルタの失敗時に Webauth に設定されるセキュリティタイプの SSID ではサポートされません。



(注) クライアントが Web 認証状態でローミングする場合、クライアントはモバイルクライアントとして見なされるのではなく、別のコントローラ上の新しいクライアントとして見なされます。

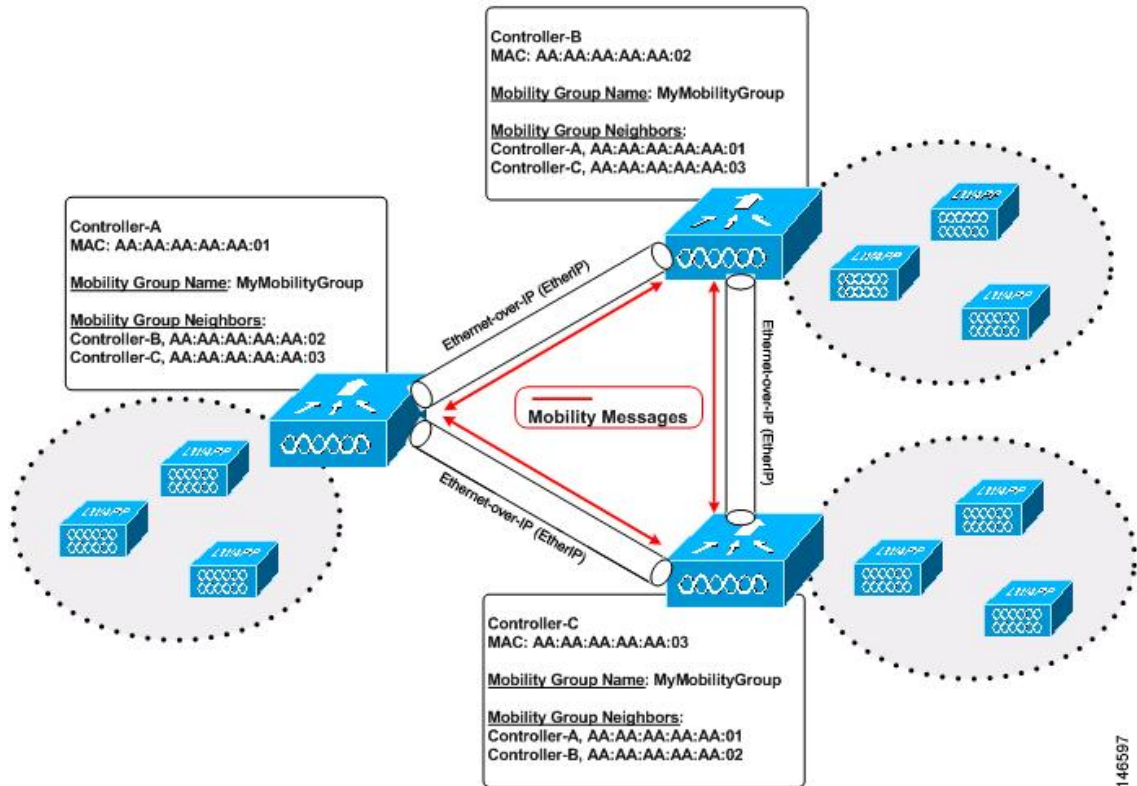
モビリティグループについて

モビリティグループは、同じモビリティグループ名で定義されるコントローラのセットで、ワイヤレスクライアントのローミングをシームレスに行う範囲を定義します。モビリティグループを作成すると、ネットワーク内で複数のコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータトラフィックを転送できるようになります。同じモビリティグループ内のコントローラは、相互のアクセスポイントを不正なデバイスとして認識しないように、クライアントデバイスのコンテキストと状態およびアクセスポイントのリストを共有できます。この情報を使用して、ネットワークはコントローラ間無線 LAN ローミングとコントローラの冗長性をサポートできます。



(注) 1つのモビリティグループのメンバーとなるコントローラは、同じモデルである必要はありません。モビリティグループは、コントローラプラットフォームの任意の組み合わせで構成できます。

図 76：単一のモビリティグループの例



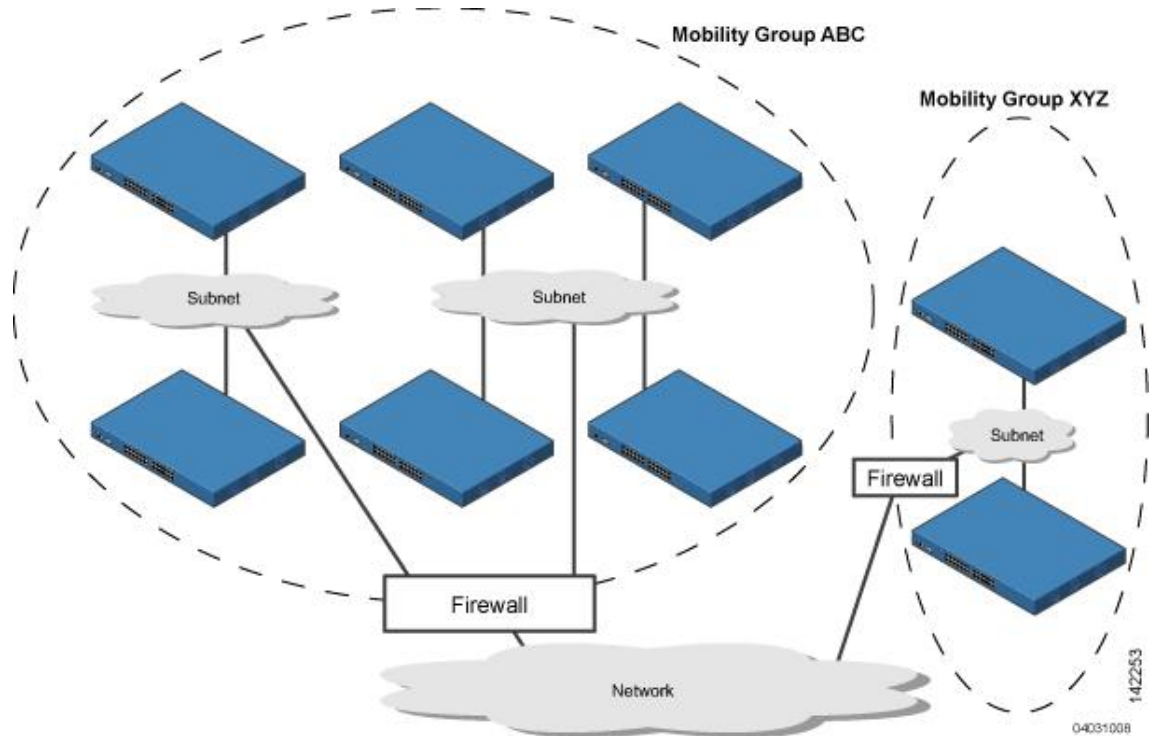
図示したように、各コントローラはモビリティグループの別メンバーのリストを使用して設定されています。新たなクライアントがコントローラに join されると、コントローラはユニキャストメッセージ（または、モビリティマルチキャストが設定されている場合はマルチキャストメッセージ）をそのモビリティグループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。

たとえば、コントローラが 6000 個のアクセスポイントをサポートする場合に、24 個のこのようなコントローラで構成されているモビリティグループは、最大 144,000 個のアクセスポイント（ $24 * 6000 = 144,000$ アクセスポイント）をサポートします。

異なるモビリティグループ名を同じ無線ネットワーク内の異なるコントローラに割り当てると、モビリティグループによって、1つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

次の図には、2つのコントローラグループに異なるモビリティグループ名を作成した結果が示されています。

図 77: 2つのモビリティグループ



ABC モビリティグループのコントローラは、相互にアクセスポイントとクライアント情報を共有します。ABC モビリティグループのコントローラは、異なるモビリティグループのXYZ コントローラとアクセスポイントとクライアントの情報を共有しません。同様に、XYZ モビリティグループのコントローラは、ABC モビリティグループのコントローラとアクセスポイントとクライアントの情報を共有しません。この機能により、ネットワークでのモビリティグループの切り離しが確実に行われます。

各コントローラはモビリティリストのピアコントローラに関する情報を保持します。コントローラ同士が相互のモビリティリストに含まれている場合は、モビリティグループ間でコントローラが通信を行うことができ、クライアントは異なるモビリティグループのアクセスポイント間でローミングを行うことができます。次の例のコントローラ1はコントローラ2または3と通信できますが、コントローラ2およびコントローラ3はコントローラ1だけと通信し、相互には通信できません。クライアントは同様に、コントローラ1とコントローラ2の間またはコントローラ1とコントローラ3の間はローミングを行うことができますが、コントローラ2とコントローラ3の間でローミングを行うことはできません。

表 31: 例

| | | |
|---------------------------------------|---------------------------------------|---------------------------------------|
| コントローラ 1
モビリティグループ: A
モビリティリスト: | コントローラ 2
モビリティグループ: A
モビリティリスト: | コントローラ 3
モビリティグループ: C
モビリティリスト: |
| コントローラ 1 (A グループ) | コントローラ 1 (A グループ) | コントローラ 1 (A グループ) |
| コントローラ 2 (A グループ) | コントローラ 2 (A グループ) | コントローラ 3 (C グループ) |
| コントローラ 3 (C グループ) ? | | |

コントローラでは、複数のモビリティグループ間でのシームレスなローミングがサポートされています。シームレスなローミングでは、クライアントはすべてのモビリティグループ間で IP アドレスを維持します。ただし、Cisco Centralized Key Management (CCKM) およびプロアクティブキーキャッシング (PKC) は、モビリティグループ間ローミングでのみサポートされています。ローミング中にモビリティグループの境界を越える場合、クライアントは完全に認証されますが、IP アドレスは維持され、レイヤ 3 ローミングのモビリティトンネリングが開始されます。

モビリティグループ内でのメッセージング

コントローラでは、モビリティメッセージを他のメンバコントローラに送信することにより、クライアントにサブネット間モビリティが提供されます。

- コントローラは、新しいクライアントがアソシエートされるたびに、モビリティリスト内のメンバに **Mobile Announce** メッセージを送信します。コントローラは自分と同じグループ（ローカルグループ）に属するメンバに対してのみメッセージを送信し、その後、再試行を送信する際に他のメンバをすべて加えます。
- マルチキャストを使用して **Mobile Announce** メッセージを送信するように、コントローラを設定できます。これにより、コントローラからネットワークに送られるメッセージは 1 コピーのみになります。このコピーはモビリティメンバすべてを含むマルチキャストグループに宛てて送られます。マルチキャストメッセージングを最大限生かすには、グループメンバすべてに対してこの機能を有効化することを推奨します。

NAT デバイスでのモビリティグループの使用

モビリティメッセージのペイロードは、ソースコントローラに関する IP アドレス情報を伝達します。この IP アドレスは、IP ヘッダーのソース IP アドレスで検証されます。ネットワークに NAT デバイスを導入すると、IP ヘッダーの送信元 IP アドレスが変更されるため、この動作に問題があります。ゲスト WLAN 機能では、NAT デバイス経由でルーティングされているモビリティパケットは、IP アドレスの不一致によりドロップされます。

モビリティグループの検索は、ソースコントローラの MAC アドレスを使用します。NAT デバイスのマッピングに従ってソース IP アドレスが変更されるため、要求元のコントローラの IP ア

ドレスを取得するために応答が送信される前に、モビリティグループのデータベースが検索されます。このプロセスは、要求元のコントローラの MAC アドレスを使用して実行されます。

NAT が有効になっているネットワークのモビリティグループを設定する際に、コントローラの実管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。さらに、PIX などのファイアウォールを使用している場合には、ファイアウォールで次のポートが開いていることを確認します。

- UDP 16666 : トンネルコントロールトラフィック用
- IP プロトコル 97 : ユーザのデータトラフィック用
- UDP 161 および 162 : SNMP



(注) コントローラ間のクライアントモビリティは、自動アンカーモビリティ（ゲストトンネリングとも呼ばれる）またはシンメトリックモビリティトンネリングが有効になっている場合のみ機能します。アシンメトリックトンネリングは、モビリティコントローラが NAT デバイスの背後にある場合にはサポートされません。これらのモビリティオプションの詳細については、「自動アンカーモビリティの設定」、および「シンメトリックモビリティトンネリングの使用」の項を参照してください。

モビリティグループを設定するための前提条件

コントローラをモビリティグループに追加する前に、グループに追加するコントローラすべてについて、次の要件が満たされていることを確認する必要があります。

- すべてのコントローラの管理インターフェイス間に IP 接続が存在する必要があります。



(注) コントローラに対し Ping することで、IP 接続を確認できます。



(注) モビリティ制御パケットは、ルーティングテーブルに基づいて、任意のインターフェイスアドレスをソースとして使用できます。モビリティグループのすべてのコントローラには、同一のサブネットの管理インターフェイスを必ず備えることを推奨します。1つのコントローラの管理インターフェイスと他のコントローラの動的インターフェイスが同じサブネット上にあるトポロジは、シームレスモビリティには推奨しません。

- モビリティリスト内のコントローラが異なるソフトウェアバージョンを使用している場合、レイヤ2またはレイヤ3のクライアントのローミングサポートは制限されます。レイヤ2またはレイヤ3クライアントローミングは、同じバージョンを使用する、またはバージョン 7.X.X を実行するコントローラ間でのみサポートされます。



(注) 異なるソフトウェアリリースが実行されているフェールオーバーコントローラを誤って設定すると、アクセスポイントがフェールオーバーコントローラに join するのに長い時間がかかることがあります。アクセスポイントが検出プロセスを CAPWAP で開始してから、LWAPP 検出に変更するからです。

- すべてのコントローラは、同じ仮想インターフェイス IP アドレスで設定する必要があります。



(注) 必要に応じて、仮想インターフェイス IP アドレスを変更するには、[Controller] > [Interfaces] ページで仮想インターフェイス名を編集します。



(注) モビリティグループ内のすべてのコントローラが同じ仮想インターフェイスを使用していない場合、コントローラ間ローミングが動作しているように見えても、ハンドオフが完了せず、クライアントの接続はしばらくの間切断されます。

- モビリティグループに追加するコントローラごとに、MAC アドレスと IP アドレスを収集しておく必要があります。この情報が必要となるのは、他の全モビリティグループメンバの MAC アドレスと IP アドレスを使用してすべてのコントローラを設定するからです。



(注) モビリティグループに追加する他のコントローラの MAC アドレスと IP アドレスは、各コントローラの GUI の [Controller > Mobility Groups] ページにあります。

- サードパーティのファイアウォール、たとえば、Cisco PIX または Cisco ASA を使用してモビリティグループを設定する際は、ポート 16666 および IP プロトコル 97 を開く必要があります。
- コントローラ間 CAPWAP データおよびコントロールトラフィックでは、ポート 5247 および 5264 を開く必要があります。

次の表に、管理および操作目的で使用する必要があるプロトコルおよびポート番号を示します。

表 32: プロトコル/サービスとポート番号

| プロトコル/サービス | ポート番号 |
|------------|-------------------|
| SSH/Telnet | TCP ポート 22 または 29 |
| TFTP | UDP ポート 69 |

| プロトコル/サービス | ポート番号 |
|---------------------|---|
| NTP | UDP ポート 123 |
| SNMP | 取得および設定では UDP ポート 161、トラップでは UDP ポート 162。 |
| HTTPS/HTTP | HTTPS の TCP ポート 443、および HTTP のポート 80 |
| Syslog | TCP ポート 514 |
| Radius Auth/Account | UDP ポート 1812 および 1813 |



(注) 異なるソフトウェアバージョンを持つコントローラ間のモビリティサポート情報については、『[Cisco Wireless Solutions Software Compatibility Matrix](#)』を参照してください。



(注) ファイアウォール上ではポートアドレス変換 (PAT) は実行できません。1対1のネットワークアドレス変換 (NAT) を設定する必要があります。

モビリティグループの設定 (GUI)

ステップ 1 [Controller] > [Mobility Management] > [Mobility Groups] の順に選択して、[Static Mobility Group Members] ページを開きます。

このページでは、[Default Mobility Group] テキストボックスにモビリティグループ名が表示され、現在モビリティグループのメンバである各コントローラの MAC アドレスと IP アドレスが示されます。最初のエントリはローカルコントローラで、これを削除することはできません。

(注) モビリティグループからいずれかのリモートコントローラを削除するには、そのコントローラの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。

ステップ 2 次のいずれかを実行して、コントローラをモビリティグループに追加します。

- コントローラを1つだけ追加する場合、または別々に複数のコントローラを追加する場合、[New] をクリックして進みます。

または

- 複数のコントローラを追加する場合、それらを一括で追加するには、[EditAll] をクリックして進みます。

(注) [EditAll] オプションを使用すると、現在のモビリティグループメンバのすべてのMACアドレスとIPアドレスを入力した後で、すべてのエントリをモビリティグループの1つのコントローラから別のコントローラにコピーして貼り付けることができます。

ステップ3 [New] をクリックして、[Mobility Group Member > New] ページを開きます。

ステップ4 次の手順でコントローラをモビリティグループに追加します。

1 [Member IP Address] テキストボックスに、追加するコントローラの管理インターフェイスのIPアドレスを入力します。

(注) ネットワークアドレス変換 (NAT) が有効になっているネットワークのモビリティグループを設定する際に、コントローラの管理インターフェイスIPアドレスではなく、NATデバイスからコントローラに送信されるIPアドレスを入力します。そうしないと、モビリティグループ内のコントローラ間でモビリティが失敗します。

2 [Member MAC Address] テキストボックスに、追加するコントローラのMACアドレスを入力します。

3 [Group Name] テキストボックスに、モビリティグループ名を入力します。

(注) モビリティグループ名では、大文字と小文字が区別されません。

4 [Hash] テキストボックスに、ピアモビリティコントローラのハッシュキーを入力します。ピアモビリティコントローラは、同じドメイン内の仮想コントローラであることが必要です。

ピアのモビリティコントローラが同じドメイン内の仮想コントローラである場合にだけ、ハッシュを設定する必要があります。

5 [Apply] をクリックして、変更を確定します。新しいコントローラが、[Static Mobility Group Members] ページのモビリティグループメンバのリストに追加されます。

