Cisco Wireless LAN Controller コンフィギュレーション ガイド リリース 7.3

初版：2012 年 08 月 28 日

最終更新：2012 年 11 月 09 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/

Text Part Number: OL-27510-01-J

【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。

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

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

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

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

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

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

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。 マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。 説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに li

対象読者 li

マニュアルの構成 li

表記法 liii

関連資料 lv

マニュアルの入手方法およびテクニカル サポート lvi

概要 1

Cisco Unified Wireless Network ソリューションの概要 1

シングルコントローラ展開 2

マルチコントローラ展開 3

オペレーティング システム ソフトウェア 4

オペレーティング システムのセキュリティ 4

Cisco WLAN ソリューションの有線セキュリティ 5

レイヤ 2 およびレイヤ 3 の動作 5

動作上の要件 6

設定要件 6

Cisco ワイヤレス LAN コントローラ 6

クライアント ロケーション 7

コントローラ プラットフォーム 7

Cisco 2500 シリーズ コントローラ 8

サポートされない機能 8

Cisco 5500 シリーズ コントローラ 9

サポートされない機能 9

Cisco Flex 7500 シリーズ コントローラ 9

サポートされない機能 10

Cisco 8500 シリーズ コントローラ 11

サポートされない機能 12
Cisco Virtual Wireless LAN Controller 12
サポートされない機能 12
Cisco Wireless Services Module 2 13
サポートされない機能 13
Cisco Services Ready Engine（SRE）の Cisco Wireless Controller 14
サポートされない機能 14
Cisco UWN ソリューション無線 LAN 15
ファイル転送 15
Power Over Ethernet 15
Cisco Wireless LAN Controller のメモリ 16
Cisco Wireless LAN Controller のフェールオーバーの保護 16
Web ブラウザと CLI インターフェイスの使用方法 19
設定ウィザードを使用したコントローラの設定 20
コントローラのコンソール ポートの接続 20
コントローラの設定（GUI） 21
その他の関連資料 32
コントローラの設定：CLI 設定ウィザードの使用 33
コントローラ Web GUI の使用方法 36
注意事項および制約事項 36
GUI へのログイン 37
GUI からのログアウト 37
Web モードおよびセキュア Web モードの有効化 37
Web モードおよびセキュア Web モードの有効化（GUI） 38
Web モードおよびセキュア Web モードの有効化（CLI） 39
外部で生成した SSL 証明書のロード 40
外部で生成した SSL 証明書について 40
SSL 証明書のロード（GUI） 41
SSL 証明書のロード（CLI） 42
コントローラ CLI の使用方法 43
コントローラ CLI へのログイン 43
注意事項および制約事項 43
ローカル シリアル接続の使用方法 44

リモート イーサネット接続の使用方法 45
CLI からのログアウト 46
CLI のナビゲーション 46
設定のないコントローラでの AutoInstall 機能の使用 47
AutoInstall 機能について 47
注意事項および制約事項 47
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 48
設定ファイルの選択 49
AutoInstall の操作例 50
その他の関連資料 51
コントローラのシステムの日時の管理 51
コントローラのシステムの日時について 51
注意事項および制約事項 51
日時を取得するための NTP サーバの設定 51
NTP 認証の設定（GUI） 52
NTP 認証の設定（CLI） 52
日時の設定（GUI） 53
日時の設定（CLI） 54
Telnet および Secure Shell セッションの設定 56
Telnet と SSH について 56
注意事項および制約事項 56
Telnet および SSH セッションの設定（GUI） 57
Telnet および SSH セッションの設定（CLI） 58
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 60
注意事項および制約事項 60
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） 61
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） 61
コントローラの無線管理 62
ワイヤレス接続の有効化（GUI） 63

ワイヤレス接続の有効化（CLI） 63
ポートとインターフェイスの設定 65
ポートとインターフェイスの概要 66
ポートについて 66
ディストリビューション システム ポートについて 67
注意事項および制約事項 67
サービス ポートについて 68
インターフェイスに関する情報 68
注意事項および制約事項 69
管理インターフェイスの設定 70
管理インターフェイスについて 70
管理インターフェイスの設定（GUI） 71
管理インターフェイスの設定（CLI） 72
AP マネージャ インターフェイスの設定 73
AP マネージャ インターフェイスについて 73
注意事項および制約事項 74
AP マネージャ インターフェイスの設定（GUI） 74
AP マネージャ インターフェイスの設定（CLI） 75
仮想インターフェイスの設定 76
仮想インターフェイスについて 76
仮想インターフェイスの設定（GUI） 77
仮想インターフェイスの設定（CLI） 77
サービス ポート インターフェイスの設定 78
サービス ポート インターフェイスについて 78
注意事項および制約事項 78
サービス ポート インターフェイスの設定（GUI） 78
サービス ポート インターフェイスの設定（CLI） 78
動的インターフェイスの設定 79
動的インターフェイスについて 79
注意事項および制約事項 80
動的インターフェイスの設定（GUI） 80
動的インターフェイスの設定（CLI） 82

動的 AP 管理について 83
WLAN について 83
ポートの設定（GUI） 85
ポートのミラーリングの設定 86
ポートのミラーリングについて 86
注意事項および制約事項 87
ポート ミラーリングの有効化（GUI） 87
Cisco 5500 シリーズ コントローラの USB コンソール ポートの使用 88
USB コンソール OS の互換性 88
Cisco USB システム管理コンソールの COM ポートの未使用ポートへの変更 89
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 90
リンク集約の設定 90
リンク集約について 90
注意事項および制約事項 90
リンク集約の有効化（GUI） 93
リンク集約の有効化（CLI） 93
リンク集約の設定の確認（CLI） 93
リンク集約をサポートするための隣接デバイスの設定 93
複数の AP マネージャ インターフェイスの設定 94
複数の AP マネージャ インターフェイスについて 94
注意事項および制約事項 94
複数の AP マネージャ インターフェイスの作成（GUI） 95
複数の AP マネージャ インターフェイスの作成（CLI） 96
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 96
VLAN Select の設定 98
VLAN Select について 98
注意事項および制約事項 99
インターフェイス グループの設定 99
インターフェイス グループについて 99
インターフェイス グループの作成（GUI） 100
インターフェイス グループの作成（CLI） 100
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） 100

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） 101
インターフェイス グループ内の VLAN の表示（CLI） 101
WLAN へのインターフェイス グループの追加（GUI） 101
WLAN へのインターフェイス グループの追加（CLI） 101
マルチキャスト最適化 102
マルチキャスト最適化について 102
マルチキャスト VLAN の設定（GUI） 102
マルチキャスト VLAN の設定（CLI） 103
コントローラ設定の構成 105
ライセンスのインストールおよび設定 106
ライセンスのインストールおよび設定に関する情報 106
ライセンスに関する注意事項および制限事項 106
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 108
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 108
PAK 証明書の取得と登録 109
ライセンスのインストール 110
ライセンスのインストール（GUI） 110
ライセンスのインストール（CLI） 111
ライセンスの表示 111
ライセンスの表示（GUI） 111
ライセンスの表示（CLI） 112
ライセンスの問題のトラブルシューティング 115
ap-count 評価ライセンスのアクティブ化 116
ap-count 評価ライセンスのアクティブ化に関する情報 116
ap-count 評価ライセンスのアクティブ化（GUI） 116
ap-count 評価ライセンスのアクティブ化（CLI） 117
ライセンスの再ホスト 118
ライセンスの再ホストについて 119
ライセンスの再ホスト 119
ライセンスの再ホスト（GUI） 119
ライセンスの再ホスト（CLI） 121

RMA 後にライセンスを交換コントローラに転送する 122
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 122
RMA 後の交換コントローラへのライセンスの転送 123
ライセンス エージェントの設定 123
ライセンス エージェントの設定について 123
ライセンス エージェントの設定（GUI） 124
ライセンス エージェントの設定（CLI） 125
802.11 帯域の設定 126
802.11 帯域の設定について 126
802.11 帯域の設定（GUI） 127
802.11 帯域の設定（CLI） 128
802.11n のパラメータの設定 130
802.11n のパラメータの設定について 130
802.11n のパラメータの設定（GUI） 131
802.11n のパラメータの設定（CLI） 132
その他の関連資料 134
802.11h のパラメータの設定 134
802.11h のパラメータの設定について 134
802.11h のパラメータの設定（GUI） 134
802.11h のパラメータの設定（CLI） 135
DHCP プロキシの設定 136
DHCP プロキシの設定について 136
注意事項および制約事項 136
DHCP プロキシの設定 136
DHCP プロキシの設定（GUI） 136
DHCP プロキシの設定（CLI） 137
DHCP タイムアウトの設定（GUI） 137
DHCP タイムアウトの設定（CLI） 137
管理者のユーザ名とパスワードの設定 137
管理者のユーザ名とパスワードの設定について 137
ユーザ名とパスワードの設定 138
ユーザ名とパスワードの設定（GUI） 138

ユーザ名とパスワードの設定（CLI） 138
パスワードの回復 139
SNMP の設定 139
SNMP の設定（CLI） 139
SNMP コミュニティ ストリング 140
SNMP コミュニティ ストリングのデフォルト値の変更（GUI） 141
SNMP コミュニティ ストリングのデフォルト値の変更（CLI） 141
SNMP v3 ユーザのデフォルト値の変更 142
SNMP v3 ユーザのデフォルト値の変更について 142
SNMP v3 ユーザのデフォルト値の変更（GUI） 143
SNMP v3 ユーザのデフォルト値の変更（CLI） 143
アグレッシブ ロード バランシングの設定 144
アグレッシブなロード バランシングの設定について 144
アグレッシブ ロード バランシングの設定 145
アグレッシブなロード バランシングの設定（GUI） 145
アグレッシブなロード バランシングの設定（CLI） 146
帯域選択の設定 147
帯域選択の設定について 147
注意事項および制約事項 147
帯域選択の設定 148
帯域選択の設定（GUI） 148
帯域選択の設定（CLI） 149
高速 SSID 変更の設定 150
高速 SSID 変更の設定について 150
高速 SSID の設定 150
高速 SSID 変更の設定（GUI） 150
高速 SSID 変更の設定（CLI） 150
802.3X のフロー制御の有効化 150
802.3 ブリッジの設定 151
802.3 ブリッジの設定について 151
注意事項および制約事項 151
802.3 ブリッジの設定 151

802.3 ブリッジの設定（GUI） 151
802.3 ブリッジの設定（CLI） 152
マルチキャスト モードの設定 152
マルチキャスト モードの設定について 152
注意事項および制約事項 154
マルチキャスト モードの設定 156
マルチキャスト モードの有効化（GUI） 156
マルチキャスト モードの有効化（CLI） 156
マルチキャスト グループの表示（GUI） 158
マルチキャスト グループの表示（CLI） 158
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） 159
クライアント ローミングの設定 159
クライアント ローミングについて 159
コントローラ内ローミング 159
コントローラ間ローミング 160
サブネット間ローミング 160
VoIP による通話ローミング 160
CCX レイヤ 2 クライアント ローミング 161
注意事項および制約事項 162
CCX クライアント ローミング パラメータの設定 162
CCX クライアント ローミング パラメータの設定（GUI） 162
CCX クライアント ローミング パラメータの設定（CLI） 163
CCX クライアント ローミング情報の取得（CLI） 163
CCX クライアント ローミング問題のデバッグ（CLI） 164
IP-MAC アドレス バインディングの設定 164
IP-MAC アドレス バインディングの設定について 164
IP-MAC アドレス バインディングの設定 165
IP-MAC アドレス バインディングの設定（CLI） 165
Quality of Service の設定 166
Quality of Service の設定について 166
Quality of Service プロファイルの設定 166
QoS プロファイルの設定（GUI） 166

QoS プロファイルの設定（CLI） 168

Quality of Service ロールの設定 169

Quality of Service ロールの設定について 169

QoS ロールの設定 170

QoS の設定（GUI） 170

QoS ロールの設定（CLI） 171

音声パラメータとビデオ パラメータの設定 172

音声パラメータとビデオ パラメータの設定について 172

コール アドミッション制御 173

帯域幅ベースの CAC 173

負荷ベース CAC 173

Expedited Bandwidth Requests 174

U-APSD 175

Traffic Stream Metrics 176

音声パラメータの設定（GUI） 177

音声パラメータの設定（CLI） 178

ビデオ パラメータの設定 180

ビデオ パラメータの設定（GUI） 180

ビデオ パラメータの設定（CLI） 181

音声設定とビデオ設定の表示 182

音声設定とビデオ設定の表示（GUI） 182

音声設定とビデオ設定の表示（CLI） 183

SIP ベースの CAC の設定 187

注意事項および制約事項 187

SIP ベースの CAC の設定（GUI） 187

SIP ベースの CAC の設定（CLI） 187

メディア パラメータの設定 188

メディア パラメータの設定（GUI） 188

優先コール番号を使用した音声優先制御の設定 189

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 189

注意事項および制約事項 189

優先コール番号の設定 190

優先コール番号の設定（GUI） 190

優先コール番号の設定（CLI） 190
EDCA パラメータの設定 191
EDCA パラメータについて 191
EDCA パラメータの設定 191
EDCA パラメータの設定（GUI） 191
EDCA パラメータの設定（CLI） 192
Cisco Discovery Protocol の設定 193
Cisco Discovery Protocol の設定について 193
注意事項および制約事項 194
Cisco Discovery Protocol の設定 195
Cisco Discovery Protocol の設定（GUI） 195
Cisco Discovery Protocol の設定（CLI） 197
Cisco Discovery Protocol 情報の表示 198
Cisco Discovery Protocol 情報の表示（GUI） 198
Cisco Discovery Protocol 情報の表示（CLI） 200
CDP デバッグ情報の取得 201
コントローラと NTP サーバの認証の設定 202
コントローラと NTP サーバの認証の設定について 202
コントローラと NTP サーバの認証の設定 202
NTP サーバの認証の設定（GUI） 202
NTP サーバの認証の設定（CLI） 202
RFID タグ追跡の設定 203
RFID タグ追跡の設定について 203
RFID タグ追跡の設定 204
RFID タグ追跡の設定（CLI） 204
RFID タグ追跡情報の表示（CLI） 205
RFID タグ追跡問題のデバッグ（CLI） 207
ロケーション設定の実行および表示 207
ロケーション設定の実行および表示について 207
コントローラと Mobility Services Engine の同期 207
ロケーションの設定 208
ロケーションの設定（CLI） 208

ロケーション設定の表示（CLI） 210
クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI） 212
NMSP 設定の表示（CLI） 213
NMSP のデバッグについて 216
コントローラのデフォルト設定へのリセット 217
コントローラのデフォルト設定へのリセットについて 217
コントローラのデフォルト設定へのリセット 217
コントローラのデフォルト設定へのリセット（GUI） 217
コントローラのデフォルト設定へのリセット（CLI） 217
VideoStream の設定 219
VideoStream について 219
注意事項および制約事項 219
VideoStream の設定 220
VideoStream（GUI）の設定 220
VideoStream の設定（CLI） 224
メディア ストリームの表示とデバッグ 225
セキュリティ ソリューションの設定 227
Cisco Unified Wireless Network Solution セキュリティ 228
セキュリティの概要 228
レイヤ 1 ソリューション 228
レイヤ 2 ソリューション 228
注意事項および制約事項 229
レイヤ 3 ソリューション 229
統合されたセキュリティ ソリューション 229
RADIUS の設定 230
RADIUS について 230
注意事項および制約事項 230
ACS 上での RADIUS の設定 232
RADIUS の設定（GUI） 233
RADIUS の設定（CLI） 238
アクセス ポイントによって送信される RADIUS 認証属性 241

RADIUS アカウンティング属性 244
TACACS+ の設定 245
TACACS+ について 245
TACACS+ VSA 247
注意事項および制約事項 247
ACS 上での TACACS+ の設定 248
TACACS+ の設定（GUI） 250
TACACS+ の設定（CLI） 252
TACACS+ 管理サーバのログの表示 253
最大ローカル データベース エントリの設定 255
最大ローカル データベース エントリの設定について 255
最大ローカル データベース エントリの設定（GUI） 256
最大ローカル データベース エントリの設定（CLI） 256
コントローラでのローカル ネットワーク ユーザの設定 256
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 256
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） 257
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） 258
その他の関連資料 259
パスワード ポリシーの設定 259
パスワード ポリシーについて 259
パスワード ポリシーの設定（GUI） 260
パスワード ポリシーの設定（CLI） 260
LDAP の設定 261
LDAP について 261
LDAP の設定（GUI） 261
LDAP の設定（CLI） 264
その他の関連資料 266
ローカル EAP の設定 266
ローカル EAP について 266
注意事項および制約事項 267
ローカル EAP の設定（GUI） 268
ローカル EAP の設定（CLI） 272

その他の関連資料 277
SpectraLink 社の NetLink 電話用システムの設定 277
SpectraLink NetLink 電話について 277
SpectraLink 社の NetLink 電話の設定 277
長いプリアンブルの有効化（GUI） 277
長いプリアンブルの有効化（CLI） 278
Enhanced Distributed Channel Access（CLI） 279
RADIUS NAC サポートの設定 279
RADIUS NAC サポートについて 279
デバイス登録 280
中央 Web 認証 280
ローカル Web 認証 280
注意事項および制約事項 281
RADIUS NAC サポートの設定（GUI） 282
RADIUS NAC サポートの設定（CLI） 282
無線による管理機能の使用 282
無線による管理機能について 282
無線による管理機能の有効化（GUI） 283
無線による管理機能の有効化（CLI） 283
動的インターフェイスによる管理機能 283
動的インターフェイスによる管理機能について 283
動的インターフェイスによる管理機能の有効化（CLI） 284
DHCP オプション 82 の設定 284
DHCP オプション 82 について 284
注意事項および制約事項 285
DHCP オプション 82 の設定（GUI） 285
DHCP オプション 82 の設定（CLI） 285
その他の関連資料 286
アクセス コントロール リストの設定と適用 286
アクセス コントロール リストについて 286
注意事項および制約事項 287
アクセス コントロール リストの設定と適用（GUI） 287

アクセス コントロール リストの設定 287

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 290

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 291

WLAN へのアクセス コントロール リストの適用 291

WLAN への事前認証アクセス コントロール リストの適用 292

アクセス コントロール リストの設定と適用（CLI） 292

アクセス コントロール リストの設定 292

アクセス コントロール リストの適用 293

管理フレーム保護の設定 294

管理フレーム保護について 294

注意事項および制約事項 296

管理フレーム保護の設定（GUI） 297

管理フレーム保護の設定の表示（GUI） 297

管理フレーム保護の設定（CLI） 298

管理フレーム保護の設定の表示（CLI） 298

管理フレーム保護の問題のデバッグ（CLI） 298

クライアント除外ポリシーの設定 299

クライアント除外ポリシーの設定（GUI） 299

クライアント除外ポリシーの設定（CLI） 300

Identity ネットワーキングの設定 301

Identity ネットワーキングについて 301

Identity ネットワーキングで使用される RADIUS 属性 302

AAA Override の設定 305

AAA Override について 305

注意事項および制約事項 306

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 306

AAA Override の設定（GUI） 308

AAA Override の設定（CLI） 308

不正なデバイスの管理 308

不正なデバイスについて 308

不正なデバイスの検出 309

注意事項および制約事項 309

WCS の相互作用と不正の検出 310
不正検出の設定（GUI） 311
不正検出の設定（CLI） 313
不正なアクセス ポイントの分類 315
不正なアクセス ポイントの分類について 315
不正分類ルールの設定（GUI） 319
不正なデバイスの表示および分類（GUI） 322
不正分類ルールの設定（CLI） 325
不正なデバイスの表示および分類（CLI） 328
Cisco TrustSec SXP の設定 333
Cisco TrustSec SXP について 333
注意事項および制約事項 334
Cisco TrustSec SXP の設定（GUI） 335
新規 SXP 接続の作成（GUI） 336
Cisco TrustSec SXP の設定（CLI） 336
Cisco Intrusion Detection System の設定 337
Cisco Intrusion Detection System について 337
回避クライアント 337
その他の情報 338
IDS センサーの設定（GUI） 338
回避クライアントの表示（GUI） 339
IDS センサーの設定（CLI） 339
回避クライアントの表示（CLI） 341
IDS シグニチャの設定 341
IDS シグニチャについて 341
IDS シグニチャの設定（GUI） 344
IDS シグニチャのアップロードまたはダウンロード 344
IDS シグニチャの有効化または無効化 346
IDS シグニチャ イベントの表示（GUI） 348
IDS シグニチャの設定（CLI） 349
IDS シグニチャ イベントの表示（CLI） 350
wIPS の設定 352