6 [Save Configuration] をクリックして、変更を保存します。

7 **ステップ a** ~ **ステップ e** を繰り返して、すべてのコントローラをモビリティグループに追加します。

8 モビリティグループに追加するすべてのコントローラごとに、この手順を繰り返します。モビリティグループ内のすべてのコントローラでは、他のすべてのモビリティグループメンバのMACアドレスとIPアドレスを設定する必要があります。

[Mobility Group Members > Edit All] ページに現在モビリティグループにあるすべてのコントローラのMACアドレス、IPアドレス、およびモビリティグループ名 (任意) が表示されます。コントローラのリストは、先頭にローカルのコントローラが表示され、1行に1つずつ表示されます。

(注) 必要に応じて、リストのコントローラを編集または削除できます。

ステップ5 次の手順で、さらにコントローラをモビリティグループに追加します。

1 編集ボックス内をクリックして、新たな行を開始します。

2 MACアドレス、管理インターフェイスのIPアドレス、および追加するコントローラのモビリティグループ名を入力します。

(注) これらの値は1行に入力し、1つまたは2つのスペースで区切ってください。

(注) モビリティグループ名では、大文字と小文字が区別されません。

- 3 モビリティグループに追加するコントローラごとに、**ステップ a** および **ステップ b** を繰り返します。
- 4 編集ボックス内のエントリ全体を強調表示して、コピーします。
- 5 [Apply] をクリックして、変更を確定します。新しいコントローラが、[Static Mobility Group Members] ページのモビリティグループメンバのリストに追加されます。
- 6 [Save Configuration] をクリックして、変更を保存します。
- 7 リストをモビリティグループ内の他のすべてのコントローラの [Mobility Group Members > Edit All] ページにあるテキストボックスに貼り付けて、[Apply] と [Save Configuration] をクリックします。

ステップ 6 [Multicast Messaging] を選択して、[Mobility Multicast Messaging] ページを開きます。
現在、設定されているモビリティグループすべての名前がページの中央に表示されます。

ステップ 7 [Mobility Multicast Messaging] ページで、[Enable Multicast Messaging] チェックボックスをオンにすると、Mobile Announce メッセージをモビリティメンバに送信するために、コントローラでマルチキャストモードを使用できるようになります。このチェックボックスをオフにしておくと、Mobile Announce メッセージはユニキャストモードで送信されます。デフォルト値はオフです。

ステップ 8 前の手順でマルチキャストメッセージングを有効化した場合は、[Local Group Multicast IP Address] テキストボックスに、ローカルモビリティグループのマルチキャストグループ IP アドレスを入力します。このアドレスは、マルチキャストモビリティメッセージングに使用されます。

(注) マルチキャストメッセージングを使用するには、ローカルモビリティグループの IP アドレスを設定する必要があります。

ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 必要に応じて、モビリティリスト内にあるローカル以外のグループのマルチキャストグループ IP アドレスを設定することもできます。このためには、ローカル以外のモビリティグループの名前をクリックして、[Mobility Multicast Messaging > Edit] ページを開き、[Multicast IP Address] テキストボックスにローカル以外のモビリティグループのマルチキャストグループ IP アドレスを入力します。

(注) ローカル以外のグループにマルチキャスト IP アドレスが設定されていない場合、コントローラはこのグループのメンバに対して、ユニキャストモードでモビリティメッセージを送信します。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

モビリティグループの設定 (CLI)

ステップ 1 このコマンドを入力して現在のモビリティ設定を確認します。

show mobility summary

ステップ 2 次のコマンドを入力して、新しいモビリティグループを作成します。

config mobility group domain *domain_name*

(注) グループ名には、最大 31 文字の ASCII 文字列を使用できます。大文字と小文字が区別されません。モビリティグループ名には、スペースは使用できません。

ステップ 3 グループメンバを追加するには、次のコマンドを入力します。

config mobility group member add *mac_address ip_address*

(注) ネットワークアドレス変換 (NAT) が有効になっているネットワークのモビリティグループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。そうしないと、モビリティグループ内のコントローラ間でモビリティが失敗します。

(注) グループメンバを削除するには、**config mobility group member delete** *mac_address* コマンドを入力します。

ステップ 4 同じドメイン内の仮想コントローラであるピアモビリティコントローラのハッシュキーを設定するには、次のコマンドを入力します。

config mobility group member hash *peer-ip-address key*

ステップ 5 次のコマンドを入力して、マルチキャストモビリティモードを有効または無効にします。

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

ここで、*local_group_multicast_address* は、ローカルモビリティグループのマルチキャストグループ IP アドレスです。このアドレスは、マルチキャストモビリティメッセージングに使用されます。

マルチキャストモビリティモードを有効にした場合、Mobile Announce メッセージはマルチキャストモードでローカルグループに送信されます。マルチキャストモビリティモードを無効にした場合、Mobile Announce メッセージはユニキャストモードでローカルグループに送信されます。デフォルト値はディセーブルです。

ステップ 6 (任意) モビリティリスト内で、非ローカルグループのマルチキャストグループ IP アドレスを設定することもできます。そのためには、次のコマンドを入力します。

config mobility group multicast-address *group_name IP_address*

ローカル以外のグループにマルチキャスト IP アドレスが設定されていない場合、コントローラはこのグループのメンバに対して、ユニキャストモードでモビリティメッセージを送信します。

ステップ 7 モビリティ設定を確認するには、次のコマンドを入力します。

show mobility summary

ステップ 8 同じドメイン内のモビリティグループメンバのハッシュキーを表示するには、次のコマンドを入力します。

show mobility group member hash

ステップ 9 次のコマンドを入力して、変更を保存します。

save config

- ステップ 10** モビリティグループに追加するすべてのコントローラごとに、この手順を繰り返します。モビリティグループ内のすべてのコントローラでは、他のすべてのモビリティグループメンバの MAC アドレスと IP アドレスを設定する必要があります。
- ステップ 11** モビリティメッセージのマルチキャスト使用のデバッグを有効または無効にするには、次のコマンドを入力します。
- ```
debug mobility multicast {enable | disable}
```
-







# 第 153 章

## モビリティ グループの統計の表示

- [モビリティ グループの統計の表示 \(GUI\) , 1171 ページ](#)
- [モビリティ グループの統計の表示 \(CLI\) , 1173 ページ](#)

### モビリティ グループの統計の表示 (GUI)

**ステップ 1** [Monitor] > [Statistics] > [Mobility Statistics] の順に選択して、[Mobility Statistics] ページを開きます。ここでは、次の内容について説明します。

- Global Mobility Statistics

- [Rx Errors] : 短すぎるパケットや不正な形式などの、一般的なプロトコルパケット受信エラー。
- [Tx Errors] : パケット送信失敗など、一般的なプロトコルパケット送信エラー。
- [Responses Retransmitted] : モビリティプロトコルは UDP を使用し、応答が受信されない場合には、複数回にわたって要求が再送信されます。ネットワークの遅延または処理の遅延のため、応答側が最初に要求に応答した後に、1 回以上の再試行要求を受信する場合があります。このテキストボックスには、応答が再送信された回数が表示されます。
- [Handoff Requests Received] : ハンドオフ要求が受信、無視または応答された合計回数。
- [Handoff End Requests Received] : ハンドオフ終了要求が受信された合計回数。これらの要求は、クライアントセッションの終了について通知するために、アンカーコントローラまたは外部コントローラによって送信されます。
- [State Transitions Disallowed] : ポリシー実行モジュール (PEM) がクライアントの状態の遷移を拒否しました。通常、その結果としてハンドオフが中断されます。
- [Resource Unavailable] : バッファなどの必要なリソースが使用できませんでした。その結果としてハンドオフが中断されます。

- Mobility Initiator Statistics

- [Handoff Requests Sent] : コントローラにアソシエートされ、モビリティグループに通知されているクライアントの数。
- [Handoff Replies Received] : 送信された要求に応答して受信されている、ハンドオフ応答の数。
- [Handoff as Local Received] : クライアントセッション全体が転送されているハンドオフの数。
- [Handoff as Foreign Received] : クライアントセッションが別の場所でアンカーされたハンドオフの数。
- [Handoff Denys Received] : 拒否されたハンドオフの数。
- [Anchor Request Sent] : スリーパーパーティ (外部から外部) ハンドオフ用に送信されたアンカー要求の数。ハンドオフが別の外部コントローラから受信され、新しいコントローラがクライアントを移動させるためのアンカーを要求しています。
- [Anchor Deny Received] : 現在のアンカーによって拒否されたアンカー要求の数。
- [Anchor Grant Received] : 現在のアンカーによって許可されたアンカー要求の数。
- [Anchor Transfer Received] : 現在のアンカー上でセッションを閉じ、要求元にアンカーを送り返したアンカー要求の数。

• Mobility Responder Statistics

- [Handoff Requests Ignored] : コントローラにクライアントが認識されていなかったために無視された、ハンドオフ要求またはクライアント通知の数。
- [Ping Pong Handoff Requests Dropped] : ハンドオフ期間が短すぎた (3 秒) ために拒否されたハンドオフ要求の数。
- [Handoff Requests Dropped] : クライアントについての認識が不完全であるか、パケットの問題が原因でドロップされたハンドオフ要求の数。
- [Handoff Requests Denied] : 拒否されたハンドオフ要求の数。
- [Client Handoff as Local] : クライアントがローカルロールにある間に送信されたハンドオフ応答の数。
- [Client Handoff as Foreign] : クライアントが外部ロールにある間に送信されたハンドオフ応答の数。
- [Anchor Requests Received] : 受信したアンカー要求の数。
- [Anchor Requests Denied] : 拒否されたハンドオフ要求の数。
- [Anchor Requests Granted] : 許可されたアンカー要求の数。
- [Anchor Transferred] : クライアントが外部コントローラから現在のアンカーとして同じサブネット上のコントローラに移動したために、転送されたアンカーの数。

**ステップ 2** 現在のモビリティ統計をクリアする場合は、[Clear Stats] をクリックします。

## モビリティグループの統計の表示 (CLI)

- **show mobility statistics** コマンドを入力して、モビリティグループの統計を参照してください。
- 現在のモビリティ統計をクリアするには、**clear stats mobility** コマンドを入力します。





# 第 154 章

## 自動アンカー モビリティの設定

- [Auto-Anchor モビリティについて](#), 1175 ページ
- [注意事項および制約事項](#), 1176 ページ
- [自動アンカー モビリティの設定 \(GUI\)](#), 1177 ページ
- [自動アンカー モビリティの設定 \(CLI\)](#), 1178 ページ

### Auto-Anchor モビリティについて

無線 LAN 上でローミング クライアントのロード バランシングとセキュリティを向上させるために、自動アンカーモビリティ（ゲスト トンネリングとも呼ばれる）を使用できます。通常のローミング状態では、クライアント デバイスは無線 LAN に join され、最初に接触するコントローラにアンカーされます。クライアントが異なるサブネットにローミングする場合、クライアントのローミング先のコントローラは、クライアント用にアンカー コントローラとの外部セッションを設定します。ただし、自動アンカー モビリティ機能を使用して、無線 LAN 上のクライアントのアンカー ポイントとしてコントローラまたはコントローラのセットを指定できます。

自動アンカー モビリティ モードでは、モビリティ グループのサブセットは WLAN のアンカー コントローラとして指定されます。この機能を使用すると、クライアントのネットワークへのエントリ ポイントに関係なく、WLAN を単一のサブネットに制限できます。それにより、クライアントは企業全体にわたりゲスト WLAN にアクセスできますが、引き続き特定のサブネットに制限されます。WLAN は建物の特定のセクション（ロビー、レストランなど）を表すことができるため、自動アンカー モビリティで地理的ロード バランシングも提供でき、WLAN のホーム コントローラのセットを効果的に作成できます。モバイルクライアントがたまたま最初に接触するコントローラにアンカーされるのではなく、特定の圏内にあるアクセス ポイントを制御するコントローラにモバイルクライアントをアンカーできます。

クライアントが WLAN のモビリティ アンカーとして事前設定されているモビリティ グループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカルセッションが作成されます。クライアントは、WLAN の事前設定されたアンカー コントローラにのみアンカーできます。指定された WLAN の場合、モ

ビリティグループのすべてのコントローラ上で同じセットのアンカーコントローラを設定する必要があります。

クライアントが WLAN のモビリティアンカーとして設定されていないモビリティグループのコントローラに最初にアソシエートすると、クライアントはローカルでそのコントローラにアソシエートし、クライアントのローカルセッションが作成され、そのクライアントがモビリティリスト内の別のコントローラに通知されます。その通知に対する回答がない場合、コントローラは WLAN に設定されたいずれかのアンカーコントローラに連絡をとり、ローカルスイッチ上のクライアントに対する外部セッションを作成します。クライアントからのパケットは EtherIP を使用してモビリティトンネルを介してカプセル化され、アンカーコントローラに送信されます。ここでカプセルを解除されて有線ネットワークへ配信されます。クライアントへのパケットは、アンカーコントローラで受信され、EtherIP を使用してモビリティトンネルを介して外部コントローラへ転送されます。外部コントローラはパケットのカプセルを解除し、クライアントへ転送します。

外部コントローラ上の特定の WLAN に複数のコントローラがモビリティアンカーとして追加されている場合、外部コントローラは IP アドレスでコントローラを内部的にソートします。最小 IP アドレスのコントローラは、最初のアンカーです。たとえば、通常の順序付きリストは、172.16.7.25、172.16.7.28、192.168.5.15 です。最初のクライアントが、外部コントローラのアンカーされた WLAN にアソシエートされている場合、クライアントのデータベースエントリはリストの最初のアンカーコントローラに送信され、2 番目のクライアントはリストの 2 番目のコントローラに送信され、アンカーリストの最後に到達するまで同様に送信されます。プロセスは最初のアンカーコントローラから始まり、繰り返されます。いずれかのアンカーコントローラがダウンしていることが検出された場合、そのコントローラにアンカーされているクライアントが認証解除され、クライアントはアンカーリスト内の残りのコントローラについてラウンドロビン方式で認証/アンカープロセスを処理します。この機能は、モビリティフェールオーバーによって通常のモビリティクライアントにも使用されます。この機能によって、モビリティグループのメンバは到着不能なメンバを検出してクライアントを再ルーティングできます。

## 注意事項および制約事項

- モビリティリストのメンバ同士が ping 要求をお互いに送信し合い、データを確認してそのデータのパスを管理することで、到着不能なメンバがないかを調べてクライアントを再ルーティングできます。それぞれのアンカーコントローラに送信する ping 要求の数と間隔は、設定可能です。この機能には、ゲストトンネリングのほか、通常のモビリティでモビリティフェールオーバーを実行できるよう、ゲスト N+1 冗長性が備わっています。
- コントローラを WLAN のモビリティアンカーとして指定するには、そのコントローラをモビリティグループメンバリストに追加する必要があります。
- WLAN のモビリティアンカーとして、複数のコントローラを設定できます。
- 自動アンカーモビリティは、Web 認証をサポートしていますが、その他のレイヤ 3 セキュリティタイプをサポートしていません。
- 外部コントローラ上の WLAN とアンカーコントローラ上の WLAN は、両方ともモビリティアンカーを使用して設定する必要があります。アンカーコントローラ上で、アンカーコン

コントローラ自体をモビリティ アンカーとして設定します。外部コントローラ上で、アンカーをモビリティ アンカーとして設定します。

- 自動アンカー モビリティは、DHCP オプション 82 と共には使用できません。
- ゲスト N+1 冗長性とモビリティ フェールオーバー機能にファイアウォールを組み合わせる使用の場合は、次のポートに空きがあることを確認してください。
  - UDP 16666 : トンネル コントロール トラフィック用
  - IP プロトコル 97 : ユーザのデータ トラフィック用
  - UDP 161 および 162 : SNMP
- アンカー コントローラと外部モビリティ間でローミングする場合、アンカー コントローラで認識されたクライアントは外部コントローラに表示されます。外部コントローラをチェックして、RA スロットル統計を表示する必要があります。
- レイヤ 3 RADIUS 認証の場合、認証の RADIUS 要求は、アンカー コントローラによって送信されます。
- モビリティ アンカーは仮想ワイヤレス LAN コントローラでサポートされていません。

## 自動アンカー モビリティの設定 (GUI)

- ステップ 1** モビリティ グループ内に到着不能なアンカー コントローラがないかを検出するには、次の手順でコントローラを設定してください。
- a) [Controller] > [Mobility Management] > [Mobility Anchor Config] の順に選択して、[Mobility Anchor Config] ページを開きます。
  - b) [Keep Alive Count] テキスト ボックスに、そのアンカーが到着不能と判断するまでにアンカー コントローラに ping 要求を送信する回数を入力します。有効な範囲は 3 ~ 20 で、デフォルト値は 3 です。
  - c) [Keep Alive Interval] テキスト ボックスには、アンカー コントローラに送信する各 ping 要求の間隔を秒単位で入力します。有効な範囲は 1 ~ 30 秒で、デフォルト値は 10 秒です。
  - d) [DSCP Value] テキスト ボックスに、DSCP 値を入力します。デフォルト値は 0 です。
  - e) [Apply] をクリックして、変更を確定します。
- ステップ 2** [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 3** 目的の WLAN または有線ゲスト LAN の青いドロップダウン矢印をクリックして、[Mobility Anchors] を選択します。[Mobility Anchors] ページが表示されます。
- このページには、すでにモビリティアンカーとして設定されているコントローラが一覧表示されるほか、そのデータと管理パスの現状が表示されます。モビリティグループ内のコントローラは、well-known UDP ポート上でお互いに通信し合い、Ethernet-over-IP (EoIP) トンネルを通じてデータ トラフィックを交換します。mping を送信して、モビリティ制御パケットの到着可能性を管理インターフェイスのモビリティ UDP ポート 16666 によってテストします。また、eping を送信して、モビリティデータ トラフィックを管理インターフェイスの EoIP ポート 97 によってテストします。[Control Path] テキスト ボックスは、mping

が成功した (up) か失敗した (down) かを表示します。[Data Path] テキストボックスは、eping が成功した (up) か失敗した (down) かを表示します。[Data Path] テキストボックスまたは [Control Path] テキストボックスに「down」が表示された場合は、モビリティアンカーが到着できず、接続できないと考えられます。

- ステップ 4** モビリティアンカーに指定されたコントローラの IP アドレスを、[Switch IP Address (Anchor)] ドロップダウンリストで選択します。
- ステップ 5** [Mobility Anchor Create] をクリックします。選択したコントローラが、この WLAN または有線ゲスト LAN のアンカーになります。
- (注) WLAN または有線ゲスト LAN のモビリティアンカーを削除するには、アンカーの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- ステップ 6** [Save Configuration] をクリックします。
- ステップ 7** ステップ 4 およびステップ 6 を繰り返し、他のコントローラをこの WLAN または有線ゲスト LAN のモビリティアンカーとして設定します。
- ステップ 8** モビリティグループのすべてのコントローラに同じセットのモビリティアンカーを設定します。

## 自動アンカー モビリティの設定 (CLI)

- コントローラは、到着不能なモビリティリストメンバを常に検出するようにプログラムされます。モビリティメンバ間で ping を交換するためのパラメータを変更するには、次のコマンドを入力します。
  - **config mobility group keepalive count count** : そのメンバが到着不能と判断されるまでにモビリティリストメンバに送信する ping 要求の回数。有効な範囲は 3 ~ 20 で、デフォルト値は 3 です。
  - **config mobility group keepalive interval seconds** : モビリティリストメンバに送信する各 ping 要求の間隔 (秒単位)。有効な範囲は 1 ~ 30 秒で、デフォルト値は 10 秒です。
- モビリティアンカーを設定している WLAN または有線ゲスト LAN を無効にするには、次のコマンドを入力します。
 

```
config {wlan | guest-lan} disable {wlan_id | guest_lan_id}
```
- WLAN または有線ゲスト LAN の新しいモビリティアンカーを作成するには、次のコマンドのいずれかを入力します。
  - **config mobility group anchor add {wlan | guest-lan} {wlan\_id | guest\_lan\_id} anchor\_controller\_ip\_address**
  - **config {wlan | guest-lan} mobility anchor add {wlan\_id | guest\_lan\_id} anchor\_controller\_ip\_address**





(注) *wlan\_id* または *guest\_lan\_id* は、存在しているが無効になっており、*anchor\_controller\_ip\_address* は、デフォルトのモビリティグループのメンバーである必要があります。



(注) 1 つ目のモビリティアンカーを設定するときに、WLAN または有線ゲスト LAN で自動アンカー モビリティを有効にします。

- WLAN または有線ゲスト LAN のモビリティアンカーを削除するには、次のコマンドのいずれかを入力します。

- **config mobility group anchor delete {wlan | guest-lan} {wlan\_id | guest\_lan\_id} anchor\_controller\_ip\_address**
- **config {wlan | guest-lan} mobility anchor delete {wlan\_id | guest\_lan\_id} anchor\_controller\_ip\_address**



(注) *wlan\_id* または *guest\_lan\_id* は必ず指定し、無効にする必要があります。



(注) 最後のアンカーを削除すると、自動アンカー モビリティ機能は無効になり、新しいアソシエーションに対しては標準のモビリティが再度使用されるようになります。

- 次のコマンドを入力して、設定を保存します。

**save config**

- 特定の WLAN または有線ゲスト LAN のモビリティアンカーとして設定されたコントローラのリストとステータスを表示するには、次のコマンドを入力します。

**show mobility anchor {wlan | guest-lan} {wlan\_id | guest\_lan\_id}**



(注) *wlan\_id* パラメータと *guest\_lan\_id* パラメータはオプションであり、リストを特定の WLAN またはゲスト LAN のアンカーに制限します。システムのすべてのモビリティアンカーを表示するには、**show mobility anchor** コマンドを入力します。

[Status] テキスト ボックスには、次のうちいずれかの値が表示されます。

UP : コントローラはアクセス可能で、データを渡すことができます。

CNTRL\_PATH\_DOWN : mpings に失敗しました。コントロールパス経由でコントローラにアクセスできないため、エラーが発生したと見なされます。

DATA\_PATH\_DOWN : epings に失敗しました。コントローラにアクセスできないため、エラーが発生したと見なされます。

CNTRL\_DATA\_PATH\_DOWN : mpings および epings の両方に失敗しました。コントローラにアクセスできないため、エラーが発生したと見なされます。

- すべてのモビリティ グループ メンバのステータスを確認するには、次のコマンドを入力します。

#### **show mobility summary**

- モビリティの問題のトラブルシューティングを行うには、次のコマンドを入力します。
  - **debug mobility handoff {enable | disable}** : モビリティのハンドオフの問題をデバッグします。
  - **debug mobility keep-alive {enable | disable} all** : すべてのモビリティアンカーの keepalive パケットをダンプします。
  - **debug mobility keep-alive {enable | disable} IP\_address** : 特定のモビリティアンカーの keepalive パケットをダンプします。



# 第 155 章

## WLAN モビリティ セキュリティの値の検証

- [WLAN モビリティ セキュリティの値について, 1181 ページ](#)

### WLAN モビリティ セキュリティの値について

すべてのアンカーまたはモビリティのイベントでは、各コントローラの WLAN セキュリティ ポリシーの値は一致する必要があります。これらの値はコントローラのデバッグで検証することができます。次の表に、WLAN モビリティ セキュリティの値と対応するセキュリティ ポリシーを示します。

表 33: WLAN モビリティ セキュリティの値

セキュリティの 16 進数値	セキュリティ ポリシー
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*

セキュリティの 16 進数値	セキュリティ ポリシー
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed (注) ソフトウェア リリース 6.0 以降を実行しているコントローラは、このセキュリティ ポリシーをサポートしていません。
0x00001000	Security_Web_Passthrough



# 第 156 章

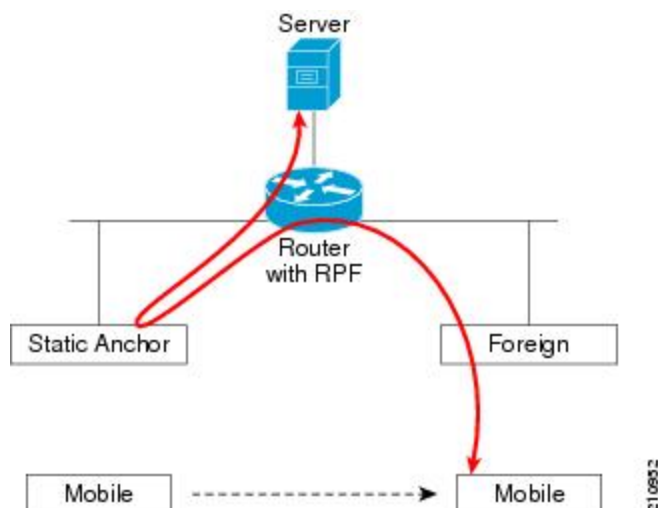
## シンメトリック モビリティ トンネリングの 使用

- [シンメトリック モビリティ トンネリングについて](#), 1183 ページ
- [注意事項および制約事項](#), 1184 ページ
- [シンメトリック モビリティ トンネリングの確認 \(GUI\)](#), 1184 ページ
- [シンメトリック モビリティ トンネリングが有効な場合の確認 \(CLI\)](#), 1184 ページ

### シンメトリック モビリティ トンネリングについて

シンメトリック モビリティ トンネリングが有効になっている場合、すべてのクライアントトラフィックがアンカー コントローラへ送信されるため、RPF チェックを問題なく通過します。

図 78: シンメトリック モビリティ トンネリングまたは双方向性トンネリング



シンメトリック モビリティ トンネリングは、次の場合にも便利です。

- 送信元 IP アドレスがパケットの受信先サブネットと一致しないため、クライアント パケットパス内のファイアウォールでパケットがドロップされる場合。
- アンカー コントローラ上のアクセス ポイント グループの VLAN が外部コントローラ上の WLAN インターフェイス VLAN と異なる場合。この場合、モビリティ イベント中に、クライアント トラフィックが誤った VLAN に送信される可能性があります。

## 注意事項および制約事項

- シンメトリック モビリティ トンネリングはデフォルトで有効です。

## シンメトリック モビリティ トンネリングの確認 (GUI)

**ステップ 1** [Controller] > [Mobility Management] > [Mobility Anchor Config] の順に選択して、[Mobility Anchor Config] ページを開きます。

**ステップ 2** [Symmetric Mobility Tunneling Mode] テキスト ボックスに [Enabled] と表示されます。

## シンメトリック モビリティ トンネリングが有効な場合の確認 (CLI)

次のコマンドを入力して、シンメトリック モビリティ トンネリングが有効であることを確認します。

**show mobility summary**



# 第 157 章

## モビリティ ping テストの実行

- [モビリティ ping テストについて, 1185 ページ](#)
- [注意事項および制約事項, 1185 ページ](#)
- [モビリティ ping テストの実行 \(CLI\) , 1186 ページ](#)

### モビリティ ping テストについて

1つのモビリティリスト内のコントローラは、well-known UDP ポート上で情報を制御し、Ethernet-over-IP (EoIP) トンネルを通じてデータトラフィックを交換することにより、お互いに通信します。UDP と EoIP は信頼できる転送メカニズムではないため、モビリティコントロールパケットまたはデータパケットがモビリティピアに配信される保証はありません。ファイアウォールによる UDP ポートや EoIP パケットのフィルタリング、あるいはルーティングの問題のために、モビリティパケットが転送中に消失する可能性があります。

### 注意事項および制約事項

コントローラソフトウェアリリース 4.0 以降を使用すると、モビリティ ping テストを実行することにより、モビリティ通信環境をテストできます。これらのテストを使用して、モビリティグループ（ゲストコントローラを含む）のメンバ間の接続を検証できます。次の 2 つの ping テストが利用できます。

- **UDP でのモビリティ ping** : このテストは、モビリティ UDP ポート 16666 上で実行されます。このテストでは、管理インターフェイスを介してモビリティ制御パケットが到達できるかどうかを確認します。
- **EoIP でのモビリティ ping** : このテストは EoIP 上で実行されます。管理インターフェイス上で、モビリティデータトラフィックをテストします。

各コントローラにつき、実行できるモビリティ ping テストは 1 度に 1 回だけです。



(注) これらの ping テストは、インターネット制御メッセージプロトコル (ICMP) ベースではありません。「ping」という用語は、エコー要求とエコー応答メッセージを示すために使用されます。



(注) ICMP パケットが 1280 バイトより大きい場合は、常に応答には 1280 バイトに切り詰められたパケットが使用されます。たとえば、ホストから管理インターフェイスに 1280 バイトを超えるパケットを使用して ping すると、常に 1280 バイトに切り詰められたパケットが使用されます。

## モビリティ ping テストの実行 (CLI)

- 2つのコントローラ間でモビリティ UDP コントロール パケット通信をテストするには、次のコマンドを入力します。

**mping mobility\_peer\_IP\_address**

*mobility\_peer\_IP\_address* パラメータは、モビリティ リストに属するコントローラの IP アドレスにする必要があります。

- 2つのコントローラ間でモビリティ EoIP データ パケット通信をテストするには、次のコマンドを入力します。

**eping mobility\_peer\_IP\_address**

*mobility\_peer\_IP\_address* パラメータは、モビリティ リストに属するコントローラの IP アドレスにする必要があります。

- モビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

**config logging buffered debugging**

**show logging**

UDP でのモビリティ ping に対するコントローラのトラブルシューティングを行うには、次のコマンドを入力します。

**debug mobility handoff enable**



(注) トラブルシューティングを行う際には、Ethereal トレース キャプチャを使用することをお勧めします。





## 第 158 章

# 固定 IP アドレスを持つクライアントのダイナミック アンカーの設定

- [固定 IP を持つクライアントのダイナミック アンカーについて, 1187 ページ](#)
- [注意事項および制約事項, 1188 ページ](#)
- [固定 IP クライアントのダイナミック アンカーの設定 \(GUI\) , 1189 ページ](#)
- [固定 IP クライアントのダイナミック アンカーの設定 \(CLI\) , 1189 ページ](#)

## 固定 IP を持つクライアントのダイナミック アンカーについて

ワイヤレス クライアントの固定 IP アドレスを設定する場合があります。これらのワイヤレス クライアントをネットワーク内で移動するときは、他のコントローラへのアソシエイトを試みることができました。クライアントが、固定 IP と同じサブネットをサポートしないコントローラにアソシエイトしようとする、クライアントはネットワーク接続に失敗します。固定 IP アドレスを持つクライアントのダイナミック トンネリングを有効にできるようになりました。

固定 IP アドレスを使用した固定 IP クライアントのダイナミック アンカーは、クライアントのサブネットが同じモビリティグループ内の別のコントローラへのトラフィックをトンネリングすることによってサポートされている、他のコントローラにアソシエイトすることができます。この機能により、クライアントが固定 IP アドレスを使用しているにもかかわらずネットワークが処理されるように WLAN を設定できます。

## 固定 IP クライアントのダイナミック アンカーの機能

次の一連の手順は、固定 IP アドレスを使用してクライアントがコントローラにアソシエイトしようとするときに実行されます。

- 1 クライアントがコントローラ、たとえば WLC-1 にアソシエイトすると、モビリティ アナウンスを行います。モビリティグループ内のコントローラが応答した場合（たとえば WLC-2）、クライアントトラフィックがコントローラ WLC-2 にトンネリングされます。結果として、コントローラ WLC 1 が外部コントローラとなり、WLC-2 がアンカー コントローラとなります。

- 2 コントローラが応答しない場合、クライアントはローカルクライアントとして処理され、認証が実行されます。クライアントのIPアドレスは孤立したパケットの処理またはARP要求の処理のいずれかによって更新されます。クライアントのIPサブネットがコントローラ（WLC-1）でサポートされていない場合、WLC-1は別のスタティックIPのモバイルアナウンスを送信し、クライアントのサブネットをサポートするコントローラ（たとえばWLC-3）がそのアナウンスに回答した場合、クライアントトラフィックはコントローラWLC-3にトンネリングされます。結果として、コントローラWLC-1がエクスポート外部コントローラとなり、WLC-3がエクスポートアンカーコントローラとなります。
- 3 確認が受信されると、クライアントトラフィックがアンカーとコントローラ（WLC-1）間でトンネリングされます。



(注) WLANをインターフェイスグループで設定し、インターフェイスグループ内のいずれかのインターフェイスが固定IPクライアントサブネットをサポートしている場合、クライアントはそのインターフェイスに割り当てられます。この状況は、ローカルまたはリモート（固定IPアンカー）で発生します。



(注) セキュリティレベル2認証は、ローカル（固定IP外部）コントローラでのみ実行されます。これは、エクスポート外部コントローラとも呼ばれます。

## 注意事項および制約事項

- 固定IPトンネリングのAAAを実行する場合、上書きしたインターフェイスを設定しないでください。上書きしたインターフェイスがクライアントサブネットをサポートしていない場合、トラフィックがクライアントに対してブロックされることがあるためです。これが可能になるのは、上書きインターフェイスグループがクライアントサブネットをサポートする極端な場合です。
- ローカルコントローラは、このクライアントエントリが存在する正しいAAAサーバに設定する必要があります。

次の制限事項は、同じWLANで固定IPトンネリングに他の機能を設定する場合に適用されます。

- 自動アンカーモビリティ（ゲストトンネリング）は同じWLANに設定できません。
- FlexConnectローカル認証は同じWLANに設定できません。
- DHCP Requiredオプションは、同じWLANに設定できません。
- FlexConnectローカルスイッチングでは、固定IPクライアントのダイナミックアンカーを設定できません。

## 固定 IP クライアントのダイナミック アンカーの設定 (GUI)

- 
- ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。
- ステップ 2 IP クライアントのダイナミック アンカーを有効にする WLAN の ID 番号をクリックします。[WLANs > Edit] ページが表示されます。
- ステップ 3 [Advanced] タブを選択して、[WLANs > Edit] ([Advanced]) ページを開きます。
- ステップ 4 [Static IP Tunneling] チェックボックスをオンして、固定 IP クライアントのダイナミック アンカリングを有効にします。
- ステップ 5 [Apply] をクリックして、変更を確定します。
- 

## 固定 IP クライアントのダイナミック アンカーの設定 (CLI)

**config wlan static-ip tunneling {enable | disable} wlan\_id** : 指定した WLAN 上で固定 IP クライアントのダイナミック アンカーを有効または無効にします。

固定 IP を使用したクライアントのコントローラをモニタし、トラブルシューティングを行うには、次のコマンドを使用します。

- **show wlan wlan\_id** : 固定 IP クライアント機能のステータスを表示できるようにします。

```
.....
Static IP client tunneling..... Enabled
.....
```

- **debug client client-mac**
- **debug dot11 mobile enable**
- **debug mobility handoff enable**





# 第 159 章

## 外部マッピングの設定

---

- [外部マッピングについて](#), 1191 ページ
- [外部コントローラの MAC マッピングの設定 \(GUI\)](#), 1191 ページ
- [外部コントローラの MAC マッピングの設定 \(CLI\)](#), 1191 ページ

### 外部マッピングについて

外部マッピングとも呼ばれる自動アンカー モビリティを使用して、別の外部コントローラ上のユーザを別の物理ロケーションから設定し、それらの物理ロケーションに基づいてサブネットまたはサブネット・グループから IP アドレスを取得できます。

### 外部コントローラの MAC マッピングの設定 (GUI)

---

- ステップ 1** [WLANS] タブを選択します。  
[WLANS] ページが表示され、使用可能な WLAN のリストが表示されます。
- ステップ 2** 目的の WLAN の青いドロップダウン矢印をクリックして、[Foreign-Maps] を選択します。  
外部のマッピングのページが表示されます。このページには、モビリティグループ内およびインターフェイスグループ内の外部コントローラの MAC アドレスもリスト表示されます。
- ステップ 3** 目的の外部コントローラ MAC、およびマッピングする必要があるインターフェイスまたはインターフェイスグループを選択し、[Add Mapping] をクリックします。
- 