wIPS について 352

注意事項および制約事項 356

アクセス ポイントでの wIPS の設定（GUI） 357

アクセス ポイントでの wIPS の設定（CLI） 357

wIPS 情報の表示（CLI） 358

Wi-Fi Direct クライアント ポリシーの設定 360

Wi-Fi Direct クライアント ポリシーについて 360

注意事項および制約事項 360

Wi-Fi Direct クライアント ポリシーの設定（GUI） 360

Wi-Fi Direct クライアント ポリシーの設定（CLI） 361

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） 361

Web 認証プロキシの設定 361

Web 認証プロキシについて 361

Web 認証プロキシの設定（GUI） 363

Web 認証プロキシの設定（CLI） 363

意図的な悪用の検出 364

WLAN の使用 365

WLAN について 366

注意事項および制約事項 366

WLAN の作成 369

WLAN の作成および削除（GUI） 369

WLAN の有効化および無効化（GUI） 370

WLAN の作成および削除（CLI） 370

WLAN の有効化および無効化（CLI） 371

WLAN の表示（CLI） 371

WLAN の検索（GUI） 372

WLAN ごとのクライアント カウントの設定 372

WLAN ごとのクライアント カウントの設定について 372

注意事項および制約事項 372

WLAN ごとのクライアント カウントの設定（GUI） 373

WLAN ごとの最大クライアント数の設定（CLI） 373

各 WLAN の AP 無線ごとの最大クライアント数の設定（GUI） 374

各 WLAN の AP 無線ごとの最大クライアント数の設定（CLI） 374
DHCP の設定 374
Dynamic Host Configuration Protocol について 374
内部 DHCP サーバ 375
外部 DHCP サーバ 375
DHCP Assignment 376
注意事項および制約事項 376
DHCP の設定（GUI） 377
DHCP の設定（CLI） 378
DHCP のデバッグ（CLI） 378
DHCP スコープの設定 379
DHCP スコープについて 379
注意事項および制約事項 379
DHCP スコープの設定（GUI） 379
DHCP スコープの設定（CLI） 380
WLAN の MAC フィルタリングの設定 382
WLAN の MAC フィルタリングについて 382
MAC フィルタリングの有効化 382
ローカル MAC フィルタの設定 382
ローカル MAC フィルタについて 382
ローカル MAC フィルタの設定（CLI） 383
注意事項および制約事項 383
無効なクライアントのタイムアウトの設定 383
無効なクライアントのタイムアウトの設定（CLI） 383
インターフェイスへの WLAN の割り当て 384
DTIM period の設定 384
DTIM period について 384
注意事項および制約事項 385
DTIM period の設定（GUI） 386
DTIM period の設定（CLI） 386
ピアツーピア ブロッキングの設定 387
ピアツーピア ブロッキングについて 387

注意事項および制約事項 389
ピアツーピア ブロッキングの設定（GUI） 389
ピアツーピア ブロッキングの設定（CLI） 390
レイヤ 2 セキュリティの設定 390
Static WEP キーの設定（CLI） 390
802.1X 動的キーおよび認可の設定（CLI） 391
802.11r BSS の高速移行の設定 392
802.11r の高速移行について 392
注意事項および制約事項 392
802.11r の高速移行の設定（GUI） 394
802.11r の高速移行の設定（CLI） 394
802.11r BSS の高速移行のトラブルシューティング 395
802.1X 認証への MAC 認証フェールオーバーの設定 396
802.1X 認証への MAC 認証フェールオーバーの設定（GUI） 396
802.1X 認証への MAC 認証フェールオーバーの設定（CLI） 396
Static WEP と Dynamic WEP の両方をサポートする WLAN の設定 397
Static WEP と Dynamic WEP の両方をサポートする WLAN について 397
WPA1 と WPA2 397
注意事項および制約事項 398
WPA1 +WPA2 の設定 399
WPA1+WPA2 の設定（GUI） 399
WPA1+WPA2 の設定（CLI） 400
Sticky PMKID キャッシュの設定 401
sticky PMKID キャッシュについて 401
注意事項および制約事項 402
Sticky PMKID キャッシュの設定（CLI） 402
CKIP の設定 403
CKIP について 403
CKIP の設定（GUI） 405
CKIP の設定（CLI） 405
セッション タイムアウトの設定 406
セッション タイムアウトについて 406

セッション タイムアウトの設定 406
セッション タイムアウトの設定（GUI） 406
セッション タイムアウトの設定（CLI） 407
VPN パススルーを使用したレイヤ 3 セキュリティの設定 408
VPN パススルーについて 408
注意事項および制約事項 408
VPN パススルーの設定 408
VPN パススルーの設定（GUI） 408
VPN パススルーの設定（CLI） 409
Web 認証を使用したレイヤ 3 セキュリティの設定 409
Web 認証について 409
注意事項および制約事項 409
その他の情報 410
Web 認証の設定 410
Web 認証の設定（GUI） 410
Web 認証の設定（CLI） 410
キャプティブ バイパスの設定 412
キャプティブ バイパスについて 412
キャプティブ バイパスの設定（CLI） 412
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 413
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 413
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） 413
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） 414
WLAN への QoS プロファイルの割り当て 415
QoS プロファイルについて 415
WLAN への QoS プロファイルの割り当て（GUI） 416
WLAN への QoS プロファイルの割り当て（CLI） 417
QoS Enhanced BSS の設定 418
QoS Enhanced BSS について 418

注意事項および制約事項 419

その他の情報 420

QBSS の設定（GUI） 420

QBSS の設定（CLI） 421

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 422

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 422

注意事項および制約事項 422

メディア セッション スヌーピングの設定（GUI） 423

メディア セッション スヌーピングの設定（CLI） 423

Key Telephone System-Based CAC の設定 427

Key Telephone System-Based CAC について 427

注意事項および制約事項 428

KTS-based CAC の設定（GUI） 428

KTS-based CAC の設定（CLI） 429

関連コマンド 430

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 430

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 430

注意事項および制約事項 431

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） 431

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） 431

シームレスな IPv6 モビリティの設定 432

IPv6 モビリティについて 432

注意事項および制約事項 432

IPv6 クライアントのための RA ガードの設定 433

RA ガードについて 433

RA ガードの設定（GUI） 434

RA ガードの設定（CLI） 434

IPv6 クライアントのための RA スロットリングの設定 434

RA スロットリングについて 434

RA スロットリングの設定（GUI） 434

RA スロットル ポリシーの設定（CLI） 435

IPv6 ネイバー ディスカバリ キャッシングの設定 436

IPv6 ネイバー ディスカバリについて 436
ネイバー バインディング タイマーの設定（GUI） 436
ネイバー バインディング タイマーの設定（CLI） 436
Cisco Client Extensions の設定 437
Cisco Client Extensions について 437
注意事項および制約事項 437
CCX Aironet IE の設定（GUI） 438
クライアントの CCX バージョンの表示（GUI） 438
CCX Aironet IE の設定（CLI） 438
クライアントの CCX バージョンの表示（CLI） 439
リモート LAN の設定 439
リモート LAN について 439
注意事項および制約事項 439
リモート LAN の設定 439
リモート LAN の設定（GUI） 439
リモート LAN の設定（CLI） 440
AP グループの設定 441
アクセス ポイント グループについて 441
注意事項および制約事項 443
アクセス ポイント グループの設定 444
アクセス ポイント グループの作成（GUI） 444
アクセス ポイント グループの作成（CLI） 446
アクセス ポイント グループの表示（CLI） 447
RF プロファイルの設定 448
RF プロファイルについて 448
注意事項および制約事項 451
RF プロファイルの設定（GUI） 451
RF プロファイルの設定（CLI） 453
AP グループへの RF プロファイルの適用（GUI） 454
AP グループへの RF プロファイルの適用（CLI） 455
802.1X 認証を使用した Web リダイレクトの設定 455
802.1X 認証を使用した Web リダイレクトについて 455

条件付き Web リダイレクト 455
スプラッシュ ページ Web リダイレクト 456
RADIUS サーバの設定（GUI） 456
Web リダイレクトの設定 457
Web リダイレクトの設定（GUI） 457
Web リダイレクトの設定（CLI） 457
WLAN ごとのアカウンティング サーバの無効化（GUI） 458
WLAN ごとのカバレッジ ホールの検出の無効化 458
WLAN 上のカバレッジ ホールの検出の無効化（GUI） 459
WLAN 上のカバレッジ ホールの検出の無効化（CLI） 459
NAC アウトオブバンド統合の設定 460
NAC アウトオブバンド統合について 460
注意事項および制約事項 461
NAC アウトオブバンド統合の設定 462
NAC アウトオブバンド統合の設定（GUI） 462
NAC アウトオブバンド統合の設定（CLI） 464
パッシブ クライアントの設定 465
パッシブ クライアントについて 465
注意事項および制約事項 465
パッシブ クライアントの設定（GUI） 466
マルチキャスト-マルチキャスト モードの有効化（GUI） 467
コントロールでのグローバル マルチキャスト モードの有効化（GUI） 468
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） 468
パッシブ クライアントの設定（CLI） 468
クライアント プロファイルの設定 469
クライアント プロファイルについて 469
注意事項および制約事項 469
クライアント プロファイルの設定 470
クライアント プロファイルの設定（GUI） 470
クライアント プロファイルの設定（CLI） 471
WLAN ごとの RADIUS 送信元サポートの設定 471
WLAN ごとの RADIUS 送信元サポートについて 471

注意事項および制約事項 472
WLAN ごとの RADIUS 送信元サポートの設定（CLI） 472
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） 473
リモート LAN の設定 473
リモート LAN について 473
注意事項および制約事項 473
リモート LAN の設定 474
リモート LAN の設定（GUI） 474
リモート LAN の設定（CLI） 475
Lightweight アクセス ポイントの制御 477
アクセス ポイント通信プロトコル 478
アクセス ポイント通信プロトコルについて 478
注意事項および制約事項 479
データ暗号化の設定 479
データ暗号化のためのガイドライン 479
Cisco 5500 シリーズ コントローラ用 DTLS イメージをアップグレードまたはダウングレード 481
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 481
データ暗号化の設定（GUI） 481
データ暗号化の設定（CLI） 482
CAPWAP の最大伝送単位情報の表示 483
CAPWAP のデバッグ 483
コントローラ ディスカバリ プロセス 484
注意事項および制約事項 484
アクセス ポイントのコントローラへの join の確認 485
アクセス ポイントのコントローラへの join の確認（GUI） 485
アクセス ポイントのコントローラへの join の確認（CLI） 486
アクセス ポイントの検索 486
アクセス ポイントの検索について 486
AP フィルタの検索（GUI） 487
インターフェイスの詳細の監視 490