### 外部コントローラの MAC マッピングの設定 (CLI)

- 外部コントローラのマッピングを追加するには、次のコマンドを入力します。

```
config wlan mobility foreign-map add wlan-id foreign_ctlr_mac interface/interface_grp name
```



# 第 160 章

## プロキシ モバイル IPv6 の設定

- [プロキシ モバイル IPv6 について, 1193 ページ](#)
- [プロキシ モバイル IPv6 の制約事項, 1194 ページ](#)
- [プロキシ モバイル IPv6 の設定 \(GUI\) , 1194 ページ](#)
- [プロキシ モバイル IPv6 の設定 \(CLI\) , 1197 ページ](#)

### プロキシ モバイル IPv6 について

プロキシ モバイル IPv6 (PMIPv6) は、任意の IP モビリティ関連シグナリングでモバイル ノードのプロキシとして動作することによってモバイルノードをサポートする、ネットワークベースのモバイル管理プロトコルです。ネットワークのモビリティ エンティティは、モバイル ノードの移動を追跡し、モビリティ シグナリングを起動して必要なルーティング状態を設定します。

主要な機能エンティティは Local Mobility Anchor (LMA) とモバイルアクセス ゲートウェイ (MAG) です。LMA はモバイル ノードの到達可能性状態を維持し、モバイル ノードの IP アドレス用のトポロジアンカー ポイントです。MAG はモバイル ノードの代わりにモビリティ管理を行います。MAG はモバイル ノードがアンカーされているアクセスリンクに存在します。コントローラは MAG 機能を実装します。

Cisco 5500 シリーズ、Cisco WiSM2、および Cisco 8500 シリーズ コントローラの場合、PMIPv6 MAG はセルラー データ ネットワークの Cisco ASR 5000 シリーズなどの LMA との統合をサポートします。

PMIPv6 クライアントの場合、Cisco WLC は中央 Web 認証およびローカル Web 認証の両方をサポートします。

PMIPv6 は 802.1X 認証を使用するクライアントでサポートされています。802.1X 認証が完了すると、Cisco AP はクライアントに対して PMIPv6 シグナリングを開始します。

AP の MAG は、ローカルにスイッチされる WLAN の FlexConnect モードの AP でサポートされています。PMIPv6 クライアントの場合、クライアントからのすべてのデータ トラフィックは、MAG と LMA の間に確立された総称ルーティング カプセル化 (GRE) トンネルで LMA にトンネ

リングされます。同様に、GRE トンネルで LMA から受信したすべてのパケットは、ワイヤレスクライアントに転送されます。

### 高速ローミング

高速ローミングは、中央アソシエーションが WLAN で有効な場合にサポートされます。中央アソシエーションが有効な場合、すべてのキー キャッシングは Cisco WLC で発生します。PMIPv6 クライアントが 1 つの AP から同じモビリティ ドメインの別の AP にローミングするとき、Cisco WLC はクライアントの PMIPv6 パラメータを PMIPv6 トンネル ペイロードで新しい AP に送信して、PMIPv6 シグナリングを開始します。また、Cisco WLC は PMIPv6 トンネル ペイロードを古い AP に送信して、LMA を持つクライアント用の総称ルーティング カプセル化 (GRE) トンネルを切断します。高速ローミングは、Cisco WLC 内および Cisco WLC 間の両方のローミングシナリオでサポートされ、ローミング中に Cisco WLC 間で PMIPv6 パラメータを送信するためにモビリティ メッセージが追加されます。

サードパーティの MAG からシスコの AP-MAG へのクライアントローミングは新しいクライアントの join に似ています。シスコの AP-MAG からサードパーティの MAG へのクライアントローミングはクライアントの退出と同様なので特別な処理は必要ありません。

## プロキシ モバイル IPv6 の制約事項

- IPv6/dual スタック クライアントはサポートされません。IPv6 クライアントはサポートされません。WLAN が PMIPv6 に対してマークされている場合、クライアントの IPv6 アドレスは学習されません。
- PMIPv6 は、FlexConnect モードの AP があるローカル スイッチング WLAN ではサポートされません。ただし、AP の MAG はこのシナリオでサポートされています。
- スプリット トンネリングはサポートされていません。
- コントローラ間のローミングは、PMIPv6 が有効になっている WLAN でのみサポートされません。

## プロキシ モバイル IPv6 の設定 (GUI)

**ステップ 1** [Controller] > [PMIPv6] > [General] の順に選択して、[PMIPv6 General] ページを開きます。

**ステップ 2** 次のパラメータの値を入力します。

- MAG APN : アクセス ポイント名 (APN) (MAG に接続している場合)。

MAG は次の 4 種類のロールのいずれかに設定できます。

- 3gpp : 3GPP (Third Generation Partnership Project standard) としてロールを指定します。
- lte : LTE (Long Term Evolution standard) としてロールを指定します。



- **wimax** : WIMAX (Worldwide Interoperability for Microwave Access standard) としてロールを指定します。
- **wlan** : WLAN (ワイヤレス LAN) としてロールを指定します。

デフォルトでは、MAG ロールは WLAN です。ただし、Lightweight アクセス ポイントの場合、MAG ロールは 3GPP に設定する必要があります。MAG ロールが 3GPP の場合、MAG の APN を指定する必要があります。

- **[Maximum Bindings Allowed]** : コントローラが MAG に送信できるバインディング アップデートの最大数。有効な範囲は 0 ~ 40000 です。
- **[Binding Lifetime]** : コントローラのバインディング エントリのライフタイム。有効な範囲は 10 ~ 65535 秒です。デフォルト値は 3600 です。バインディング ライフタイムは 4 秒の倍数であることが必要です。
- **[Binding Refresh Time]** : コントローラのバインディング エントリのリフレッシュ時間。有効な範囲は 4 ~ 65535 秒です。デフォルト値は 300 秒です。バインディング リフレッシュ時間は 4 秒の倍数であることが必要です。
- **[Binding Initial Retry Timeout]** : コントローラがプロキシバインディング確認 (PBA) を受信しない場合のプロキシバインディング アップデート (PBU) 間の初期タイムアウト。有効な範囲は 100 ~ 65535 秒です。デフォルト値は 1000 秒です。
- **[Binding Maximum Retry Timeout]** : コントローラがプロキシバインディング確認 (PBA) を受信しない場合のプロキシバインディング アップデート (PBU) 間の最大タイムアウト。有効な範囲は 100 ~ 65535 秒です。デフォルト値は 32000 秒です。
- **[Replay Protection Timestamp]** : 受信したプロキシバインディング確認のタイムスタンプと現在の日時との時間差の上限。有効範囲は 1 ~ 255 ミリ秒です。デフォルト値は 7 ミリ秒です。
- **[Minimum BRI Retransmit Timeout]** : コントローラが BRI メッセージを再送信するまでに待機する時間の最小値。有効な範囲は 500 ~ 65535 秒です。デフォルト値は 1000 秒です。
- **[Maximum BRI Retransmit Timeout]** : コントローラが Binding Revocation Indication (BRI) メッセージを再送信するまでに待機する時間の最大値。有効な範囲は 500 ~ 65535 秒です。デフォルト値は 2000 秒です。
- **[BRI Retries]** : コントローラが Binding Revocation Acknowledgment (BRA) メッセージを受信する前に BRI メッセージを再送信する最大回数。有効な範囲は 1 ~ 10 です。デフォルト値は、1 です

**ステップ 3** [Apply] をクリックします。

設定をクリアするには、[Clear Domain] をクリックします。

**ステップ 4** LMA を作成するには、次の手順に従います。

- a) [Controll] > [PMIPv6] > [LMA] を順に選択し、[New] をクリックします。
- b) 次のパラメータの値を入力します。

- **[Member Name]** : コントローラに接続された LMA の名前。

- [Member IP Address] : コントローラに接続された LMA の IP アドレス。

c) [Apply] をクリックします。

**ステップ 5** PMIPv6 プロファイルを作成するには、次の手順を実行します。

- [Controll] > [PMIPv6] > [Profiles] を順に選択し、[New] をクリックします。
- [PMIPv6 Profile > New] ページで、次のパラメータの値を入力します。

- [Profile Name] : プロファイルの名前。
- [Network Access Identifier] : プロファイルにアソシエートされたネットワーク アクセス識別子 (NAI) の名前。
- [LMA Name] : プロファイルのアソシエートする LMA の名前。
- [Access Point Node] : コントローラに接続されているアクセス ポイント ノードの名前。

c) [Apply] をクリックします。

**ステップ 6** [PMIPv6 Profile > New] ページで、次のパラメータの値を入力します。

- [Profile Name] : プロファイルの名前。
- [Network Access Identifier] : プロファイルにアソシエートされたネットワーク アクセス識別子 (NAI) の名前。
- [LMA Name] : プロファイルのアソシエートする LMA の名前。
- [Access Point Node] : コントローラに接続されているアクセス ポイント ノードの名前。

**ステップ 7** WLAN の PMIPv6 パラメータを設定するには、次の手順に従います。

- [WLANs] > [WLAN ID] の順に選択して、[WLANs > Edit] ページを開きます。
- [Advanced] タブをクリックします。
- [PMIP] の [PMIP Mobility Type] ドロップダウン リストで、モビリティ タイプを次のオプションから選択します。
  - [None] : 簡易 IP を使用して WLAN を設定します
  - [PMIPv6] : PMIPv6 だけを使用して WLAN を設定します
- [PMIP Profile] ドロップダウン リストから、WLAN の PMIP プロファイルを選択します。
- [PMIP Realm] ボックスに、WLAN のデフォルト レルムを入力します。
- [Apply] をクリックします。

**ステップ 8** [Save Configuration] をクリックします。

## プロキシ モバイル IPv6 の設定 (CLI)

**ステップ 1** 次のコマンドを使用して MAG を設定します。

- 次のコマンドを入力して、許可される最大バインディング アップデート エントリを設定します。  
**config pmipv6 mag binding maximum *units***
- 次のコマンドを入力して、バインディング エントリのライフタイムを設定します。  
**config pmipv6 mag lifetime *units***
- 次のコマンドを入力して、バインディング リフレッシュ 間隔を設定します。  
**config pmipv6 mag refresh-time *units***
- 次のコマンドを入力して、PBA が到着しない場合の PBU 間の初期タイムアウトを設定します。  
**config pmipv6 mag init-retx-time *units***
- 次のコマンドを入力して、PBA が到着しない場合の PBU 間の最大初期タイムアウトを設定します。  
**config pmipv6 mag max-retx-time *units***
- 次のコマンドを入力して、リプレイ保護メカニズムを設定します。  
**config pmipv6 mag replay-protection {*timestamp window units* | *sequence-no* | *mobile-node-timestamp*}**
- 次のコマンドを入力して、binding revocation indication (BRI) メッセージを再送信する前に MAG が待機する最小時間または最大時間を秒単位で設定します。  
**config pmipv6 mag bri delay {*min* | *max*} *units***
- 次のコマンドを入力して、binding revocation acknowledgment (BRA) メッセージを受信する前に、MAG が BRI メッセージを再送信する最大回数を設定します。  
**config pmipv6 mag bri retries *units***
- 次のコマンドを入力して、MAG の LMA リストを設定します。  
**config pmipv6 mag lma *lma-name* *ipv4-address ip-address***
- 次のコマンドを入力して、MAG のアクセス ポイント名 (APN) を追加します。  
**config pmipv6 mag apn *apn-name***

MAG は次の 4 種類のロールのいずれかに設定できます。

- **3gpp** : 3GPP (Third Generation Partnership Project standard) としてロールを指定します。
- **lte** : LTE (Long Term Evolution standard) としてロールを指定します。
- **wimax** : WIMAX (Worldwide Interoperability for Microwave Access standard) としてロールを指定します。
- **wlan** : WLAN (ワイヤレス LAN) としてロールを指定します。

デフォルトでは、MAG ロールは WLAN です。ただし Lightweight アクセス ポイントの場合、MAG ロールは 3GPP に設定する必要があります。MAG ロールが 3GPP の場合、MAG の APN を指定する必要があります。

- 次のコマンドを入力して、APN を削除します。

```
config pmipv6 delete mag apn apn-name
```

**ステップ 2** 次のコマンドを入力して、PMIPv6 ドメイン名を設定します。

```
config pmipv6 domain domain-name
```

(注) このコマンドは、コントローラの MAG 機能も有効にします。

**ステップ 3** 次のコマンドを入力して、PMIPv6 ドメインにプロファイルを追加します。

```
config pmipv6 add profile profile-name nai {user@realm | @realm | *} lma lma-name apn apn-name
```

(注) NAI はネットワーク アクセス識別子を意味します。APN はアクセス ポイント名を意味します。

**ステップ 4** 次のコマンドを入力して、PMIPv6 エンティティを削除します。

```
config pmipv6 delete {domain domain-name | lma lma-name | profile profile-name nai {user@realm | @realm | *}}
```

**ステップ 5** 次のコマンドを使用して、WLAN の PMIPv6 パラメータを設定します。

- 次のコマンドを入力して、WLAN のデフォルト レalmを設定します。

```
config wlan pmipv6 default-realm {realm-name | none} wlan-id
```

- 次のコマンドを入力して、1 つまたはすべての WLAN のモビリティ タイプを設定します。

```
config wlan pmipv6 mobility-type {none | pmipv6} {wlan-id | all}
```

- 次のコマンドを入力して、PMIPv6 WLAN のプロファイル名を設定します。

```
config wlan pmipv6 profile-name name wlan-id
```

**ステップ 6** 次のコマンドを入力して、変更を保存します。

```
save config
```

**ステップ 7** 次の **show** コマンドを使用して、PMIPv6 設定の詳細を表示します。

- 次のコマンドを入力して、PMIPv6 ドメインのプロファイルの詳細を表示します。

```
show pmipv6 domain domain-name profile profile-name
```

- 次のコマンドを入力して、すべての PMIPv6 プロファイルの要約を表示します。

```
show pmipv6 profile summary
```

- 次のコマンドを入力して、MAG の PMIPv6 に関するグローバル情報を表示します。

```
show pmipv6 mag globals
```

- 次のコマンドを入力して、LMA または NAI の MAG バインディングに関する情報を表示します。

```
show pmipv6 mag bindings {lma lma-name | nai nai-name}
```

- 次のコマンドを入力して、MAG に関する統計情報を表示します。

**show pmipv6 mag stats domain** *domain-name* **peer** *peer-name*

- 次のコマンドを入力して、すべてのクライアントの PMIPv6 に関する情報を表示します。

**show client summary**

- 次のコマンドを入力して、クライアントの PMIPv6 に関する情報を表示します。

**show client details** *client-mac-address*

- 次のコマンドを入力して、WLAN の PMIPv6 に関する情報を表示します。

**show wlan** *wlan-id*

---





## 新しいモビリティの設定

- [新しいモビリティについて](#), 1201 ページ
- [新しいモビリティの制約事項](#), 1202 ページ
- [新しいモビリティの設定 \(GUI\)](#), 1202 ページ
- [新しいモビリティの設定 \(CLI\)](#), 1204 ページ

### 新しいモビリティについて

新しいモビリティは、Cisco Catalyst 3850 シリーズ スイッチおよび Cisco 5760 シリーズ ワイヤレス LAN コントローラなどのワイヤレス コントロール モジュール (WCM) を使用した統合 アクセス コントローラと互換性のあるコントローラを有効にします。新しいモビリティでは、Catalyst 3850 のモビリティ エージェント (MA) によって統合アクセス モードの 5508 または WiSM2 でモビリティ コントローラ (MC) 機能を実行できます。

Cisco 2500 シリーズ ワイヤレス LAN コントローラ、Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco WiSM2、または Cisco 5760 ワイヤレス LAN コントローラは、Cisco Catalyst 3850 シリーズ スイッチによりモビリティ コントローラとして機能します。モビリティ コントローラは、モビリティ エージェントとモビリティ Oracle から成る階層アーキテクチャの一部です。

Cisco Catalyst 3850 シリーズ スイッチのモビリティ エージェントのグループは、スイッチ ピア グループを形成できます。Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco WiSM2、および Cisco 5760 ワイヤレス LAN コントローラの内部モビリティ エージェントは、独自のスイッチ ピア グループを形成します。モビリティ コントローラ、モビリティ エージェントおよびモビリティ Oracle は単一の Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco WiSM2、および Cisco 5760 ワイヤレス LAN コントローラに設定できます。各モビリティ コントローラは、複数のスイッチ ピア グループを持つことができるサブドメインを形成します。Cisco 5500 シリーズ ワイヤレス LAN コントローラ、Cisco WiSM2、または Cisco 5760 ワイヤレス LAN コントローラは、デフォルトではモビリティ エージェントです。ただし、Cisco Catalyst 3850 シリーズ スイッチは、モビリティ エージェントとモビリティ コントローラの両方として、またはモビリティ エージェントとしてのみ機能することができます。デフォルトでは、新しいモビリティは無効になっています。

新しいモビリティを有効または無効にする場合は、設定を保存してコントローラをリブートする必要があります。

## 新しいモビリティの制約事項

- 新しいモビリティは、Cisco 2500 シリーズ ワイヤレス LAN コントローラ、Cisco 5500 シリーズ ワイヤレス LAN コントローラ、および Cisco WiSM2 でのみサポートされます。
- Mobility Controller と Mobility Oracle 間のキープアライブは DTLS 暗号化されません。
- シームレスなモビリティの場合、コントローラは新しいモビリティまたは古いモビリティ（フラット モビリティ）のいずれかを使用する必要があります。
- 2 種類のモビリティ間の相互運用性はサポートされていません。コントローラを、リリース 7.5 から、新しいモビリティをサポートしていないリリース 7.4.100.0、7.3.101.0、7.2、7.0、またはそれ以前（7.3.112.0 以前のすべてのリリース）のコントローラ ソフトウェア リリースにダウングレードすると、コントローラは自動的にフラットモビリティ（古いモビリティ）に移行します。これはモビリティアーキテクチャの違い、およびフラットモビリティ（EOIP トンネル）と新しいモビリティ（CAPWAP トンネル）間の非相互運用性が原因です。
- Mobility Oracle のハイ アベイラビリティはサポートされていません。
- リリース 7.6 では、モビリティ コントローラ機能は Cisco 8500 シリーズの WLC でサポートされていません。



（注） モビリティ Oracle 機能も Cisco 8500 シリーズの WLC でサポートされていません。

## 新しいモビリティの設定（GUI）

**ステップ 1** [Controller]>[Mobility Management]>[Mobility Configuration] を選択し、コントローラ上で新しいモビリティを有効にして設定します。

（注） 新しいモビリティを有効または無効にする場合は、設定を保存してコントローラをリブートする必要があります。

**ステップ 2** 新しいモビリティを設定するには、[Enable New Mobility (Converged Access)] チェックボックスをオンまたはオフにします。

（注） 新しいモビリティを有効にする場合は、設定を保存してコントローラをリブートする必要があります。

**ステップ 3** Mobility Oracle としてコントローラを設定するには、[Mobility Oracle] チェックボックスをオンまたはオフにします。

（注） Mobility Oracle はオプションであり、1 つの完全なモビリティ ドメインの下で、クライアント データベースを保持します。



- ステップ 4** モビリティ グループのマルチキャスト モードを設定するには、[Multicast Mode] チェックボックスをオンまたはオフにします。
- ステップ 5** [Multicast IP Address] テキスト ボックスに、スイッチのピア グループのマルチキャスト IP アドレスを入力します。
- ステップ 6** [Mobility Oracle IP Address] テキスト ボックスに、Mobility Oracle の IP アドレスを入力します。  
[Mobility Oracle] チェックボックスをオンにした場合、このフィールドの値は入力できません。
- ステップ 7** ネットワーク アドレス変換 (NAT) がない場合は、[Mobility Controller Public IP Address] テキスト ボックスに、コントローラの IP アドレスを入力します。  
(注) コントローラに NAT が設定されている場合は、パブリック IP アドレスがネットワーク アドレスに変換された IP アドレスです。
- ステップ 8** [Mobility Keep Alive Count] テキスト ボックスに、ピアが到達不能と判断されるまでに ping 要求をピア コントローラに送信する回数を入力します。有効な範囲は 3 ~ 20 です。デフォルト値は 3 です。
- ステップ 9** [Mobility Keep Alive Interval] テキスト ボックスに、ピア コントローラに送信する各 ping 要求の間隔を秒単位で入力します。範囲は 1 ~ 30 です。デフォルト値は 10 秒です。
- ステップ 10** [Mobility DSCP] テキスト ボックスに、モビリティ コントローラに対して設定できる DSCP 値を入力します。範囲は 0 ~ 63 です。デフォルト値は 0 です
- ステップ 11** [Apply] をクリックします。
- ステップ 12** [Controller > Mobility Management > Switch Peer Group] を選択して、スイッチのピア グループに対してメンバを追加または削除します。  
このページには、すべてのスイッチのピア グループ、およびそれらの詳細 (ブリッジ ドメイン ID、マルチキャスト IP アドレス、マルチキャスト モードのステータスなど) が表示されます。必要に応じて、スイッチのピア グループ名をクリックして [Edit] ページに移動し、パラメータを更新します。
- ステップ 13** [Controller > Mobility Management > Mobility Controller] を選択して、すべてのモビリティ コントローラ、およびそれらの詳細 (IP アドレス、MAC アドレス、クライアント数、リンク ステータスなど) を表示します。
- ステップ 14** [Controller > Mobility Management > Mobility Clients] を選択して、すべてのモビリティ クライアントおよびそれらのパラメータを表示します。
- ステップ 15** [Client MAC Address] および [Client IP Address] テキスト ボックスに、モビリティ クライアントの MAC アドレスと IP アドレスをそれぞれ入力します。
- ステップ 16** [Anchor MC IP Address] および [Anchor MC Public IP Address] テキスト ボックスに、アンカー モビリティ コントローラの IP アドレスとパブリック IP アドレスをそれぞれ入力します。
- ステップ 17** [Foreign MC IP Address] および [Foreign MC Public IP Address] テキスト ボックスに、外部 MC の IP アドレスとパブリック IP アドレスをそれぞれ入力します。
- ステップ 18** [Client Association Time] テキスト ボックスに、モビリティ クライアントをモビリティ コントローラに関連付ける時間を入力します。
- ステップ 19** [Client Entry Update Timestamp] テキスト ボックスに、クライアント エントリを更新するタイムスタンプを入力します。

## 新しいモビリティの設定 (CLI)

- 次のコマンドを入力して、コントローラ上で新しいモビリティを有効または無効にします。  
**config mobility new-architecture {enable | disable}**



(注) 新しいモビリティを有効または無効にする場合は、設定を保存してコントローラをリブートする必要があります。

- 次のコマンドを入力して、Mobility Oracle を有効にするか、または外部 Mobility Oracle を設定します。  
**config mobility oracle {enable | disable | ip ip\_address}**  
ここでの *ip\_address* とは Mobility Oracle の IP アドレスです。Mobility Oracle は 1 つの完全なモビリティドメインの下で、クライアントデータベースを保持します。これは、ステーションデータベース、モビリティコントローラへのインターフェイス、および NTP サーバで構成されます。モビリティドメイン全体に Mobility Oracle は 1 つのみです。
- 次のコマンドを入力して、スイッチのピアグループを作成または削除します。  
**config mobility switchPeerGroup {create | delete} peer-group-name**  
ここでの *peer-group-name* とはスイッチのピアグループの名前です。
- 次のコマンドを入力して、フラット (古い) モビリティと新しいモビリティの互換性のためにメンバスイッチの MAC アドレスを設定します。  
**config mobility group member add ip\_address { [group-name] | mac-address | [public-ip-address] }**  
この *ip\_address* とはメンバの IP アドレスです。  
*group-name* は、デフォルトのグループ名と異なる場合、メンバスイッチグループ名です。  
*mac-address* は、メンバスイッチの MAC アドレスです。
- 次のコマンドを入力して、メンバを追加または削除し、スイッチのピアグループのブリッジドメイン ID とマルチキャストアドレスを設定します。  
**config mobility switchPeerGroup {bridge-domain-id peer-group-name bridge domain id | member {add | delete} IP\_address [public\_IP\_address] peer-group-name | multicast-address peer-group-name multicast\_IP\_address}**  
ここでの *peer-group-name* とはスイッチのピアグループの名前です。  
*IP\_address* はスイッチのピアグループメンバの IP アドレスです。  
*public\_IP\_address* はスイッチのピアグループメンバのパブリック IP アドレスです。
- 次のコマンドを入力して、Mobility Oracle に応じたモビリティコントローラの詳細を表示します。  
**show mobility oracle summary**
- 次のコマンドを入力して、Mobility Oracle クライアントデータベースの要約と詳細を表示します。  
**show mobility oracle client {summary | detail}**

- モビリティの統計情報を確認するには、次のコマンドを入力します。  
**show mobility statistics**
- モビリティ設定を確認するには、次のコマンドを入力します。  
**show mobility summary**
- 次のコマンドを入力して、変更を保存します。  
**save config**
- 次のコマンドを入力して、モビリティ パケットのデバッグを有効または無効にします。  
**debug mobility packet {enable | disable}**
- 次のコマンドを入力して、Mobility Oracle のイベントおよびエラーのデバッグを有効または無効にします。  
**debug mobility oracle {events | errors} {enable| disable}**





## 索引

### 数字

- 11n Mode パラメータ [88](#)
- 1250 シリーズ アクセス ポイント [969, 970, 971](#)
  - PoE を使用する際の送信電力設定 [970](#)
  - PoE を使用する際の動作モード [969](#)
  - および [PoE Status] フィールド [971](#)
- 7920 AP CAC パラメータ [727](#)
- 7920 Client CAC パラメータ [727](#)
- 7920 サポート モード [727](#)
  - 設定 [727](#)
  - 説明 [727](#)
- 7921 サポート モード [726](#)
- 802.11a/n Radios ページ (Monitor メニューから) [851](#)
- 802.11a/n (または 802.11b/g/n) Radios ページ [169, 1042](#)
- 802.11a (または 802.11b/g) > EDCA Parameters ページ [178](#)
- 802.11a (または 802.11b/g) Global Parameters ページ [80, 1050](#)
- 802.11a (または 802.11b/g) Network Status パラメータ [80, 91, 92](#)
- 802.11a (または 802.11b) > Client Roaming ページ [140](#)
- 802.11a (または 802.11b) > Voice Parameters ページ [163, 166, 175](#)
- 802.11g Support パラメータ [80](#)
- 802.11h Global Parameters ページ [91](#)
- 802.11h、説明 [91](#)
- 802.11n [87, 975](#)
  - クライアント [975](#)
  - デバイス [87](#)
- 802.1Q-in-Q VLAN タギング [818, 819, 827, 828](#)
  - CLI を使用した設定 [819, 828](#)
  - GUI を使用した設定 [818, 827](#)
- 802.1Q-in-Q VLAN タグ [816, 825](#)
- 802.1Q VLAN トランク ポート [347](#)
- 802.1X [682, 683, 696](#)
  - 設定 [683](#)
  - 説明 [696](#)
  - 動的キー設定 [682](#)

- 802.1x Authentication パラメータ [858](#)
- 802.3 Bridging パラメータ [120](#)
- 802.3X フロー制御、有効化 [120](#)
- 802.3 ブリッジ [119, 120](#)
  - CLI を使用した設定 [120](#)
  - GUI を使用した設定 [119, 120](#)
- 802.3 フレーム [119](#)

### A

- Access Control List Name パラメータ [527, 535, 540](#)
- Access Control Lists > Edit ページ [529, 1126](#)
- Access Control Lists > New ページ [527, 540](#)
- Access Control Lists ページ [527](#)
- Access Mode パラメータ [110, 243](#)
- Accounting Server パラメータ [781](#)
- ACL 「アクセスコントロールリスト (ACL)」を参照 [525, 1123](#)
- ACL Name パラメータ [529, 530](#)
- ACL の設定 (GUI) [527](#)
- Action パラメータ [529, 536, 1126](#)
- Add AAA Client ページ (CiscoSecure ACS で) [430, 459](#)
- Add AP ボタン [1133](#)
- Add New Rule ボタン [527, 535](#)
- Admin Status パラメータ [375, 376](#)
- Admission Control (ACM) パラメータ [163](#)
- AES-CCMP [696](#)
- Aggregated MAC Service Data Unit (A-MSDU) [90](#)
- AirMagnet Enterprise Analyzer [335](#)
- Aironet IE パラメータ [752](#)
- Airopeek [335](#)
- All APs > Access Point Name > VLAN Mappings ページ [1115](#)
- [All APs > Details for] ([Advanced]) ページ [835, 887, 964](#)
  - リンク遅延の設定 [964](#)
- All APs > Details for (Credentials) ページ [855, 859](#)
- [All APs > Details for] (FlexConnect) ページ [1114](#)
- All APs > Details for (General) ページ [1114](#)

[All APs > Details for] ([High Availability]) ページ [933, 938](#)  
 [All APs] ページ [845, 1039](#)  
 AnchorTime パラメータ [1021](#)  
 Anonymous Provision パラメータ [493](#)  
 Antenna Gain パラメータ [1043](#)  
 Antenna Type パラメータ [1042](#)  
 Antenna パラメータ [1042](#)  
 ap-count 評価ライセンス、アクティブ化 [70, 71](#)  
   CLI の使用 [70, 71](#)  
   GUI の使用 [70](#)  
 AP > Clients > Traffic Stream Metrics ページ [169](#)  
 AP801 アクセス ポイント [863](#)  
   コントローラで使用 [863](#)  
   説明 [863](#)  
 AP Authentication Policy ページ [544](#)  
 AP Core Dump パラメータ [887](#)  
 AP Ethernet MAC Addresses パラメータ [873](#)  
 AP Failover Priority パラメータ [938](#)  
 AP Group Name パラメータ [763](#)  
 AP Groups > Edit (APs) ページ [764](#)  
 AP Groups ページ [763, 789](#)  
 AP Mode パラメータ [335, 909, 1039, 1114](#)  
 AP Name パラメータ [764](#)  
 AP Primary Discovery Timeout パラメータ [933](#)  
 AP マネージャ インターフェイス [349, 357](#)  
   および動的インターフェイス [349](#)  
   説明 [357](#)  
 AP ローカル認証 [1119](#)  
   GUI の使用 [1119](#)  
 Assignment Method パラメータ [1043](#)  
 ATF [997](#)  
   ATF 設定 [997](#)  
 Authority ID Information パラメータ [493, 1135, 1137](#)  
 Authority ID パラメータ [493, 1135](#)  
 Authorize LSC APs against auth-list パラメータ [875](#)  
 Authorize MIC APs against auth-list or AAA パラメータ [875](#)  
 AutoInstall [42, 43, 44, 45, 46](#)  
   described [46](#)  
   取得 [43](#)  
     TFTP サーバ情報 [43](#)  
     インターフェイス用の DHCP アドレス [43](#)  
   使用 [42](#)  
   設定ファイルの選択 [44](#)  
   説明 [42](#)  
   操作例 [45](#)  
 Average Data Rate パラメータ [146, 150, 721](#)  
 Average Real-Time Rate パラメータ [146, 151, 721](#)

Avoid Cisco AP Load パラメータ [1021](#)  
 Avoid Foreign AP Interference パラメータ [1021, 1172](#)  
 Avoid Non-802.11a (802.11b) Noise パラメータ [1021](#)

## B

Back-up Primary Controller Name フィールド [933](#)  
 Back-up Secondary Controller Name パラメータ [933](#)  
 Beacon Period パラメータ [80](#)  
 Bind Username パラメータ [483](#)  
 Burst Data Rate パラメータ [146, 150, 721](#)  
 Burst Real-Time Rate パラメータ [147, 151, 721](#)

## C

CAC [166, 168, 169, 727](#)  
   7920 電話に対する設定 [727](#)  
   CLI を使用した表示 [169](#)  
   有効化 [166, 168](#)  
     CLI の使用 [168](#)  
     GUI の使用 [166](#)  
 CAPWAP 優先モード [841, 842, 843](#)  
   設定 [843](#)  
     CLI の使用 [843](#)  
 CA Server URL パラメータ [872](#)  
 CC の設定 (CLI) [470](#)  
 CCKM [698, 1130](#)  
   FlexConnect グループ [1130](#)  
   設定 [698](#)  
 CCX [752, 753, 959](#)  
   Aironet IE の設定 [753](#)  
     CLI の使用 [753](#)  
   クライアントのバージョンの表示 [753](#)  
     GUI の使用 [753](#)  
   説明 [752](#)  
   リンク テスト [959](#)  
 CCXv5 Req ボタン [324](#)  
 CCX Version パラメータ [753](#)  
 CCX 無線管理 [1049](#)  
   flexconnect の考慮事項 [1049](#)  
   機能 [1049](#)  
 CCX レイヤ 2 クライアント ローミング [139, 140, 141, 142](#)  
   CLI を使用した情報の取得 [141](#)  
   CLI を使用したデバッグ [142](#)  
   設定 [141](#)  
     CLI の使用 [141](#)

- CCX レイヤ 2 クライアント ローミング (続き)  
 説明 [139, 140](#)
- CDP > AP Neighbors > Detail ページ [187](#)
- CDP > Interface Neighbors > Detail ページ [186](#)
- CDP > Traffic Metrics ページ [187](#)
- CDP Advertisement Version パラメータ [183](#)
- CDP AP Neighbors ページ [186](#)
- CDP Protocol Status パラメータ [183](#)
- CDP State パラメータ [184](#)
- Certificate Authority (CA) 証明書 [223, 224, 225, 490, 495](#)  
 概要 [223](#)  
 ダウンロード [224, 225](#)  
 CLI の使用 [225](#)  
 GUI の使用 [224](#)  
 ローカル EAP での使用 [490, 495](#)
- Certificate File Name パラメータ [250](#)
- Certificate File Path パラメータ [250](#)
- Certificate Issuer パラメータ [492](#)
- Certificate Password パラメータ [221, 250](#)
- Certificate Type パラメータ [875](#)
- Change Rules Priority パラメータ [579](#)
- Channel Announcement パラメータ [91](#)
- Channel Assignment Leader パラメータ [1022](#)
- Channel Assignment Method パラメータ [1020](#)
- Channel Quiet Mode パラメータ [91](#)
- Channel Scan Duration パラメータ [1026](#)
- Channel Width パラメータ [1022](#)
- Channel パラメータ [335, 1042](#)
- Check Against CA Certificates パラメータ [492](#)
- Check Certificate Date Validity パラメータ [492](#)
- CIDS Sensor Add ページ [604](#)
- CIDS Shun List ページ [605](#)
- Cisco Aironet 700 シリーズ [919](#)
- Cisco 2500 シリーズ コントローラ [9](#)
- Cisco 3300 シリーズ Mobility Services Engine (MSE) 、wIPS  
 での使用 [619](#)
- Cisco 5500 シリーズ Wireless LAN Controller [9, 345, 346, 360, 361](#)  
 説明 [9](#)  
 複数の AP マネージャ インターフェイス [360, 361](#)  
 ポート [345, 346](#)
- Cisco 7921 Wireless IP Phone [725](#)
- Cisco AV ペア [777, 778, 779](#)
- Cisco Centralized Key Management (CCKM) 。CCKM を参照 [696](#)
- Cisco Clean Access (CCA) [787](#)
- Cisco CleanAir の設定 [1073, 1076](#)  
 CLI の使用 [1076](#)  
 GUI の使用 [1073](#)
- Cisco Discovery Protocol (CDP) [181, 183, 184, 185, 186, 187, 188](#)  
 GUI を使用した有効化 [183, 184](#)  
 サポートされるデバイス [181](#)  
 設定 [183, 184, 185](#)  
 CLI の使用 [184, 185](#)  
 GUI の使用 [183, 184](#)  
 説明 [181](#)  
 トラフィック情報の表示 [188](#)  
 CLI の使用 [188](#)  
 ネイバーの表示 [186, 187, 188](#)  
 CLI の使用 [188](#)  
 GUI の使用 [186, 187](#)
- Cisco Discovery Protocol パラメータ [184](#)
- Cisco Licensing Web サイト [74](#)
- Cisco Logo パラメータ [255](#)
- CiscoSecure Access Control Server (ACS) [428](#)
- Cisco Unified Wireless Network (UWN) ソリューション [6](#)  
 説明 [6](#)
- CleanAir の概要 [1065](#)
- Clear Filter リンク [649, 848, 882](#)
- Clear Stats on All APs ボタン [881](#)
- Clear Stats ボタン [1172](#)
- CLI [38, 39, 41, 42, 57, 298](#)  
 使用 [38, 42](#)  
 トラブルシューティング コマンド [298](#)  
 ナビゲーション [41](#)  
 ログアウト [41](#)  
 ログイン [39](#)  
 ワイヤレス接続の有効化 [57](#)
- Client Certificate Required パラメータ [492](#)
- Client Protection パラメータ [545](#)
- Clients > AP > Traffic Stream Metrics ページ [169](#)  
 [Clients > Detail] ページ [926](#)  
 クライアントの詳細情報の表示 [926](#)  
 ワークグループブリッジのステータスの表示 [926](#)
- Client Type パラメータ [926](#)
- CLI を使用した FlexConnect AP の設定 [1118](#)
- CLI を使用した電波品質のモニタリング [1088](#)
- Commands > Reset to Factory Defaults ページ [198](#)
- Community Name パラメータ [110](#)
- Conditional Web Redirect パラメータ [780](#)
- Configuration File Encryption パラメータ [231](#)
- Configuration Wizard - 802.11 Configuration ページ [26](#)