アクセス ポイント無線の検索 492
アクセス ポイント無線の検索について 492
アクセス ポイント無線の検索（GUI） 492
アクセス ポイントのグローバル クレデンシャルの設定 494
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 494
注意事項および制約事項 494
アクセス ポイントのグローバル資格情報の設定（GUI） 495
アクセス ポイントのグローバル資格情報の設定（CLI） 496
アクセス ポイントの認証の設定 497
アクセス ポイントに対する認証の設定について 497
注意事項および制約事項 497
アクセス ポイントの認証を設定するための前提条件 498
アクセス ポイントの認証の設定 498
アクセス ポイントの認証の設定（GUI） 498
アクセス ポイントの認証の設定（CLI） 499
スイッチの認証の設定 501
組み込みアクセス ポイントの設定 501
組み込みアクセス ポイントについて 501
注意事項および制約事項 501
その他の関連資料 503
自律アクセス ポイントの Lightweight モードへの変換 503
自律アクセス ポイントの Lightweight モードへの変換について 503
注意事項および制約事項 503
Lightweight モードから Autonomous モードへの復帰 504
以前のリリース（CLI）への復帰 504
MODE ボタンと TFTP サーバを使用して前のリリースへの復帰 504
アクセス ポイントの認可 505
SSC を使用したアクセス ポイントの認可 505
SSC を使用する仮想コントローラのアクセス ポイントの認可 505
SSC（GUI）の設定 506
SSC の設定（CLI） 506
MIC を使用したアクセス ポイントの認可 506

LSC を使用したアクセス ポイントの認可 507
ローカルで有効な証明書（GUI）の設定 508
ローカルで有効な証明書（CLI）の設定 509
アクセス ポイントの認可（GUI） 511
アクセス ポイントの認可（CLI） 511
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 512
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 512
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） 512
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） 513
DHCP オプション 43 および DHCP オプション 60 の使用 513
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 514
アクセス ポイントの Syslog サーバの設定（CLI） 516
アクセス ポイントの join 情報の表示 517
アクセス ポイントの join 情報の表示（GUI） 517
アクセス ポイントの join 情報の表示（CLI） 518
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 519
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 519
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 520
無線コア ダンプの取得（CLI） 520
無線コア ダンプのアップロード（GUI） 521
無線コア ダンプのアップロード（CLI） 521
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 522
アクセス ポイントのコア ダンプのアップロード（GUI） 522
アクセス ポイントのコア ダンプのアップロード（CLI） 523
AP クラッシュ ログ情報の表示 523
AP クラッシュ ログ情報の表示（GUI） 523
AP クラッシュ ログ情報の表示（CLI） 524

変換されたアクセス ポイントの MAC アドレスの表示 524
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 524
Lightweight アクセス ポイントでの固定 IP アドレスの設定 525
固定 IP アドレスの設定（GUI） 525
固定 IP アドレスの設定（CLI） 526
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 527
アクセス ポイントの回復：TFTP リカバリ手順の使用 527
OfficeExtend アクセス ポイントの設定 527
OfficeExtend アクセス ポイントについて 527
OEAP 600 シリーズ アクセス ポイント 528
ローカル モードの OEAP 529
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 530
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 531
認証の設定 535
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 536
リモート LAN の設定 536
チャネルの管理と設定 537
その他の注意事項 538
セキュリティの実装 538
OfficeExtend アクセス ポイントのライセンシング 539
OfficeExtend アクセス ポイントの設定 539
OfficeExtend アクセス ポイントの設定（GUI） 539
OfficeExtend アクセス ポイントの設定（CLI） 542
OfficeExtend アクセス ポイントでの個人 SSID の設定 544
OfficeExtend アクセス ポイント統計情報の表示 547
Cisco ワークグループ ブリッジの使用 547
Cisco ワークグループ ブリッジについて 547
注意事項および制約事項 548
WGB の設定例 551

ワークグループ ブリッジのステータスの表示（GUI） 551
ワークグループ ブリッジのステータスの表示（CLI） 552
WGB の問題のデバッグ（CLI） 552
Cisco 以外のワークグループ ブリッジの使用 553
Cisco 以外のワークグループ ブリッジについて 553
注意事項および制約事項 553
バックアップ コントローラの設定 555
バックアップ コントローラの設定について 555
注意事項および制約事項 555
バックアップ コントローラの設定（GUI） 556
バックアップ コントローラの設定（CLI） 558
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 560
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 560
注意事項および制約事項 560
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） 561
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） 561
フェールオーバー プライオリティの設定の表示（CLI） 562
アクセス ポイントの再送信間隔および再試行回数の設定 563
アクセス ポイントの再送信間隔および再試行回数の設定について 563
注意事項および制約事項 563
アクセス ポイントの再送信間隔と再試行回数の設定（GUI） 563
アクセス ポイントの再送信間隔と再試行回数の設定（CLI） 564
国番号の設定 565
国番号の設定について 565
注意事項および制約事項 565
国番号の設定（GUI） 566
国番号の設定（CLI） 568
アクセス ポイントの -J 規制ドメインから -U 規制ドメインへの移行 571
アクセス ポイントの -J 規制ドメインから -U 規制ドメインへの移行について 571
注意事項および制約事項 572
アクセス ポイントの -U 規制ドメインへの移行（CLI） 573
日本での W56 帯域の使用 574

動的周波数選択 575
アクセス ポイントでの RFID トラッキングの最適化 577
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 577
アクセス ポイントでの RFID トラッキングの最適化（GUI） 577
アクセス ポイントでの RFID トラッキングの最適化（CLI） 578
プローブ要求フォワーディングの設定 579
プローブ要求フォワーディングの設定について 579
プローブ要求フォワーディングの設定（CLI） 579
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 580
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 580
コントローラとアクセス ポイント上の Unique Device Identifier の取得（GUI） 581
コントローラとアクセス ポイント上の Unique Device Identifier の取得（CLI） 581
リンク テストの実行 581
リンク テストの実行について 581
リンク テストの実行（GUI） 583
リンク テストの実行（CLI） 583
リンク遅延の設定 584
リンク遅延の設定について 584
注意事項および制約事項 584
リンク遅延の設定（GUI） 585
リンク遅延の設定（CLI） 586
TCP MSS の設定 587
TCP MSS の設定について 587
TCP MSS の設定（GUI） 587
TCP MSS の設定（CLI） 587
Power over Ethernet の設定 588
Power over Ethernet の設定について 588
注意事項および制約事項 589
Power over Ethernet の設定（GUI） 590
Power over Ethernet の設定（CLI） 592
点滅する LED の設定 594
点滅する LED の設定について 594

点滅する LED の設定（CLI） 594

クライアントの表示 595

クライアントの表示（GUI） 595

クライアントの表示（CLI） 597

アクセス ポイントの LED 状態の設定 598

注意事項および制約事項 598

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） 598

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） 598

特定のアクセス ポイントで LED 状態の設定（GUI） 599

特定のアクセス ポイントで LED 状態の設定（CLI） 599

メッシュ アクセス ポイントの制御 601

Cisco Aironet メッシュ アクセス ポイントについて 602

注意事項および制約事項 603

その他の関連資料 603

アクセス ポイントのロール 603

ネットワーク アクセス 604

ネットワークのセグメント化 604

Cisco 屋内メッシュ アクセス ポイント 604

Cisco 屋外メッシュ アクセス ポイント 605

メッシュ導入モード 606

ワイヤレス メッシュ ネットワーク 606

ワイヤレス バックホール 607

ユニバーサル アクセス 607

ポイントツーマルチポイント無線ブリッジング 607

ポイントツーポイント無線ブリッジング 608

メッシュ レンジの設定（CLI） 609

AP1522 レンジ計算ツールの前提条件 610

AP1552 レンジ計算ツールの前提条件 610

アーキテクチャの概要 611

ワイヤレス アクセス ポイントの制御およびプロビジョニング（CAPWAP） 611

Cisco Adaptive Wireless Path Protocol ワイヤレス メッシュ ルーティング 611

メッシュ ネイバー、親、および子 611

設計上の考慮事項 612
無線メッシュの制約 612
ワイヤレス バックホール データ レート 612
ClientLink テクノロジー 616
ClientLink の設定（CLI） 618
ClientLink に関連するコマンド 619
コントローラの計画 620
メッシュ アクセス ポイントのメッシュ ネットワークへの追加 621
MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加 622
コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（GUI） 622
コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（CLI） 623
メッシュ アクセス ポイントのロール定義 624
MAP および RAP とコントローラとのアソシエーションについて 624
AP ロールの設定（GUI） 625
AP ロールの設定（CLI） 625
DHCP 43 および DHCP 60 を使用した複数のコントローラの設定 626
バックアップ コントローラの設定 627
バックアップ コントローラの設定について 627
注意事項および制約事項 627
バックアップ コントローラの設定（GUI） 629
バックアップ コントローラの設定（CLI） 631
RADIUS サーバを使用した外部認証および認可の設定 633
RADIUS サーバの設定 634
RADIUS サーバへのユーザ名の追加 634
メッシュ アクセス ポイントの外部認証の有効化 635
メッシュ アクセス ポイントの外部認証の有効化（GUI） 636
メッシュ アクセス ポイントの外部認証のイネーブル化（CLI） 636
セキュリティ統計の表示 637
グローバル メッシュ パラメータの設定 637
グローバル メッシュ パラメータについて 637

グローバル メッシュ パラメータの設定（GUI） 637
グローバル メッシュ パラメータの設定（CLI） 642
グローバル メッシュ パラメータ設定の表示（CLI） 643
ローカル メッシュ パラメータの設定 644
ワイヤレス バックホール データ レートの設定 645
イーサネット ブリッジングの設定 647
イーサネット ブリッジングの有効化（GUI） 648
ブリッジ グループ名の設定 648
ブリッジ グループ名の設定（CLI） 649
ブリッジ グループ名の確認（GUI） 649
ブリッジ グループ名の確認（CLI） 649
Public Safety 帯域設定の構成 649
4.9 GHz 帯域の有効化 651
Cisco 3200 との相互運用性の設定 651
Public Safety 4.9 GHz 帯域の設定ガイドライン 652
AP1522 が Cisco 3200 とアソシエートできるように設定（GUI） 653
Cisco 3200 と 1522 および 1524PS とのアソシエーションの有効化（CLI） 653
電力およびチャネルの設定 654
電力およびチャネルの設定（GUI） 654
シリアル バックホールでのチャネルの設定（CLI） 655
アンテナ ゲインの設定 656
アンテナ ゲインの設定（GUI） 657
アンテナ ゲインの設定（CLI） 657
シリアル バックホール アクセス ポイントでのバックホール チャネル選択解除 657
バックホール チャネル選択解除の設定（GUI） 658
バックホール チャネル選択解除の設定（CLI） 659
バックホール チャネル選択解除のガイドライン 662
動的チャネル割り当ての設定（GUI） 663
拡張機能の設定 666
バックホール用 2.4 GHz 無線の使用 667