- Configuration Wizard - Management Interface Configuration ページ [21](#)
  - Configuration Wizard - Miscellaneous Configuration ページ [22](#)
  - Configuration Wizard - Service Interface Configuration ページ [19](#)
  - Configuration Wizard - Set Time ページ [27](#)
  - Configuration Wizard - SNMP Summary ページ [18, 20](#)
  - Configuration Wizard - System Information ページ [17](#)
  - Configuration Wizard - Virtual Interface Configuration ページ [23](#)
  - Configuration Wizard Completed ページ [28](#)
  - Configure オプション、RRM の無効化用 [1042](#)
  - Control and Provisioning of Wireless Access Points プロトコル (CAPWAP) [831, 832, 836](#)
    - MTU 情報の表示 [836](#)
    - 制約事項 [832](#)
    - 説明 [831](#)
    - デバッグ [836](#)
  - Controller Time Source Valid パラメータ [544](#)
  - [Core Dump] ページ [310](#)
  - Country Code [948](#)
    - CLI を使用した表示 [948](#)
  - 国番号 [945](#)
    - 説明 [945](#)
  - Country Code の設定 (CLI) [948](#)
  - Country Code の設定 (GUI) [947](#)
  - Country Code パラメータ [947](#)
  - Country ページ [947](#)
  - Coverage Exception Level per AP パラメータ [1024](#)
  - Coverage Hole Detection Enabled パラメータ [782](#)
  - CPU、5500 シリーズ コントローラ [296](#)
  - CSR の生成 [244](#)
  - Custom Signatures ページ [613](#)
- D**
- Data Encryption パラメータ [835, 910](#)
  - Data Path パラメータ [1177](#)
  - Data Rates パラメータ [81](#)
  - DCA Channel Sensitivity パラメータ [1021](#)
  - DCA Channels パラメータ [1023](#)
  - Default Mobility Group パラメータ [1165](#)
  - Default Routers パラメータ [662](#)
  - Description パラメータ [474](#)
  - Destination Port パラメータ [528, 1126](#)
  - Destination パラメータ [527, 1125](#)
  - Detect and Report Ad-Hoc Networks パラメータ [566](#)
  - DHCP Addr. Assignment Required パラメータ [658](#)
  - DHCP proxy [99](#)
    - configuring [99](#)
    - using the CLI [99](#)
  - DHCP Option 82 Remote ID Field Format パラメータ [522](#)
  - DHCP Parameters ページ [98, 100](#)
  - DHCP Scopes ページ [661](#)
  - DHCP Server IP Addr パラメータ [658](#)
  - DHCP オプション 43、コントローラ ディスカバリ プロセス [838](#)
  - DHCP オプション 82 [521, 522](#)
    - 設定 [522](#)
    - GUI の使用 [522](#)
    - 説明 [521](#)
    - 例 [521](#)
  - DHCP サーバ [655](#)
    - 内部 [655](#)
  - DHCP スコープ [661](#)
    - 説明 [661](#)
  - DHCP タイムアウト [100](#)
    - GUI を使用した設定 [100](#)
  - DHCP プロキシ [97](#)
    - 説明 [97](#)
  - Diagnostic Channel パラメータ [319](#)
  - Direction パラメータ [529](#)
  - Diversity パラメータ [1043](#)
  - DNS Domain Name パラメータ [662](#)
  - DNS IP Address パラメータ [890](#)
  - DNS Servers パラメータ [662](#)
  - Domain Name パラメータ [890](#)
  - Download File to Controller ページ [218, 224, 231, 264](#)
    - CA 証明書のダウンロード [224](#)
    - カスタマイズされた Web 認証ログイン ページのダウンロード [264](#)
    - 設定ファイルのダウンロード [231](#)
    - ログイン バナー ファイルのダウンロード [218](#)
  - Download SSL Certificate パラメータ [250](#)
  - [Download] ボタン [222, 224, 265](#)
    - CA 証明書のダウンロード [224](#)
    - カスタマイズされた Web 認証ログイン ページのダウンロード [265](#)
    - デバイスの証明書のダウンロード [222](#)
  - DSCP パラメータ [528, 1126](#)
  - DTIM [673](#)
  - DTLS [59](#)
  - DTLS データ暗号化。「データ暗号化」を参照 [832](#)
  - DTPC Support パラメータ [80](#)
  - Dynamic AP Management パラメータ [355, 372](#)
    - 管理インターフェイス [355](#)



Dynamic AP Management パラメータ (続き)

動的インターフェイス 372

Dynamic WEP Key Index パラメータ 491

## E

EAPOL-Key Max Retries パラメータ 491

EAPOL-Key Timeout パラメータ 491

EAP Profile Name パラメータ 493

EAP パラメータ 493

EDCA Profile パラメータ 178

Edit QoS Profile ページ 146

Edit QoS Role Data Rates ページ 150

Egress Interface パラメータ 275

Email Input パラメータ 276

Enable AP Local Authentication パラメータ 1134

Enable Check for All Standard and Custom Signatures パラメータ 614

Enable Counters パラメータ 527, 540

Enable Coverage Hole Detection パラメータ 1024

Enable CPU ACL パラメータ 530

Enable DHCP Proxy パラメータ 98

Enable Dynamic AP Management パラメータ 385

Enable EAP-FAST Authentication パラメータ 1134

Enable LEAP Authentication パラメータ 1134

Enable Least Latency Controller Join パラメータ 910

Enable Link Latency パラメータ 910, 964

Enable Low Latency MAC パラメータ 178

Enable LSC on Controller パラメータ 872

Enable NAT Address パラメータ 354

Enable OfficeExtend AP パラメータ 909

Enable Password パラメータ 855

Enable Server Status パラメータ 482

Enable Tracking Optimization パラメータ 952

Encryption Key パラメータ 706

Enhanced Distributed Channel Access (EDCA) パラメータ 179, 180

CLI を使用した設定 179, 180

Enter Saved Permission Ticket File Name パラメータ 75

EoIP ポート 1185

epings 1186

Expedited Bandwidth パラメータ 164

Expiration Timeout for Rogue AP and Rogue Client Entries パラメータ 565

Extensible Authentication Protocol (EAP; 拡張認証プロトコル) 495, 496, 499

タイムアウトおよび失敗の回数 499

アクセス ポイントごと 499

クライアントごと 499

ローカル タイマーの設定 495, 496

## F

Fallback Mode パラメータ 435

File Compression パラメータ 887

File Name to Save Credentials パラメータ 74

File Type パラメータ 204, 211, 213, 218, 221, 224, 226, 229, 231, 264, 315, 510, 511

CA 証明書のダウンロード 224

PAC のアップロード 226

RADIUS AVP リストのアップロード 511

RADIUS AVP リストのダウンロード 510

カスタマイズされた Web 認証ログイン ページのダウンロード 264

コントローラ ソフトウェアのアップグレード 204, 211, 213

設定ファイルのアップロード 229

設定ファイルのダウンロード 231

デバイスの証明書のダウンロード 221

パケット キャプチャ ファイルのアップロード 315

ログイン バナー 218

Fingerprint パラメータ 605

FIPS の設定 (CLI) 469

FlexConnect 1099, 1101, 1104, 1113, 1118

帯域幅の制限 1101

デバッグ 1113, 1118

認証プロセス 1099, 1104

FlexConnect Mode AP Fast Heartbeat Timeout パラメータ 933

FlexConnect グループ 1129, 1130, 1131

CCKM 1130

説明 1129

バックアップ RADIUS サーバ 1130

ローカル認証 1131

FlexConnect グループ サポート 1132

Fragmentation Threshold パラメータ 80

FTP サーバ ガイドライン 200

**G**

- General (controller) ページ [380, 1036](#)
  - RF グループの設定 [1036](#)
  - リンク集約の有効化 [380](#)
- General (security) ページ [471](#)
- General ページ [490](#)
- Generate Rehost Ticket ボタン [75](#)
- Global AP Failover Priority パラメータ [938](#)
- [Global Configuration] ページ [932, 938](#)
  - アクセスポイントのフェールオーバープライオリティの設定 [938](#)
  - バックアップコントローラの設定 [932](#)
- Group Mode パラメータ [1037, 1171](#)
- Group Name パラメータ [1133, 1166](#)
- Guest LAN パラメータ [275](#)
- Guest User Role パラメータ [474](#)
- Guest User パラメータ [474](#)
- GUI [32](#)
  - 使用 [32](#)
  - 注意事項 [32](#)
- GUI の使用 [529](#)
- GUI を使用した電波品質のモニタリング [1087](#)

**H**

- Headline パラメータ [255](#)
- hex2pcap 出力例 [332](#)
- Holdtime パラメータ [183](#)
- HTTP Access パラメータ [34](#)
- [HTTP Configuration] ページ [33](#)
- HTTPS Access パラメータ [34](#)
- Hysteresis パラメータ [140](#)

**I**

- Identity Request Max Retries パラメータ [491](#)
- Identity Request Timeout パラメータ [491](#)
- IDS シグニチャ [609, 614, 615, 617](#)
  - frequency [615](#)
  - MAC frequency [615, 617](#)
  - Quiet time [615, 617](#)
  - 説明 [609](#)
  - 測定間隔 [615](#)
  - 追跡方法 [614](#)
  - パターン [614](#)

- IDS センサー [603](#)
  - 説明 [603](#)
- IGMP Timeout パラメータ [125](#)
- IGMP スヌーピング [793](#)
- IKE Diffie Hellman Group パラメータ [435](#)
- IKE Phase 1 パラメータ [435](#)
- Index パラメータ、IDS 用 [604](#)
- Ingress Interface パラメータ [275](#)
- Injector Switch MAC Address パラメータ [972](#)
- Install License ボタン [63](#)
- Interface Name パラメータ [764, 788, 789](#)
- [Interfaces > Edit] ページ [384](#)
  - 複数の AP マネージャ インターフェイスの作成 [384](#)
- Interface パラメータ [658](#)
- Interference threshold パラメータ [1025](#)
- Interval パラメータ [1021](#)
- Inventory ページ [958](#)
- Invoke Channel Update Now ボタン [1020](#)
- Invoke Power Update Now ボタン [1017](#)
- IP Mask パラメータ [110](#)
- IPSec パラメータ [434](#)
- IP アドレスと MAC アドレス間のバインディング [143](#)
  - 説明 [143](#)

**K**

- Keep Alive Count パラメータ [1177](#)
- Keep Alive Interval パラメータ [1177](#)
- Key Encryption Key (KEK) パラメータ [433](#)
- Key Index パラメータ [706](#)
- Key Size パラメータ [706](#)
- Key Wrap Format パラメータ [433](#)
- Key Wrap パラメータ [433, 434](#)

**L**

- LAG Mode on Next Reboot パラメータ [380](#)
- Last Auto Channel Assignment パラメータ [1022](#)
- Layer2 Access Control Lists > Edit ページ [537](#)
- Layer2 Access Control Lists > New ページ [535](#)
- Layer2 Access Control Lists ページ [535](#)
- Layer2 ACL パラメータ [537](#)
- Layer 2 Security パラメータ [698, 706, 780](#)
- Layer 3 Security パラメータ [275, 710, 712, 716, 780](#)
  - VPN パススルー [710, 716](#)
  - Web 認証 [712](#)

## Layer 3 Security パラメータ (続き)

Web リダイレクト [780](#)有線ゲスト アクセスの場合 [275](#)LDAP [483, 484](#)サーバの優先順位の選択 [483](#)設定 [484](#)GUI の使用 [484](#)LDAP Servers パラメータ [493](#)LDAP Servers ページ [482](#)LDAP サーバ [484](#)WLAN への割り当て [484](#)Lease Time パラメータ [662](#)LED [292, 980](#)解釈 [292](#)設定 [980](#)License Commands ページ [63](#)License Detail ページ [64, 69](#)Licenses ページ [64, 69](#)Lifetime パラメータ [239, 474](#)lightweight モード、自律モードへの復帰 [868](#)Link Status パラメータ [376](#)Link Trap パラメータ [376](#)Lobby Ambassador Guest Management > Guest Users List ページ [239](#)Local Auth Active Timeout パラメータ [491](#)Local EAP Authentication パラメータ [493](#)Local Management Users > New ページ [238](#)Local Management Users ページ [238](#)Local Mode AP Fast Heartbeat Timer パラメータ [932](#)Local Net Users > New ページ [474](#)Local Significant Certificates (LSC) - AP Provisioning ページ [872](#)Local Significant Certificates (LSC) - General ページ [872](#)LWAPP-enabled アクセス ポイント [868, 869, 883, 884, 885, 886, 889](#)アップロード [885, 886](#)アクセス ポイントのコア ダンプ [886](#)無線コア ダンプ [885, 886](#)クラッシュ情報のコントローラへの送信 [884](#)自律モードへの復帰 [868, 869](#)デバッグ コマンド [883](#)無線コア ダンプの取得 [884](#)リセット ボタンの無効化 [889](#)

## M

MAC フィルタリング [665, 669](#)WLAN の設定 [665, 669](#)Management Frame Protection パラメータ [544](#)Management IP Address パラメータ [909](#)Master Controller Configuration ページ [838](#)Master Controller Mode パラメータ [838](#)Max-Login Ignore Identity Response パラメータ [491](#)Maximum Local Database Entries パラメータ [471](#)Max RF Bandwidth パラメータ [163, 167](#)MCS データ レート [88](#)Member MAC Address パラメータ [1166](#)Message Logs page [302](#)Message Authentication Code Key (MACK) パラメータ [434](#)Message パラメータ、Web 認証用 [255](#)Metrics Collection パラメータ [165](#)MFP Client Protection パラメータ [544](#)MIC [705](#)Min Failed Client Count per AP パラメータ [1024](#)Minimum RSSI パラメータ [140](#)MMH MIC [706, 707](#)設定 [706, 707](#)Mobility Anchor Create ボタン [1178](#)Mobility Anchors オプション [1177](#)MODE access point ボタン [889](#)Mode パラメータ [140, 1050](#)mpings [1186](#)Multicast Groups ページ [127](#)Multicast ページ [125](#)

## N

NAC State パラメータ [764, 789](#)NAC アウトオブバンド統合 [785, 787](#)図 [787](#)注意事項 [785](#)NAC アウトオブバンドのサポート [789, 790](#)特定のアクセス ポイントグループに対する設定 [789, 790](#)CLI の使用 [790](#)GUI の使用 [789](#)NAC インバンド モード [786](#)Native VLAN ID パラメータ [1114](#)NAT アドレス [354, 356, 371, 373](#)管理インターフェイス [354, 356](#)動的インターフェイス [371, 373](#)

Neighbor Packet Frequency パラメータ **1026**  
 Netbios Name Servers パラメータ **662**  
 Netmask パラメータ **662**  
 Network Mobility Services Protocol (NMSP) **194**  
 Network パラメータ **662**  
 NTP サーバ **46**  
   日時を取得するための設定 **46**  
 Number of Attempts to LSC パラメータ **872**  
 Number of Hits パラメータ **529**

## O

OEAP のトラブルシューティング **340**  
 OfficeExtend AP パラメータ **910**  
 OfficeExtend アクセス ポイント **340, 897, 898, 907, 909, 911, 916, 917**  
   LED **340**  
   一般的なセットアップ **897**  
   および NAT **898**  
   サポートされるアクセス ポイント モデル **898**  
   設定 **909, 911, 916**  
     GUI の使用 **909, 911**  
     個人 SSID **916**  
   説明 **897**  
   統計情報の表示 **917**  
   配置 **340**  
     ファイアウォールの要件 **907**  
 OfficeExtend アクセス ポイントの [Home] ページ **915**  
 Order Used for Authentication パラメータ **436, 463**  
 Over-ride Global Credentials パラメータ **856, 859, 910**  
 Override Global Config パラメータ **267, 276**  
 Override Interface ACL パラメータ **530**

## P

P2P Blocking パラメータ **678**  
 Params パラメータ **872**  
 Password パラメータ **226, 474, 855, 858**  
   PAC **226**  
     アクセス ポイント認証の **858**  
     アクセス ポイントの **855**  
     ローカル ネットユーザ **474**  
 PEAP パラメータ **492**  
 Personal SSID パラメータ **916**  
 Physical Mode パラメータ **375**  
 Physical Status パラメータ **376**  
 ping テスト **1186**  
 ping リンク テスト **959**  
 PMKID キャッシュ **700**  
 PMK キャッシュ ライフタイム タイマー **699**  
 PoE Status パラメータ **971**  
 Pool End Address パラメータ **662**  
 Pool Start Address パラメータ **662**  
 Port Number パラメータ **275, 375, 434, 462, 482**  
   LDAP サーバ **482**  
   RADIUS サーバ **434**  
   TACACS+ サーバ **462**  
   コントローラ **375**  
   有線ゲスト アクセスの場合 **275**  
 Ports ページ **375**  
 Port パラメータ、IDS 用 **604**  
 Power Injector Selection パラメータ **972**  
 Power Injector State パラメータ **972**  
 Power Neighbor Count パラメータ **1018**  
 Power Over Ethernet (PoE) パラメータ **376**  
 Power over Ethernet (PoE) **13, 971, 972, 973**  
   設定 **971, 972, 973**  
     CLI の使用 **973**  
     GUI の使用 **971, 972**  
   説明 **13**  
 Power Threshold パラメータ **1018**  
 Preauthentication ACL パラメータ **531, 780**  
 Primary Controller のパラメータ **933**  
 Primary RADIUS Server パラメータ **1133**  
 Priority Order > Local-Auth ページ **490**  
 Priority Order > Management User ページ **436, 463**  
 Privacy Protocol パラメータ **243**  
 Profile Name パラメータ **275, 646, 756**  
 Protected Access Credential (PAC) **226, 227, 228, 490, 1135**  
   アップロード **226, 227, 228**  
     CLI の使用 **227, 228**  
     GUI の使用 **226**  
   概要 **226**  
   ローカル EAP での使用 **490, 1135**  
 Protection Type パラメータ **544, 1039**  
 Protocol Type パラメータ **147**  
 Protocol パラメータ **528, 1126**  
 PSK **696**  
   説明 **696**  
 PSK Format パラメータ **698**

- Q**
- QBSS 726
  - QoS 145, 719
    - レベル 145, 719
  - QoS プロファイル 146, 148, 149
    - 設定 146, 148, 149
      - CLI の使用 148, 149
      - GUI の使用 146, 148
  - QoS ロール 149, 151
    - 設定 149, 151
      - CLI の使用 151
      - GUI の使用 149, 151
  - Quality of Service (QoS) パラメータ 720
  - Quarantine パラメータ 371, 788
    - NAC アウトオブバンド統合 788
    - 動的インターフェイス 371
  - Query Interval パラメータ 604
- R**
- 無線リソース管理 (RRM) 1014, 1017, 1020, 1023, 1024, 1026, 1032, 1035, 1038, 1041, 1042, 1048, 1049
    - CCX の機能。「CCX 無線管理」を参照 1049
    - RRM の無効化 1041
    - Wireless > 802.11a/n (または 802.11b/g/n) > RRM > TPC パラメータ 1017
    - カバレッジ ホールの検出 1014, 1024
      - GUI を使用したコントローラごとの設定 1024
      - 説明 1014
    - 更新間隔 1035, 1038
      - 設定 1026
        - GUI を使用した監視間隔 1026
    - チャンネルおよび送信電力設定の静的割り当て 1042
      - GUI の使用 1042
    - チャンネルおよび電力の動的割り当ての無効化 1048
      - CLI の使用 1048
    - チャンネルの指定 1020, 1023
    - デバッグ 1032
  - RADIUS 428, 430, 438, 440, 1130
    - ACS での設定 428, 430
    - FIPS 標準 438
    - FlexConnect の使用方法 1130
    - KEK パラメータ 438
    - MACK パラメータ 438
      - サーバのフォールバック動作 440
    - RADIUS AVP リストのアップロード (GUI) 511
    - RADIUS AVP リストのアップロードおよびダウンロード (CLI) 512
    - RADIUS AVP リストのダウンロード 511
    - RADIUS AVP リストのダウンロード (GUI) 510
    - RADIUS アカウンティング サーバでのレルムの設定 (CLI) 515
    - RADIUS アカウンティング サーバでのレルムの設定 (GUI) 515
    - RADIUS 認証サーバでのレルムの設定 (CLI) 515
    - RADIUS 認証サーバでのレルムの設定 (GUI) 515
    - RADIUS 認証属性 441
    - RADIUS 認証属性、Airespace 444
    - rc4-preference、Web 管理の設定 35
    - Re-sync ボタン 605
    - Redirect URL After Login パラメータ 255
    - Refresh-time Interval パラメータ 183
    - Regenerate Certificate ボタン 250
    - Rehost Ticket File Name パラメータ 75
    - Remote Authentication Dial-In User Service (リモート認証ダイヤルイン ユーザ サービス)。「RADIUS」を参照 427
    - Request Max Retries パラメータ 491
    - Request Timeout パラメータ 491
    - Reserved Roaming Bandwidth パラメータ 164
    - Reset Link Latency ボタン 964
    - Reset Personal SSID パラメータ 909
    - RF-Network Name パラメータ 1036
    - RF Channel Assignment パラメータ 1048
    - RFID タグ 193, 196
      - 説明 193
      - 追跡 196
        - CLI を使用したデバッグ 196
    - RF グループ 1033, 1034, 1036, 1037, 1038
      - 概要 1033, 1036
      - カスケード 1034
      - 固定 1034
      - ステータスの表示 1037, 1038
        - CLI の使用 1038
        - GUI の使用 1037
      - 設定 1036
        - GUI の使用 1036
    - RF グループの設定 1016
      - CLI の使用 1016
    - RF グループ名 1035
      - 説明 1035
    - RF グループ モードの設定 1015
      - GUI の使用 1015

- RF グループ リーダー [1034](#)
    - 説明 [1034](#)
  - RLDP。「Rogue Location Discovery Protocol (RLDP)」を参照 [563](#)
  - Rogue Detection パラメータ [565, 910](#)
  - Rogue Location Discovery Protocol パラメータ [565](#)
  - Rogue Policies ページ [565](#)
  - Role Name パラメータ [150](#)
  - Role パラメータ [474](#)
  - RRM「無線リソース管理 (RRM)」を参照 [1009](#)
  - RSNA ログ [326](#)
    - 設定 [326](#)
    - 説明 [326](#)
  - RSSI Low Check [80, 82](#)
  - Rx SOP の設定 [1060](#)
    - GUI の使用 [1060](#)
  - RxSOP [1059](#)
  - RxSOP の設定 [1061](#)
    - CLI の使用 [1061](#)
- ## S
- Save and Reboot ボタン [224](#)
  - Save Licenses ボタン [63](#)
  - Scan Threshold パラメータ [140](#)
  - Scope Name パラメータ [662](#)
  - SE-Connect [1092](#)
  - Search AP ウィンドウ [851, 881](#)
  - Search WLANs ウィンドウ [648, 845](#)
  - Secondary Controller のパラメータ [934](#)
  - Secondary RADIUS Server パラメータ [1133](#)
  - Select APs from Current Controller パラメータ [1133, 1134](#)
  - Sequence パラメータ [527, 536, 1125](#)
  - Server Address パラメータ [604](#)
  - Server Index (Priority) パラメータ [433, 462, 482](#)
  - Server IP Address パラメータ [336, 433, 462, 482](#)
    - LDAP サーバ [482](#)
    - RADIUS サーバ [433](#)
    - TACACS+ サーバ [462](#)
    - 無線スニファ用 [336](#)
  - Server Key パラメータ [493, 1135](#)
  - Server Status パラメータ [434, 462](#)
  - Server Timeout パラメータ [434, 462, 483](#)
  - Set Priority ボタン [69](#)
  - Set to Factory Default ボタン [1026](#)
  - Severity Level Filtering パラメータ [299](#)
  - Shared Secret Format パラメータ [433, 462](#)
  - Shared Secret パラメータ [433, 462](#)
  - Short Preamble Enabled パラメータ [501](#)
  - Signature Events Summary ページ [615](#)
  - Sniff パラメータ [335](#)
  - SNMP v1 / v2c Community ページ [110](#)
  - SNMP V3 Users ページ [243](#)
  - SNMP v3 ユーザ [242, 243](#)
    - GUI を使用したデフォルト値の変更 [242, 243](#)
  - SNMP エンジン ID [109](#)
  - SNMP、設定 [108](#)
  - Source パラメータ、ACL [527, 1125](#)
  - SpectraLink NetLink 電話 [501](#)
    - 概要 [501](#)
  - Spectrum Expert [1091](#)
    - GUI を使用した設定 [1091](#)
  - Spectrum Expert の設定 [1091](#)
  - Splash Page Web Redirect パラメータ [780](#)
  - SSH [53, 55, 337, 910, 912](#)
    - アクセスポイントのトラブルシューティング [55, 337](#)
      - GUI の使用 [55, 337](#)
    - および OfficeExtend アクセスポイント [910, 912](#)
      - 設定 [53, 55](#)
        - CLI の使用 [53, 55](#)
  - SSH パラメータ [56, 338](#)
  - SSID [645, 646, 647](#)
    - 設定 [646, 647](#)
      - CLI の使用 [647](#)
      - GUI の使用 [646](#)
    - 説明 [645](#)
  - SSLv2、Web 管理の設定 [35](#)
  - SSL 認証 [35, 37](#)
    - ロード [35, 37](#)
      - CLI の使用 [37](#)
      - GUI の使用 [35, 37](#)
  - SSL プロトコル [33](#)
  - State パラメータ [605, 615](#)
  - Static IP パラメータ [890](#)
  - Status パラメータ [110, 275, 646, 662, 756](#)
    - DHCP スコープ [662](#)
    - SNMP コミュニティの [110](#)
    - WLAN [646, 756](#)
      - ゲスト LAN の場合 [275](#)
  - [Summary] ページ [53](#)
  - Switch IP Address (Anchor) パラメータ [1178](#)
  - SX/LC/T Small Form-Factor Plug-in (SFP) モジュール [347](#)
  - Symmetric Mobility Tunneling Mode パラメータ [1184](#)
  - syslog [326, 327](#)
    - 説明 [326](#)

syslog (続き)

ログ [326, 327](#)

[Syslog Configuration] ページ [299](#)

Syslog Facility パラメータ [300](#)

Syslog Server IP Address パラメータ [299](#)

Syslog サーバ [299](#)

コントローラからの削除 [299](#)

重大度レベルのフィルタリング [299](#)

[System Resource Information] ページ [297](#)

## T

TACACS+ [455, 456, 460, 463](#)

アカウントिंग [456](#)

許可 [456](#)

設定 [463](#)

GUI の使用 [463](#)

説明 [455](#)

認証 [455](#)

ロール [460](#)

TACACS+ (Authentication, Authorization, or Accounting)

Servers > New ページ [462](#)

TACACS+ (Authentication, Authorization, or Accounting)

Servers ページ [461](#)

TACACS+ Administration .csv ページ (CiscoSecure ACS  
で) [465, 466](#)

Telnet [55, 56, 337, 338](#)

アクセス ポイントのトラブルシューティング [55, 56,](#)  
[337, 338](#)

CLI の使用 [56, 338](#)

GUI の使用 [55, 56, 337, 338](#)

[Telnet-SSH Configuration] ページ [52](#)

Telnet セッション [51, 53](#)

設定 [51, 53](#)

GUI の使用 [51, 53](#)

Telnet パラメータ [56, 338](#)

Tertiary Controller のパラメータ [934](#)

text2pcap 出力例 [333](#)

Time Length Value (TLV) 、CDP のサポート [181, 182](#)

Time to Live for the PAC パラメータ [493, 1135](#)

Traffic Specifications (TSPEC) 要求 [161](#)

例 [161](#)

Traffic Stream Metrics (TSM) [162, 169, 170, 171](#)

説明 [162](#)

統計情報の表示 [169, 170, 171](#)

CLI の使用 [170, 171](#)

GUI の使用 [169](#)

Transfer Mode パラメータ [204, 211, 213, 221, 224, 226, 229, 231,](#)  
[264, 315, 510, 511](#)

CA 証明書のダウンロード [224](#)

PAC のアップロード [226](#)

RADIUS AVP リストのアップロード [511](#)

RADIUS AVP リストのダウンロード [510](#)

カスタマイズされた Web 認証ログイン ページのダウ  
ンロード [264](#)

コントローラ ソフトウェアのアップグレード [204, 211,](#)  
[213](#)

設定ファイルのアップロード [229](#)

設定ファイルのダウンロード [231](#)

デバイスの証明書のダウンロード [221](#)

パケットキャプチャ ファイルのアップロード [315](#)

Transition Time パラメータ [141](#)

Trap Logs ページ [730](#)

Tx Power Level Assignment パラメータ [1048](#)

Type パラメータ [275, 646, 756](#)

## U

U-APSD [162, 169, 170](#)

ステータスの表示 [169, 170](#)

CLI の使用 [170](#)

GUI の使用 [169](#)

説明 [162](#)

UCAPL の設定 (CLI) [470](#)

UDP Lite [985, 986](#)

UDP、RADIUS での使用 [428](#)

UDP ポート [1185](#)

Unique Device Identifier (UDI) [957, 958](#)

取得 [958](#)

CLI の使用 [958](#)

GUI の使用 [958](#)

説明 [957](#)

Upload CSV File パラメータ [1134](#)

[Upload File from Controller] ページ [226, 229, 315, 885](#)

Upload ボタン [227, 308, 315, 512, 613](#)

RADIUS AVP リストのアップロード [512](#)

Use AES Key Wrap パラメータ [433](#)

User Access Mode パラメータ [238](#)

User Attribute パラメータ [483](#)

User Base DN パラメータ [483](#)

User Credentials パラメータ [483](#)

Username パラメータ [855, 858, 859](#)

User Name パラメータ [474](#)

User Object Type パラメータ [483](#)

User Profile Name パラメータ 243

User パラメータ 226

## V

Validate Rogue Clients Against AAA パラメータ 566

Validity パラメータ 226

VCI 文字列 877

Verify Certificate CN Identity パラメータ 492

VLANs 369

説明 369

VLAN 351

注意事項 351

VLAN Identifier パラメータ 358, 371, 372

AP マネージャ インターフェイス 358

動的インターフェイス 371, 372

VLAN ID パラメータ 788, 1115

VLAN Select 387

voice-over-IP (VoIP) による通話ローミング 138

Voice RSSI パラメータ 1024

VoIP Snooping and Reporting パラメータ 730

VoIP コール、エラー コード 734

VoIP スヌーピング 729, 730

説明 729, 730

VPN Gateway Address パラメータ 710

VPN パススルー 709, 716

GUI を使用した設定 716

説明 709

## W

webauth.tar ファイル 267

webauth bundle 263

Web Authentication Type パラメータ 255, 262, 265

Web Auth Type パラメータ 267, 276

Web Policy パラメータ 531, 780

Web Session Timeout パラメータ 34

Web 認証 249, 250, 251, 254, 711

WLAN の設定 711

GUI の使用 711

証明書 249, 250

GUI を使用して取得 249, 250

説明 251

プロセス 254

ログイン成功ページ 254

SSLv2、Web 認証の、無効 255

Web 認証ログイン ページ 253, 255, 256, 257, 261, 262, 265

外部 Web サーバからのカスタマイズ 262

GUI の使用 262

デフォルト 253

デフォルトの選択 256, 257

CLI の使用 256, 257

プレビュー 255, 265

変更されたデフォルトの例 261

Web ブラウザ セキュリティ警告 252

Web モード 33

説明 33

Web リダイレクトの設定 (GUI) 780

Web Login ページ 262

WEP キー、設定 682

WGB Wired Clients ページ 926

WGB パラメータ 926

WLAN 646, 647, 648, 670, 682, 757, 1120

クライアントを接続 1120

削除 646, 647

CLI の使用 647

GUI の使用 646

作成 757

GUI の使用 757

セキュリティ設定の確認 682

セッションタイムアウト 670

説明 670

有効化または無効化 647, 648

CLI の使用 648

GUI の使用 647

WLAN でのレルムの設定 (CLI) 514

WLAN でのレルムの設定 (GUI) 514

WLAN ID パラメータ 646, 756

WLAN Profile パラメータ 474

[WLANs > Edit] ([Advanced]) ページ 319, 782

診断チャネルの設定 319

[WLANs > Edit] ([Security] > [AAA Servers]) ページ 268, 781

WLAN のアカウントिंग サーバの無効化 781

外部認証に対して RADIUS または LDAP サーバを選択 268

[WLANs > Edit] ([Security] > [Layer 3]) ページ 780

Web リダイレクトの設定 780

WLANs > Edit ページ 275, 646, 756

WLAN SSID パラメータ 240, 764, 789

WLAN へのアクセス ポイント グループのマップ 764, 789

ゲストユーザの設定 240



- WLANs ページ [645, 647, 652, 756, 1177](#)
  - WLAN 上の AP ローカル認証 [1119](#)
    - CLI の使用 [1119](#)
  - WLAN 上のローカル認証 [1119](#)
    - GUI の使用 [1119](#)
  - WLAN でのカバレッジ ホール検出の設定 (GUI) [782](#)
  - WLAN でのローカル EAP タイムアウト パラメータの拡張  
認証プロトコル (EAP) 設定 [496](#)
  - WLAN への ACL の適用 [530](#)
  - WLAN へのレイヤ 2 ACL の適用 [537](#)
  - WLAN モビリティセキュリティ値 [1181](#)
  - WMM [160, 727, 728](#)
    - CAC を使用 [160](#)
    - 設定 [727, 728](#)
    - 説明 [727](#)
  - WMM パラメータ [178, 179](#)
  - WPA2 Policy パラメータ [698](#)
  - wplus ライセンス。ライセンス [59](#)
  - wplus ライセンス。「ライセンス」を参照 [60](#)
- あ**
- アクセス コントロール リスト (ACL) [329, 526, 527, 531, 532, 540, 1124](#)
    - WLAN への適用 [532](#)
      - CLI の使用 [532](#)
    - counters [540](#)
      - GUI を使用した設定 [540](#)
    - カウンタ [527, 531](#)
      - CLI を使用した設定 [531](#)
      - GUI を使用した設定 [527](#)
    - コントローラの CPU への適用 [532](#)
      - CLI の使用 [532](#)
    - 設定 [531, 532](#)
      - CLI の使用 [531, 532](#)
    - デバッグ ファシリティでの使用 [329](#)
    - ルール [526, 532, 1124](#)
  - アクセス ポイント [139, 292, 837, 838, 870, 871, 875, 881, 882, 891, 892](#)
    - join 情報の表示 [881, 882](#)
      - GUI の使用 [881, 882](#)
    - LED [292](#)
      - 解釈 [292](#)
    - アクセス ポイントとコントローラの join の確認 [838](#)
    - 許可 [870, 871](#)
      - LSC の使用 [871](#)
      - MIC の使用 [871](#)
    - アクセス ポイント (続き)
      - 許可 (続き)
        - SSC の使用 [870](#)
      - 許可リスト [875](#)
      - 経路ローミング [139](#)
      - サイズの大きなイメージのサポート [891, 892](#)
      - プライミング [837](#)
    - アクセス ポイント グループ [764, 765, 766](#)
      - アクセス ポイントの割り当て [765, 766](#)
        - CLI の使用 [766](#)
        - GUI の使用 [765](#)
      - 削除 [764, 765](#)
        - CLI の使用 [765](#)
        - GUI の使用 [764](#)
      - 作成 [765, 766](#)
        - CLI の使用 [765, 766](#)
      - 表示 [766](#)
    - アクセス ポイントでの RFID トラッキング、最適化 [952](#)
      - GUI の使用 [952](#)
    - アクセス ポイントの 802.1X 認証 [857, 859, 860](#)
      - 設定 [859, 860](#)
        - CLI の使用 [859, 860](#)
        - スイッチ [860](#)
      - 説明 [857](#)
    - アクセス ポイントの MAC アドレス [888](#)
      - コントローラ GUI に表示された [888](#)
    - アクセス ポイントのイベント ログ、表示 [306](#)
    - アクセス ポイントのカウント、5500 シリーズ コントローラ  
の認証された層 [61](#)
    - アクセス ポイントのグローバル クレデンシャル [855, 856](#)
      - 無効化 [855, 856](#)
        - CLI の使用 [856](#)
        - GUI の使用 [855](#)
    - アクセス ポイントのコア ダンプ、アップロード [886](#)
      - GUI の使用 [886](#)
    - アクセス ポイントのスニファの設定 [335](#)
      - GUI の使用 [335](#)
    - アクセス ポイントのフェールオーバー プライオリ  
ティ [938, 939](#)
      - CLI を使用した表示 [939](#)
        - 設定 [938](#)
        - GUI の使用 [938](#)
      - 設定 [938](#)
        - CLI の使用 [938](#)
      - 説明 [938](#)
    - アクセス ポイント無線、検索 [851](#)
    - アクセス ポイント モニタ サービス、デバッグ [339](#)