5 GHz から 2.4 GHz へのバックホールの変更 668
2.4 GHz から 5 GHz へのバックホールの変更 668
現在使用中のバックホールの確認 669
ユニバーサル クライアント アクセス 669
ユニバーサル クライアント アクセスの設定（GUI） 669
ユニバーサル クライアント アクセスの設定（CLI） 670
シリアル バックホール アクセス ポイントのユニバーサル クライアント アクセス 670
Extended Universal Access の設定（GUI） 671
Extended Universal Access の設定（CLI） 673
拡張ユニバーサル アクセスの設定：Cisco Prime Infrastructure 674
イーサネット VLAN タギングの設定 674
イーサネット ポートに関する注意 675
イーサネット VLAN タギングのガイドライン 676
VLAN 登録 678
イーサネット VLAN タギングの有効化（GUI） 680
イーサネット VLAN タギングの設定（CLI） 682
イーサネット VLAN タギング設定詳細の表示（CLI） 682
ワークグループ ブリッジとメッシュ インフラストラクチャとの相互運用性 684
ワークグループ ブリッジの設定 685
サポートされるワークグループ ブリッジ モードと容量 686
WGB クライアントのステータスの表示 688
注意事項および制約事項 688
例：ワークグループ ブリッジの設定 689
WGB アソシエーションの確認 691
リンク テストの結果 693
WGB 有線/ワイヤレス クライアント 694
クライアント ローミング 695
WGB ローミングのガイドライン 696
設定例 696
トラブルシューティングのヒント 697
屋内メッシュ ネットワークの音声パラメータの設定 698
CAC 698

QoS および DSCP マーキング 699
カプセル化 699
メッシュ アクセス ポイントでのキューイング 701
ブリッジ バックホール パケット 704
LAN 間のブリッジ パケット 704
メッシュ ネットワークでの音声使用のガイドライン 705
メッシュ ネットワークでの音声コールのサポート 706
メッシュ ネットワークの音声詳細の表示（CLI） 707
ビデオのメッシュ マルチキャストの抑制の有効化 711
メッシュ ネットワークでのマルチキャストの有効化（CLI） 712
IGMP スヌーピング 712
メッシュ AP のローカルで有効な証明書 713
注意事項および制約事項 714
メッシュ AP の LSC と通常の AP の LSC の違い 714
LSC AP での証明書検証プロセス 715
LSC の設定（CLI） 715
LSC 関連のコマンド 717
コントローラ CLI show コマンド 718
コントローラ GUI セキュリティ設定 719
展開ガイドライン 720
スロット バイアス オプション 721
スロット バイアス オプションについて 721
スロット バイアスの無効化 721
注意事項および制約事項 721
スロット バイアスに関連するコマンド 722
優先される親の選択 723
注意事項および制約事項 723
優先される親の設定 723
同一チャネルの干渉 725
メッシュ アクセス ポイントのメッシュ統計情報の表示 725
メッシュ アクセス ポイントのメッシュ統計情報の表示（GUI） 726
メッシュ アクセス ポイントのメッシュ統計情報の表示（CLI） 731

メッシュ アクセス ポイントのネイバー統計情報の表示 732
メッシュ アクセス ポイントのネイバー統計情報の表示（GUI） 733
メッシュ アクセス ポイントのネイバー統計情報の表示（CLI） 735
屋内アクセス ポイントのメッシュ アクセス ポイントへの変換 736
屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更 737
屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更（GUI） 738
屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更（CLI） 738
屋内メッシュ アクセス ポイントの非メッシュ Lightweight アクセス ポイントへの変換（1130AG、1240AG） 739
Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定 740
注意事項および制約事項 740
Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定（GUI） 742
Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定（CLI） 743
コントローラ ソフトウェアと設定の管理 745
コントローラ ソフトウェアのアップグレード 745
コントローラ ソフトウェアのアップグレードに関するガイドライン 746
コントローラ ソフトウェアのアップグレード（GUI） 750
コントローラ ソフトウェアのアップグレード（CLI） 752
アクセス ポイントへのイメージのプレダウンロード 755
アクセス ポイントのプレダウンロードのプロセス 755
注意事項および制約事項 756
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） 757
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） 759
アクセス ポイントへのイメージのプレダウンロード（CLI） 761
コントローラとのファイルのやり取り 764
ログイン バナー ファイルのダウンロード 764
ログイン バナー ファイルのダウンロード（GUI） 765
ログイン バナー ファイルのダウンロード（CLI） 766

ログイン バナーのクリア（GUI） 767
デバイスの証明書のダウンロード 768
デバイスの証明書のダウンロード（GUI） 769
デバイスの証明書のダウンロード（CLI） 769
CA 証明書のダウンロード 771
CA 証明書のダウンロード（GUI） 772
CA 証明書のダウンロード（CLI） 772
PAC のアップロード 774
PAC のアップロード（GUI） 775
PAC のアップロード（CLI） 775
設定ファイルのアップロードおよびダウンロード 777
設定ファイルのアップグレード 777
設定ファイルのアップロード（GUI） 778
設定ファイルのアップロード（CLI） 778
設定ファイルのダウンロード 779
設定ファイルのダウンロード（GUI） 780
設定ファイルのダウンロード（CLI） 781
設定の保存 782
設定ファイルの編集 783
コントローラの設定のクリア 784
コントローラ設定の消去 784
コントローラのリセット 785
ユーザ アカウントの管理 787
ゲスト アカウントの作成について 787
注意事項および制約事項 788
Lobby Ambassador アカウントの作成 788
ロビー アンバサダー アカウントの作成（GUI） 788
ロビー アンバサダー アカウントの作成（CLI） 789
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） 790
ゲスト ユーザ アカウントの表示 791
ゲスト アカウントの表示（GUI） 791
ゲスト アカウントの表示（CLI） 791

Web 認証証明書の入手 792
Web 認証証明書について 792
Web 認証証明書の入手 792
Web 認証証明書の入手（GUI） 792
Web 認証証明書の入手（CLI） 793
Web 認証プロセス 794
注意事項および制約事項 794
デフォルトの Web 認証ログイン ページの選択 796
デフォルトの Web 認証ログイン ページについて 796
注意事項および制約事項 797
デフォルトの Web 認証ログイン ページの選択（GUI） 797
デフォルトの Web 認証ログイン ページの選択（CLI） 798
例：カスタマイズされた Web 認証ログイン ページの作成 800
例：変更されたデフォルトの Web 認証ログイン ページの例 803
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 804
カスタマイズされた Web 認証ログイン ページについて 804
注意事項および制約事項 804
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 804
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） 804
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） 805
その他の関連資料 805
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 806
注意事項および制約事項 806
その他の関連資料 807
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） 807
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） 808
その他の関連資料 809
例：カスタマイズされた Web 認証ログイン ページ 809
Web 認証ログイン ページの設定の確認（CLI） 809
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 810

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 810
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） 810
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） 811
有線ゲスト アクセスの設定 813
有線ゲスト アクセスについて 813
有線ゲストのアクセスを設定するための前提条件 814
注意事項および制約事項 815
有線ゲスト アクセスの設定 816
有線ゲスト アクセスの設定（GUI） 816
有線ゲスト アクセスの設定（CLI） 818
IPv6 クライアントのゲスト アクセスのサポート 823
Radio Resource Management の設定 825
Radio Resource Management について 825
無線リソースの監視 826
送信電力の制御 826
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 827
動的チャネル割り当て 827
カバレッジ ホールの検出と修正 829
RRM の利点 830
注意事項および制約事項 830
RRM の設定 830
RF グループ モードの設定（GUI） 831
RF グループ モードの設定（CLI） 832
送信電力制御の設定（GUI） 833
Off-Channel Scanning Defer の設定 834
Off-Channel Scanning Defer について 834
WLAN に対する Off-Channel Scanning Defer の設定 835
WLAN に対する Off-Channel Scanning Defer の設定（GUI） 835
WLAN に対する Off-Channel Scanning Defer の設定（CLI） 835

動的チャネル割り当ての設定（GUI） 836
カバレッジ ホールの検出の設定（GUI） 841
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） 843
RRM の設定（CLI） 845
RRM 設定の表示（CLI） 849
RRM 問題のデバッグ（CLI） 851
RRM ネイバー ディスカバリ パケットの設定 852
RRM NDP および RF グループ化について 852
RRM NDP の設定（CLI） 852
RF グループの設定 853
RF グループについて 853
RF グループ リーダー 853
RF グループ名 855
RF グループの設定 855
RF グループ名の設定（GUI） 856
RF グループ名の設定（CLI） 856
RF グループ ステータスの表示 856
RF グループ ステータスの表示（GUI） 857
RF グループ ステータスの表示（CLI） 857
RRM の無効化 858
RRM の無効化について 858
注意事項および制約事項 858
アクセス ポイント無線へのチャネルおよび送信電力設定の静的割り当て 859
チャネルおよび送信電力設定の静的割り当て（GUI） 859
チャネルおよび送信電力設定の静的割り当て（CLI） 861
コントローラにおけるチャネルおよびパワーの動的割り当てのグローバルな無効化 864
チャネルおよび電力の動的割り当ての無効化（GUI） 864
チャネルおよび電力の動的割り当ての無効化（CLI） 864
RF グループ内の不正アクセス ポイント検出の設定 865
RF グループ内の不正アクセス ポイント検出について 865
RF グループ内の不正アクセス ポイント検出の設定 865

RF グループ内の不正アクセス ポイント検出の有効化（GUI） 865
RF グループ内の不正アクセス ポイント検出の設定（CLI） 866
CCX 無線管理機能の設定 867
CCX 無線管理機能について 867
無線測定要求 867
ロケーション調整 868
CCX 無線管理の設定 868
CCX 無線管理の設定（GUI） 868
CCX 無線管理の設定（CLI） 869
CCX 無線管理情報の表示（CLI） 869
CCX 無線管理問題のデバッグ（CLI） 871
Cisco CleanAir の設定 873
CleanAir について 873
Cisco CleanAir システムにおけるコントローラの役割 874
Cisco CleanAir で検出できる干渉の種類 874
永続的デバイス 876
永続的デバイスの検出 876
永続的デバイスの伝搬 876
注意事項および制約事項 876
Cisco CleanAir の設定 878
コントローラでの Cisco CleanAir の設定 878
コントローラでの Cisco CleanAir の設定（GUI） 879
コントローラでの Cisco CleanAir の設定（CLI） 881
アクセス ポイントに対する Cisco CleanAir の設定 885
アクセス ポイントに対する Cisco CleanAir の設定（GUI） 885
アクセス ポイントに対する Cisco CleanAir の設定（CLI） 886
干渉デバイスのモニタリング 887
干渉デバイスをモニタリングするための前提条件 887
干渉デバイスのモニタリング（GUI） 887
干渉デバイスのモニタリング（CLI） 889
アクセス ポイントによる干渉源の検出 889
デバイスのタイプによる干渉源の検出 890

永続的干渉源の検出 890
永続的デバイスのモニタリング（GUI） 891
永続的デバイスのモニタリング（CLI） 892
無線帯域の電波品質のモニタリング 892
無線帯域の電波品質のモニタリング（GUI） 892
無線帯域の電波品質のモニタリング（CLI） 893
電波品質のサマリーの表示 893
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 893
ある無線帯域のアクセス ポイントの電波品質の表示 894
無線帯域の電波品質（ワースト ケース）のモニタリング（GUI） 894
無線帯域の電波品質（ワースト ケース）のモニタリング（CLI） 895
電波品質のサマリーの表示（CLI） 895
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） 895
ある無線帯域のアクセス ポイントの電波品質の表示（CLI） 895
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） 896
永続的干渉源の検出（CLI） 897
Spectrum Expert の接続の設定 897
Spectrum Expert の設定（GUI） 898
関連資料 900
CleanAir の機能履歴 900
FlexConnect の設定 901
FlexConnect について 901
FlexConnect 認証プロセス 902
注意事項および制約事項 906
FlexConnect の設定 909
リモート サイトでのスイッチの設定 909
FlexConnect に対するコントローラの設定 910
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） 911
FlexConnect に対するコントローラの設定（GUI） 912
FlexConnect に対するコントローラの設定（CLI） 915

FlexConnect のアクセス ポイントの設定 916
FlexConnect のアクセス ポイントの設定（GUI） 916
FlexConnect のアクセス ポイントの設定（CLI） 918
WLAN 上のローカル認証用のアクセス ポイントの設定（GUI） 920
WLAN 上のローカル認証用のアクセス ポイントの設定（CLI） 921
クライアント デバイスの WLAN への接続 921
FlexConnect ACL の設定 922
アクセス コントロール リストについて 922
注意事項および制約事項 922
FlexConnect ACL の設定 923
FlexConnect ACL の設定（GUI） 923
FlexConnect ACL の設定（CLI） 925
FlexConnect ACL の表示およびデバッグ（CLI） 926
FlexConnect グループの設定 926
FlexConnect グループについて 926
FlexConnect グループおよびバックアップ RADIUS サーバ 927
FlexConnect グループおよび CCKM 927
FlexConnect グループおよび Opportunistic Key Caching 928
FlexConnect グループおよびローカル認証 928
FlexConnect グループの設定（GUI） 929
FlexConnect グループの設定（CLI） 932
FlexConnect グループの VLAN-ACL マッピングの設定（GUI） 934
FlexConnect グループの VLAN-ACL マッピングの設定（CLI） 935
VLAN-ACL マッピングの表示（CLI） 935
FlexConnect の AAA Override の設定 935
AAA Override について 935
注意事項および制約事項 935
アクセス ポイント上の FlexConnect に対する AAA Override の設定（GUI） 936
アクセス ポイント上の FlexConnect に対する VLAN Override の設定（CLI） 937
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 937

FlexConnect AP のアップグレードに関する情報 937
注意事項および制約事項 938
FlexConnect AP のアップグレードの設定（GUI） 938
FlexConnect AP のアップグレードの設定（CLI） 939
モビリティ グループの設定 941
モビリティについて 941
モビリティ グループについて 945
モビリティ グループ内でのメッセージング 947
NAT デバイスでのモビリティ グループの使用 947
モビリティ グループの設定 949
モビリティ グループを設定するための前提条件 949
モビリティ グループの設定（GUI） 951
モビリティ グループの設定（CLI） 954
モビリティ グループの統計の表示 955
モビリティ グループの統計の表示（GUI） 956
モビリティ グループの統計の表示（CLI） 957
自動アンカー モビリティの設定 958
Auto-Anchor モビリティについて 958
注意事項および制約事項 959
自動アンカー モビリティの設定（GUI） 960
自動アンカー モビリティの設定（CLI） 961
WLAN モビリティ セキュリティの値の検証 963
WLAN モビリティ セキュリティの値について 963
シンメトリック モビリティ トンネリングの使用 964
シンメトリック モビリティ トンネリングについて 964
注意事項および制約事項 965
シンメトリック モビリティ トンネリングの確認 965
シンメトリック モビリティ トンネリングの確認（GUI） 965
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） 965
モビリティ ping テストの実行 966
モビリティ ping テストについて 966
注意事項および制約事項 966

モビリティ ping テストの実行（CLI） 967
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 967
スタティック 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 967
スタティック IP クライアントのダイナミック アンカーの機能 968
注意事項および制約事項 968
スタティック IP クライアントのダイナミック アンカーの設定（GUI） 969
スタティック IP クライアントのダイナミック アンカーの設定（CLI） 969
外部マッピングの設定 970
外部マッピングについて 970
外部コントローラの MAC マッピングの設定（GUI） 970
外部コントローラの MAC マッピングの設定（CLI） 970
モバイル コンシェルジュの設定 971
モバイル コンシェルジュについて 971
モバイル コンシェルジュの設定（802.11u） 971
モバイル コンシェルジュの設定（802.11u）（GUI） 971
モバイル コンシェルジュの設定（802.11u）（CLI） 973
802.11u Mobility Services Advertisement Protocol の設定 974
802.11u MSAP について 974
802.11u MSAP の設定（GUI） 974
MSAP の設定（CLI） 975
975
802.11u HotSpot の設定 975
802.11u HotSpot について 975
802.11u Hotspot の設定（GUI） 975
Hotspot 2.0 の設定（CLI） 976
976
アクセス ポイントでの HotSpot2 の設定（GUI） 978
アクセス ポイントでの HotSpot2 の設定（CLI） 979
トラブルシューティング 983
LED の解釈 984
LED の解釈について 984
コントローラの LED の解釈 984
Lightweight アクセス ポイント LED の解釈 984

システム メッセージ 984
システム メッセージについて 984
システム リソースの表示 988
システム リソースの表示について 988
注意事項および制約事項 988
システム リソースの表示（GUI） 989
システム リソースの表示（CLI） 989
CLI を使用したトラブルシューティング 990
システム ロギングとメッセージ ロギングの設定 991
システム ロギングとメッセージ ロギングについて 991
システム ロギングとメッセージ ロギングの設定（GUI） 992
メッセージ ログの表示（GUI） 995
システム ロギングとメッセージ ロギングの設定（CLI） 995
システム ログとメッセージ ログの表示（CLI） 999
アクセス ポイント イベント ログの表示 1000
アクセス ポイント イベント ログについて 1000
アクセス ポイント イベント ログの表示（CLI） 1000
ログとクラッシュ ファイルのアップロード 1001
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 1001
ログとクラッシュ ファイルのアップロード（GUI） 1002
ログとクラッシュ ファイルのアップロード（CLI） 1003
コントローラからのコア ダンプのアップロード 1004
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 1004
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） 1004
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） 1005
コントローラから TFTP または FTP サーバへのコア ダンプのアップロード（CLI） 1006
パケット キャプチャ ファイルのアップロード 1007
パケット キャプチャ ファイルのアップロードについて 1007
注意事項および制約事項 1008

パケット キャプチャ ファイルのアップロード（GUI） 1009
パケット キャプチャ ファイルのアップロード（CLI） 1010
メモリ リークの監視 1010
メモリ リークの監視（CLI） 1011
CCXv5 クライアント デバイスのトラブルシューティング 1012
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 1012
注意事項および制約事項 1012
診断チャネルの設定 1013
診断チャネルの設定（GUI） 1013
診断チャネルの設定（CLI） 1014
クライアント レポートの設定 1018
クライアント レポートの設定（GUI） 1019
クライアント レポートの設定（CLI） 1021
ローミング診断とリアルタイム診断の設定 1024
ローミング診断とリアルタイム診断の設定（CLI） 1025
デバッグ ファシリティの使用方法 1027
デバッグ ファシリティの使用方法について 1027
デバッグ ファシリティの設定（CLI） 1029
無線スニファの設定 1033
無線スニファについて 1033
注意事項および制約事項 1033
アクセス ポイントのスニファの設定（GUI） 1034
アクセス ポイントのスニファの設定（CLI） 1036
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 1037
注意事項および制約事項 1037
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） 1038
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） 1039
アクセス ポイント監視サービスのデバッグ 1040
アクセス ポイント監視サービスのデバッグについて 1040
アクセス ポイント監視サービスの問題のデバッグ（CLI） 1040

OfficeExtend アクセス ポイントのトラブルシューティング 1040
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 1040
OfficeExtend の LED の解釈 1041
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 1041
一般的な問題のトラブルシューティング 1041

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。 この章の内容は、次のとおりです。

- 対象読者，li ページ
- マニュアルの構成，li ページ
- 表記法，liii ページ
- 関連資料，lv ページ
- マニュアルの入手方法およびテクニカル サポート，lvi ページ

対象読者

このマニュアルは、Cisco Wireless LAN Controller 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。

マニュアルの構成

このガイドは次の章にわかれています。

章タイトル	説明
概要，（1 ページ）	ワイヤレス LAN コントローラのネットワークでの役割と機能の概要について説明します。
Web ブラウザと CLI インターフェイスの使用方法，（19 ページ）	初期設定およびコントローラへのログイン方法について説明します。
ポートとインターフェイスの設定，（65 ページ）	コントローラの物理ポートとインターフェイスについて説明し、それらの設定手順を示します。