新しいモビリティ：GUI 設定 **1202**

暗号 **697, 698, 699**

設定 **698, 699**

説明 **697**

## い

イーサネット接続、リモートで使用 **41**

意図的な悪用 **639**

イベント報告、MFP に対する **543**

イメージのプレダウロード **207**

インターネットグループ管理プロトコル (IGMP) **122, 125, 126**

スヌーピング **122**

設定 **125, 126**

CLI の使用 **126**

GUI の使用 **125**

インターフェイス **348, 369**

概要 **348, 369**

インターフェイスグループ **388, 393**

インフラストラクチャ MFP **542**

コンポーネント **542**

インラインパワー **969**

拡張ネイバーリスト (続き)

要求 (E2E) **139**

隔離 VLAN **354, 371, 788, 1103, 1109**

FlexConnect を使用 **1103**

NAC アウトオブバンド統合で **788**

使用 **1109**

設定 **354, 371**

仮想インターフェイス **363, 364**

説明 **363, 364**

カバレッジホールの検出 **782, 1024, 1025, 1030**

WLAN 上の無効化 **782**

説明 **782**

コントローラごとの設定 **1024, 1025, 1030**

CLI の使用 **1030**

GUI の使用 **1024, 1025**

カバレッジホールの検出と修正 **1014**

監視間隔、GUI を使用した設定 **1026**

干渉 **1012, 1066**

管理インターフェイス **353**

説明 **353**

管理者アクセス権 **241**

管理フレーム検証 **543**

管理フレーム保護 (MFP) **541**

タイプ **541**

## え

エンドユーザライセンス契約 (EULA) **63**

## お

オペレーティングシステム **6**

セキュリティ **6**

ソフトウェア **6**

音声設定 **165**

設定 **165**

GUI の使用 **165**

オンラインヘルプ、使用 **32**

## か

回避クライアント **603**

説明 **603**

拡張ネイバーリスト **139**

説明 **139**

## き

キー置換 **705, 706, 707**

設定 **706, 707**

説明 **705**

キャパシティ Adder ライセンス。「ライセンス」を参照 **59**

## く

クライアント **752, 753, 975, 976, 977, 1120**

CCX バージョンの表示 **752, 753**

CLI の使用 **753**

GUI の使用 **752**

WLAN への接続 **1120**

表示 **975, 976, 977**

CLI の使用 **977**

GUI の使用 **975, 976**

クライアント MFP **542**

クライアント除外ポリシーの設定 (CLI) **548**

クライアント除外ポリシーの設定 (GUI) **547**

クライアント レポート [324](#)

説明 [324](#)

クライアント ローミング、設定 [142](#)

クライアント ロケーション、Prime Infrastructure の使用 [9](#)

クラッシュ ファイル [308](#)

アップロード [308](#)

CLI の使用 [308](#)

## け

ゲスト WLAN、作成 [240](#)

ゲスト ユーザ アカウント [240](#)

表示 [240](#)

CLI の使用 [240](#)

GUI の使用 [240](#)

## こ

コア ダンプ ファイル [309, 312](#)

5500 シリーズ コントローラ から TFTP または FTP サーバへのアップロード [312](#)

説明 [309](#)

工場出荷時設定 [198](#)

GUI を使用したリセット [198](#)

高速 SSID 変更 [117](#)

GUI を使用した設定 [117](#)

高速ハートビート タイマー [931, 932, 934](#)

設定 [932, 934](#)

CLI の使用 [934](#)

GUI の使用 [932](#)

説明 [931](#)

固定 IP アドレス [890](#)

設定 [890](#)

GUI の使用 [890](#)

固定 IP アドレスを持つクライアントのダイナミックアンカー [1187](#)

設定 [1187](#)

コントローラ [4, 5, 8, 9, 205, 207, 233, 837](#)

概要 [8](#)

シングルコントローラ展開 [4](#)

設定 [233](#)

保存 [233](#)

ソフトウェアのアップグレード [205, 207](#)

CLI の使用 [207](#)

GUI の使用 [205](#)

コントローラ (続き)

ディスカバリ プロセス [837](#)

プラットフォーム [9](#)

マルチ コントローラ展開 [5](#)

コントローラ CPU への ACL の適用 [530](#)

コントローラ間ローミング [138, 1156](#)

説明 [138](#)

例 [1156](#)

コントローラ内ローミング [137, 1155](#)

図示 [1155](#)

説明 [137](#)

コントローラのシリアル番号、検索 [75, 76](#)

コントローラの設定 (GUI) [17](#)

コントローラの役割 [1066](#)

コントローラのリセット [236](#)

コンフィギュレーション ファイル [230, 231, 235](#)

ダウンロード [230, 231](#)

GUI の使用 [230, 231](#)

編集 [235](#)

## さ

サードパーティ証明書のダウンロード [246, 247](#)

CLI の使用 [247](#)

GUI の使用 [246](#)

サービス ポート [348](#)

サービス ポート インターフェイス [355, 364, 367](#)

設定 [355, 364](#)

GUI の使用 [355, 364](#)

説明 [367](#)

最大ローカル データベース エントリ [471](#)

GUI を使用した設定 [471](#)

サブネット間モビリティ [1162](#)

サブネット間ローミング [138, 1158](#)

図示 [1158](#)

説明 [138](#)

サポートされたブラウザ [32](#)

## し

時刻、設定 [46](#)

NTP サーバの使用 [46](#)

自己署名証明書 (SSC) [870](#)

アクセス ポイントの許可に使用 [870](#)

## シスコ ワイヤレス ソリューション 3

説明 3

システム メッセージ 292

システム リソース 296, 297

CLI を使用した表示 297

GUI を使用した表示 296

システム ロギング 299

設定 299

GUI の使用 299

システム ログ、CLI を使用した表示 306

事前認証アクセス コントロール リスト (ACL) 262, 532, 1108

WLAN への適用 532

CLI の使用 532

外部 Web サーバの 262, 1108

失敗した Voice over IP (VoIP) コールのエラー コード 734

自動アンカー モビリティ 1175, 1177, 1178

概要 1175

設定 1177, 1178

GUI の使用 1177, 1178

集約方法、指定 89

条件付き Web リダイレクト 777, 778

説明 778

診断チャネル 318, 319

設定 319

GUI の使用 319

説明 318

シンメトリック モビリティ トンネリング 1183, 1184

概要 1183

図示 1184

ステータスの確認 1184

CLI の使用 1184

## す

スタティック IP アドレス 889

説明 889

ステートフル DHCPv6 IP アドレス指定 743

スニファ。「無線スニファ」を参照 334

## せ

製品認証キー (PAK) 61, 62

登録 62

ライセンスのアップグレードの入手 61

セキュリティ 423

概要 423

設定ウィザード 15, 28, 29

CLI バージョン 28, 29

説明 15

設定の保存 233

## そ

送信電力 1044

CLI を使用した静的割り当て 1044

GUI を使用した静的割り当て 1044

送信電力のしきい値、減少 1027

送信電力の動的制御、設定 80

送信電力レベル 1043

ソフトウェア、アップグレード 199, 203, 205

CLI の使用 205

GUI の使用 203

注意事項 199

## た

帯域幅ベースの CAC 160, 163, 165

説明 160

有効化 163, 165

CLI の使用 165

GUI の使用 163

耐障害性 1098

タイムスタンプ、ログおよびデバッグ メッセージ内での有効化または無効化 305

タイムゾーン 48, 49

CLI を使用した設定 49

GUI を使用した設定 48

ダイレクトされたローミング要求 139

## ち

チャックポイント、RFID タグ追跡用 194

## て

ディスカバリ要求タイマー、設定 935

ディストリビューション システム ポート 346, 347

データの暗号化 [835, 836, 912](#)

および OfficeExtend アクセス ポイント [912](#)

設定 [835, 836](#)

CLI の使用 [835, 836](#)

GUI の使用 [835](#)

デバイス証明書 [220, 222](#)

概要 [220](#)

ダウンロード [220, 222](#)

GUI の使用 [220, 222](#)

デバッグ コマンド、送信 [883](#)

デバッグ ファシリティ [329, 330](#)

説明 [329, 330](#)

デバッグ ファシリティの設定 [331](#)

デフォルトグループ アクセス ポイント グループ [760](#)

デフォルトの enable パスワード [853](#)

## と

動的 AP 管理 [356, 373](#)

管理インターフェイス [356](#)

動的インターフェイス [373](#)

動的 AP マネージャ インターフェイス [350](#)

動的インターフェイスの例 [360](#)

動的チャンネル割り当て (DCA) [1012, 1022, 1023, 1028, 1030](#)

40 MHz チャネルライゼーション [1022](#)

設定 [1023, 1028, 1030](#)

CLI の使用 [1028, 1030](#)

GUI の使用 [1023](#)

説明 [1012](#)

ドメイン ネーム サーバ (DNS) ディスカバリ [838](#)

トラップ ログ [908](#)

OfficeExtend アクセス ポイントの [908](#)

トラブルシューティング [297, 318, 879, 883](#)

CCXv5 クライアント [318](#)

アクセス ポイント join プロセス [879, 883](#)

問題 [297](#)

トンネル属性、Identity ネットワーキング [555](#)

## に

日本の国番号 [946](#)

認証されたローカル認証バインド方式 [482, 484](#)

## は

パケット キャプチャ ファイル [313, 314, 316](#)

Wireshark でのサンプル出力 [314](#)

アップロード [316](#)

CLI の使用 [316](#)

説明 [313](#)

パスワード [298](#)

クリア テキストでの表示 [298](#)

パスワードのガイドライン [858](#)

パッシング クライアント [791](#)

## ひ

ピアツーピア ブロック [678](#)

説明 [678](#)

日付 [46](#)

NTP サーバでの設定 [46](#)

評価ライセンス [60](#)

5500 シリーズ コントローラにインストールされた [60](#)

## ふ

ファイル転送 [13](#)

フィルタ、クライアントの表示用 [976](#)

フェールオーバーの保護 [14](#)

負荷ベース CAC [160, 163](#)

説明 [160](#)

有効化 [163](#)

GUI の使用 [163](#)

複数の AP マネージャ インターフェイスの作成 (CLI) [385](#)

複数の AP マネージャ インターフェイスの作成 (GUI) [384](#)

複数の Country Code [947, 948](#)

設定 [947, 948](#)

CLI の使用 [948](#)

GUI の使用 [947, 948](#)

不正なアクセス ポイント [566, 569, 1039](#)

アラーム [1039](#)

自動的な阻止 [566, 569](#)

CLI の使用 [569](#)

GUI の使用 [566](#)

不正の検出 [567, 912](#)

および OfficeExtend アクセス ポイント [912](#)

不正の状態 [576](#)

プレダウロードのガイドラインおよび制限事項 [209](#)

プローブ要求、説明 [955](#)

## ほ

ポート **375**  
 設定 **375**

## ま

マルチキャスト VLAN **398**  
 GUI の使用 **398**  
 マルチキャスト クライアント テーブル、表示 **128**  
 マルチキャスト最適化 **397**  
 マルチキャスト モード **121, 123, 124**  
 説明 **121, 123**  
 注意事項 **124**

## む

無効なクライアント、タイムアウトの設定 **669**  
 無線コア ダンプ **884, 885**  
 アップロード **885**  
 GUI の使用 **885**  
 説明 **884**  
 無線スニファ **335, 336**  
 サポート対象のソフトウェア **335**  
 設定 **336**  
 GUI の使用 **336**  
 前提条件 **335**  
 無線測定要求 **1049, 1051, 1052**  
 CLI を使用した状態の表示 **1052**  
 概要 **1049**  
 設定 **1051**  
 CLI で **1051**  
 GUI で **1051**  
 無線による管理 **517**  
 説明 **517**  
 無線リソース管理 (RRM) の設定 **1031**  
 CLI を使用した表示 **1031**  
 無線リソースの監視 **1010**

## め

メッセージのログ **299, 302, 306**  
 設定 **299**  
 GUI の使用 **299**

メッセージのログ (続き)  
 表示 **302, 306**  
 CLI の使用 **306**  
 GUI の使用 **302**

メモリ **13**  
 タイプ **13**  
 メモリ リーク、モニタ **316**

## も

モニタリング **1087**  
 モビリティ **1155**  
 概要 **1155**  
 モビリティ ping テスト、実行 **1185**  
 モビリティ アンカー。「自動アンカー モビリティ」を参照 **1175**  
 モビリティ グループ **1034, 1159, 1162**  
 RF グループとの違い **1034**  
 図示 **1159**  
 内部でのメッセージング **1162**  
 モビリティ グループの NAT デバイス **1162**  
 モビリティを使用したプロアクティブ キー キャッシング (PKC) **1162**

## ゆ

有線ゲスト アクセス **273, 274**  
 設定の概要 **274**  
 説明 **273, 274**  
 ユニキャスト モード **121**

## ら

ライセンス **61, 62, 63, 64, 65, 73, 74, 76, 77**  
 RMA 後の交換コントローラへの転送 **77**  
 SKU **62**  
 インストール **63, 64**  
 CLI の使用 **63, 64**  
 GUI の使用 **63**  
 再ホスト **73, 74, 76**  
 GUI の使用 **74, 76**  
 説明 **73**  
 削除 **63, 64**  
 CLI の使用 **63**  
 GUI の使用 **64**

## ライセンス (続き)

取得 [61, 62](#)表示 [65](#)CLI の使用 [65](#)保存 [63, 64](#)CLI の使用 [64](#)GUI の使用 [63](#)ライセンスの再ホスト。「ライセンス」を参照 [74](#)

## リ

リリース間モビリティ [1163](#)リンク集約 (LAG) [377, 378](#)図示 [378](#)説明 [377, 378](#)リンク遅延 [912, 963](#)および OfficeExtend アクセス ポイント [912](#)説明 [963](#)リンクテスト [959, 960, 961](#)オプション [960](#)実施 [960, 961](#)CLI の使用 [961](#)GUI の使用 [960](#)パケットのタイプ [959](#)ボタン [960](#)

## れ

レイヤ 2 [7](#)動作 [7](#)レイヤ 2 ACL の AP への適用 [537](#)レイヤ 2 ACL の設定 - GUI [535](#)レイヤ 3 [7, 424](#)セキュリティ [424](#)説明 [424](#)動作 [7](#)

## ろ

ローカル EAP [489, 498, 499, 500](#)CLI を使用した情報の表示 [498](#)デバッグ [499, 500](#)例 [489](#)ローカルで有効な証明書 (LSC) [871, 873](#)設定 [871, 873](#)GUI の使用 [871, 873](#)説明 [871](#)ローカル認証、ローカル スイッチング [1101](#)ローカル ユーザ データベース、キャパシティ [237](#)ローミング診断とリアルタイム診断 [325, 326](#)説明 [325](#)ログ [326](#)説明 [326](#)表示 [326](#)ローミングの最適化 [1055](#)ローミングの最適化の設定 [1056](#)GUI の使用 [1056](#)ローミング理由レポート [139](#)ログ [307, 309, 326](#)RSNA [326](#)アップロード [307, 309](#)CLI の使用 [309](#)GUI の使用 [307](#)ログインバナー ファイル [217, 218, 219, 220](#)クリア [220](#)説明 [217](#)ダウンロード [218, 219](#)CLI の使用 [219](#)GUI の使用 [218, 219](#)ロケーション [1050](#)調整 [1050](#)

## わ

ワークグループブリッジ (WGB) [898, 909, 915, 916, 921, 922, 925, 926](#)図示 [898, 909, 915, 916, 922](#)ステータスの表示 [925, 926](#)CLI の使用 [926](#)GUI の使用 [925, 926](#)設定例 [925](#)説明 [921](#)デバッグ [926](#)ワールドモード [80, 82](#)ワイヤレス侵入防御システム (wIPS) [619](#)説明 [619](#)