章タイトル	説明
コントローラ設定の構成, （105 ページ）	コントローラの設定方法について説明します。
VideoStream の設定, （219 ページ）	コントローラの VideoStream 設定の設定方法について説明します。
セキュリティ ソリューションの設定, （227 ページ）	ワイヤレス LAN のアプリケーション固有のソリューションについて説明します。
WLAN の使用, （365 ページ）	システム上でワイヤレス LAN と SSID を設定する方法について説明します。
Lightweight アクセス ポイントの制御, （477 ページ）	Lightweight アクセス ポイントをコントローラに接続する方法、およびアクセスポイントの設定を管理する方法について説明します。
メッシュ アクセスポイントの制御, （601 ページ）	メッシュ アクセス ポイントをコントローラに接続する方法、およびアクセス ポイントの設定を管理する方法について説明します。
コントローラ ソフトウェアと設定の管理, （745 ページ）	コントローラ ソフトウェアおよび設定のアップグレード方法と管理方法について説明します。
ユーザ アカウントの管理, （787 ページ）	ゲスト ユーザ アカウントの作成方法と管理方法、Web 認証プロセス、および Web 認証ログインのカスタマイズ方法について説明します。
Radio Resource Management の設定, （825 ページ）	Radio Resource Management（RRM）について、コントローラ上での設定方法も含めて説明します。
Cisco CleanAir の設定, （873 ページ）	コントローラと Lightweight アクセス ポイントにシスコ CleanAir の機能を設定する方法について説明します。
モビリティ グループの設定, （941 ページ）	モビリティ グループについて、コントローラ上での設定方法も含めて説明します。
FlexConnect の設定, （909 ページ）	FlexConnect について、コントローラとアクセス ポイント上での機能の設定方法も含めて説明します。
モバイル コンシェルジュの設定, （971 ページ）	HotSpot 2.0 の設定方法について説明します。
トラブルシューティング, （983 ページ）	コントローラと Lightweight アクセス ポイントの LED パターンに関する情報と、Cisco Unified Wireless Network Solution インターフェイスに表示されるシステム メッセージの一覧を示し、コントローラの問題のトラブルシューティングに使用できる CLI コマンドについて説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表 *1*：表記法

表記法	用途
太字フォント	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、**太字**フォントで示しています。
イタリック体フォント	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、イタリック体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。
{ 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。

警告

「危険」の意味です。 人身事故を予防するための注意事項が記述されています。 機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。（このマニュアルに記載されている警告の翻訳を参照するには、付録の「翻訳版の安全上の警告」を参照してください）。

警告タイトル	説明
Waarschuwing	Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)
Varoitus	Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)
Attention	Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).
Warnung	Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)
Avvertenza	Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).
Advarsel	Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)

警告タイトル	説明
Aviso	Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").
¡Advertencia!	Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")
Varning	Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)

関連資料

Cisco Unified Wireless Network ソリューションについては、併せて次のマニュアルも参照してください。

- Cisco Wireless LAN Controller configuration guides：http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html
- Cisco Wireless LAN Controller command references：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 documentation：http://www.cisco.com/en/US/products/ps12239/products_documentation_roadmaps_list.html
- Cisco Mobility Services Engine documentation：http://www.cisco.com/en/US/products/ps9806/tsd_products_support_series_home.html

Cisco Unified Wireless Network ソリューションのユーザ向けマニュアルを参照するには、次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

マニュアルの入手方法およびテクニカル サポート

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

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

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

概要

この章では、コントローラの構成要素と機能について説明します。 この章の内容は、次のとおりです。

- Cisco Unified Wireless Network ソリューションの概要，1 ページ
- オペレーティング システム ソフトウェア，4 ページ
- オペレーティング システムのセキュリティ，4 ページ
- レイヤ 2 およびレイヤ 3 の動作，5 ページ
- Cisco ワイヤレス LAN コントローラ，6 ページ
- コントローラ プラットフォーム，7 ページ
- Cisco UWN ソリューション無線 LAN，15 ページ
- ファイル転送，15 ページ
- Power Over Ethernet，15 ページ
- Cisco Wireless LAN Controller のメモリ，16 ページ
- Cisco Wireless LAN Controller のフェールオーバーの保護，16 ページ

Cisco Unified Wireless Network ソリューションの概要

Cisco Unified Wireless Network（Cisco UWN）ソリューションは、企業およびサービス プロバイダーに 802.11 無線ネットワーキング ソリューションを提供するように設計されています。 Cisco UWN ソリューションを使用すると、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、Radio Resource Management（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。

Cisco UWN 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 Network Control System。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。 NCS には、大規模システムの監視と制御を容易にするツールが備わっています。 NCS は、Windows 2000、Windows 2003、および Red Hat Enterprise Linux ES サーバ上で動作します。

（注） NCS ソフトウェア リリース 1.1 は、コントローラ ソフトウェア リリース 7.2 を実行するコントローラとともに使用する必要があります。

- 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。

Cisco UWN 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。 これによって、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 NCS 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。

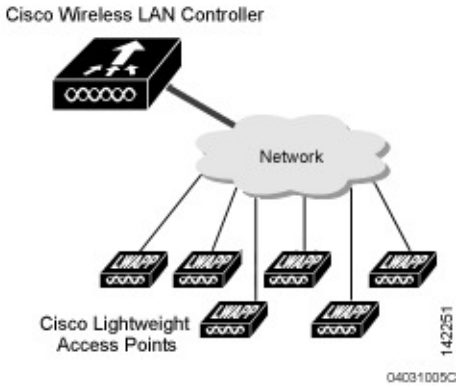
- ネットワークに追加された Lightweight アクセス ポイントの自動検出と自動設定。
- Lightweight アクセス ポイントの完全制御。
- ネットワークを介したコントローラへの Lightweight アクセス ポイントの接続。 ネットワーク機器は、アクセス ポイントに Power over Ethernet（PoE）を提供してもしなくてもかまいません。

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



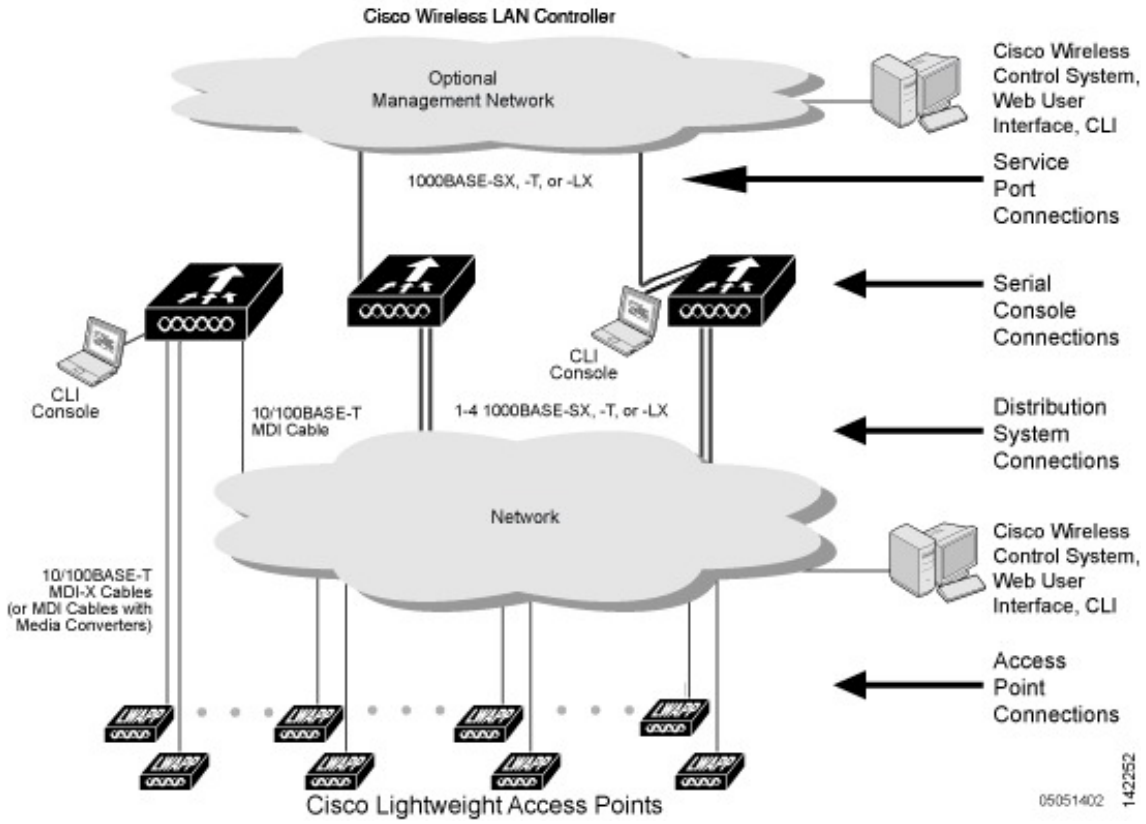
マルチコントローラ展開

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 Radio Resource Management（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、業界標準の認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。

Cisco WLAN ソリューションの有線セキュリティ

コントローラと Lightweight アクセス ポイントには、それぞれ固有の署名付き X.509 証明書が添付されます。 この署名付き証明書は、ダウンロードしたコードを読み込む前の検証に使用され、悪意のあるコードがハッカーによってコントローラや Lightweight アクセス ポイントにダウンロードされることを防ぎます。

また、コントローラと Lightweight アクセス ポイントでは、ダウンロードしたコードを、署名付き証明書を使用して検証してから読み込むことで、ハッカーが Cisco Wireless Controller や Lightweight アクセス ポイントに悪意のあるコードをダウンロードできないようにしています。

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 でのみ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）はサポートされていません。

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, （16 ページ）で説明します。

WCS 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 ポイントをリブートできます。

（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、リブ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 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。 Radio Resource Management（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 5500 シリーズ コントローラ
- Catalyst 6500 シリーズ スイッチ Wireless Services Module（WiSM2s）
- Cisco Flex 7500 シリーズ コントローラ
- Cisco Services Ready Engine（SRE）の Cisco Wireless Controller
- Cisco 8500 シリーズ コントローラ
- Cisco Virtual Wireless LAN Controller

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 Cisco Unified Wireless Network（CUWN）のコンポーネントであり、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）、Context Aware（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 Wireless Controller は、5 台および 25 台の単位で、最大 50 台の Lightweight アクセス ポイントをサポートします。最小構成は 5 台です。

Cisco 2500 シリーズのコントローラは、802.11 a/b/g の強力なカバレッジを提供します。また、802.11n とシスコの次世代のワイヤレス ソリューションおよび Cisco Enterprise Wireless Mesh を使用して信頼性を向上させます。

サポートされない機能

- 有線ゲスト アクセス
- Cisco 2500 シリーズ コントローラをゲストのアンカー コントローラとして設定することはできません。 ただし、外部コントローラとして設定し、ゲスト トラフィックを DMZ のゲスト アンカー コントローラにトンネリングすることはできます。
- 帯域幅コントラクト
- サービス ポート
- Apple Talk ブリッジ
- LAG
- マルチキャスト-ユニキャスト
- 使用権ライセンス
- ハイ アベイラビリティ
- PMIPv6

（注） Cisco WiSM2 と Cisco 5500 シリーズ コントローラでサポートされていない機能は、Cisco 2500 シリーズ コントローラでもサポートされません。

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。 5508 コントローラは、最大 500 台の Lightweight アクセス ポイントと 7000 台のワイヤレス クライアント（クライアント ロケーション機能を使用する場合は、5000 台のワイヤレス クライアントと 2500 個の RFID タグ）をサポートする、大企業や高密度アプリケーションに最適なコントローラです。

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。

サポートされない機能

- スパニングツリー プロトコル（STP）
- ポートのミラーリング
- レイヤ 2 アクセス コントロール リスト（ACL）のサポート
- VPN 終端（IPSec および L2TP など）
- VPN パススルー オプション

（注） ACL を使用してオープン WLAN を作成すると、この機能を Cisco 5500 シリーズ コントローラで再現できます。

- 802.3 ブリッジング、AppleTalk、および Point-to-Point Protocol over Ethernet（PPPoE）の設定

（注） Cisco 5500 シリーズ コントローラはデフォルトでこれらのパケットをブリッジ処理します。 必要に応じて、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ができます。

- インターフェイス上でのフラグメントされた ping
- 使用権ライセンス

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リング要件を満たすように設計されています。 Cisco Unified Wireless ソリューションでは、FlexConnect とモニタ モードという主要な 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。

注意事項および制約事項

FlexConnect の導入の場合のみ、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。

サポートされない機能

- 静的 AP マネージャ インターフェイス

（注） Cisco 7500 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。

- L3 ローミング
- VideoStream
- TrustSec SXP
- IPv6/デュアル スタック クライアントのサポート

（注） IPv6 クライアント ブリッジングおよび Router Advertisement Guard がサポートされています。

- 内部 DHCP サーバ
- ローカル モードのアクセス ポイント

（注） ローカル モードで Cisco FLEX 7500 シリーズ コントローラに関連付けられた AP は、FlexConnect モードに自動的に変換されます。

- Mesh
- LAG
- スパニングツリー プロトコル（STP）
- Cisco FLEX 7500 シリーズ コントローラをゲストのアンカー コントローラとして設定することはできません。 ただし、外部コントローラとして設定し、ゲスト トラフィックを DMZ のゲスト アンカー コントローラにトンネリングすることはできます。
- Multicast
- PMIPv6

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、AP を 6000、クライアントを 64000、FlexConnect グループを 2000、FlexConnect グループごとの AP を 100、AP グループを 6000、さらに VLAN を最大 4095 までサポートします。

（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。

注意事項および制約事項

- 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。
- ローカルと 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 マルチキャストをディセーブルにし、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 が必要でない場合は、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 スヌーピングをイネーブルにしてください。 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。

サポートされない機能

- LAG
- Cisco 8500 シリーズ コントローラをゲストのアンカー コントローラとして設定することはできません。 ただし、外部コントローラとして設定し、ゲスト トラフィックを DMZ のゲスト アンカー コントローラにトンネリングすることはできます。
- TrustSec SXP
- ローカル認証（認証サーバとして機能するコントローラ）
- 内部 DHCP サーバ
- 有線ゲスト アクセス
- ローカルにスイッチされるクライアント用のデータ DTLS

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。 Virtual Wireless LAN Controller 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。

サポートされない機能

- データ DTLS
- Cisco 600 シリーズ OfficeExtend アクセス ポイント
- ワイヤレス レート制限
- 内部 DHCP サーバ
- ローカル モードのアクセス ポイント
- モビリティ/ゲスト アンカー
- マルチキャスト ユニキャスト モード
- IPv6
- PMIPv6
- WGB

- VideoStream
- ハイ アベイラビリティ
- 屋外メッシュ アクセス ポイント

（注） AP1552 などの屋外 AP は、FlexConnect モードで、AP がメッシュ導入で使用されていない場合にサポートされます。

（注） 2500 シリーズ コントローラに直接接続する場合は、ローカル モードの AP のみサポートされます。

Cisco Wireless Services Module 2

Cisco Wireless Services Module 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。 次の機能があります。

- 最大 1000 個のアクセス ポイントと 15,000 個のクライアントを接続
- 他のワイヤレス LAN コントローラより高いクライアント密度をサポート
- 500 のアクセス ポイントを同時に更新する機能
- ビデオ、音声、ゲスト、ロケーション、エンタープライズ ワイヤレス メッシュ、およびテレワーク用のレイヤ 3 モビリティ サービス
- レイヤ 1 Wireless Intrusion Prevention System（wIPS）機能による高度なワイヤレス セキュリティ

サポートされない機能

- スパニングツリー プロトコル（STP）
- ポートのミラーリング
- レイヤ 2 アクセス コントロール リスト（ACL）のサポート
- VPN 終端（IPSec および L2TP など）
- VPN パススルー オプション
- 802.3 ブリッジング、AppleTalk、および Point-to-Point Protocol over Ethernet（PPPoE）の設定
- インターフェイス上でのフラグメントされた ping

Cisco Services Ready Engine（SRE）の Cisco Wireless Controller

Cisco Services Ready Engine（SRE）の Cisco Wireless Controller 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 Wireless Controller はエントリ レベルのコントローラであり、802.11n のパフォーマンスとスケーラビリティを備えています。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、Cisco Integrated Services Routers Generation 2（ISR G2）用のルータ ブレードであり、モジュールの Cisco Wireless Controller 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 Unified Wireless Network のコンポーネントとして、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、中央集中型セキュリティ ポリシー、Wireless Intrusion Prevention System（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 Context Aware 機能、音声とビデオのための Quality of Service（QoS）を備えています。

Cisco SRE の Cisco Wireless LAN Controller では、5 ～ 50 のアクセス ポイントをサポートします。またアクセス ポイントは 5 または 25 の単位で追加することができます。 ライセンス構成では、基本機能セットの一部としてエンタープライズワイヤレス メッシュなどさまざまなビジネス向けのモビリティのニーズに対応します。このため、物理的に有線ネットワークに接続することは困難または不可能な場所においても、アクセス ポイントがワイヤレス接続を動的に確立できるようになります。

Cisco Wireless Controller アプリケーションのライセンスと導入オプションは柔軟性が高く、Cisco SRE Internal Service Module（ISM）300 および Cisco SRE Service Module（SM）700 および SM 900 で使用できます。

サポートされない機能

- 有線ゲスト アクセス
- 自動アンカー コントローラとして設定できません。 ただし、外部コントローラとしては設定できます
- 帯域幅コントラクト
- 直接接続モードのアクセス ポイント
- サービス ポートのサポート
- Apple Talk ブリッジ
- LAG

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。

Power Over Ethernet

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。 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。

Lightweight アクセス ポイントは、802.3af 準拠デバイスまたは外部電源装置から電力供給を受けることができます。

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。

十分な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

Web ブラウザと CLI インターフェイスの使用方法

この章では、コントローラの初期設定およびログインの方法を説明します。 この章の内容は、次のとおりです。

- 設定ウィザードを使用したコントローラの設定，20 ページ
- コントローラのコンソール ポートの接続，20 ページ
- コントローラの設定（GUI），21 ページ
- その他の関連資料，32 ページ
- コントローラの設定：CLI 設定ウィザードの使用，33 ページ
- コントローラ Web GUI の使用方法，36 ページ
- 外部で生成した SSL 証明書のロード，40 ページ
- 外部で生成した SSL 証明書について，40 ページ
- SSL 証明書のロード（GUI），41 ページ
- SSL 証明書のロード（CLI），42 ページ
- コントローラ CLI の使用方法，43 ページ
- コントローラ CLI へのログイン，43 ページ
- 設定のないコントローラでの AutoInstall 機能の使用，47 ページ
- AutoInstall 機能について，47 ページ
- 注意事項および制約事項，47 ページ
- その他の関連資料，51 ページ
- コントローラのシステムの日時の管理，51 ページ
- Telnet および Secure Shell セッションの設定，56 ページ

• コントローラの無線管理，62 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。

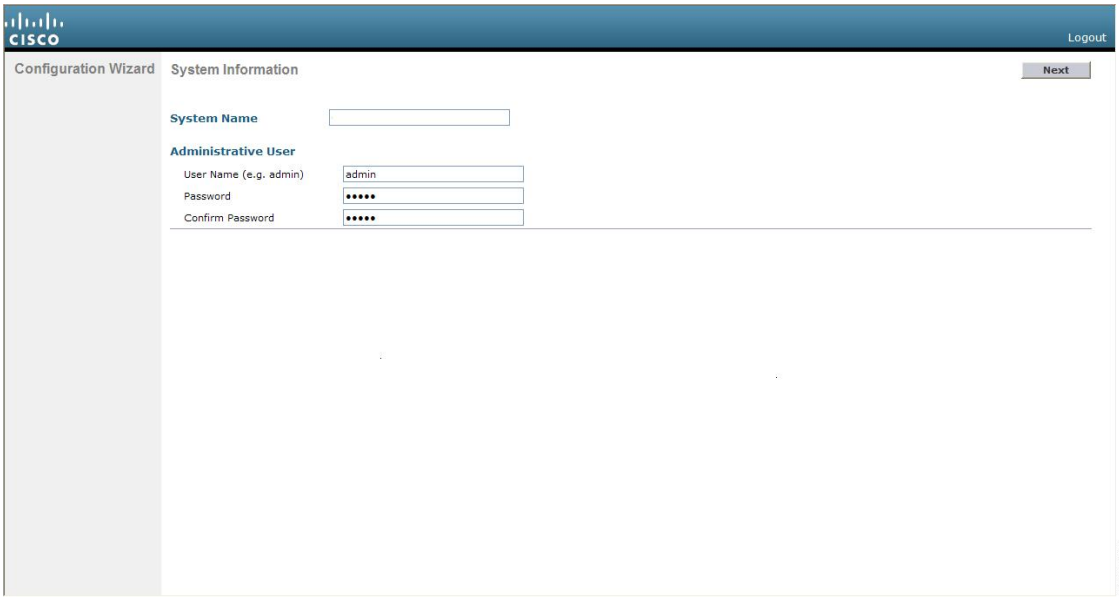
コントローラの電源投入時自己診断テストに合格した場合は、起動スクリプトによって設定ウィザードが実行されます。画面の指示に従って、基本設定を入力してください。

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（例：209.165.200.225）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 以降または Firefox 2.0.0.11 以降を起動して、http://209.165.200.225 にアクセスします。 すると、設定ウィザードが表示されます。

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



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。

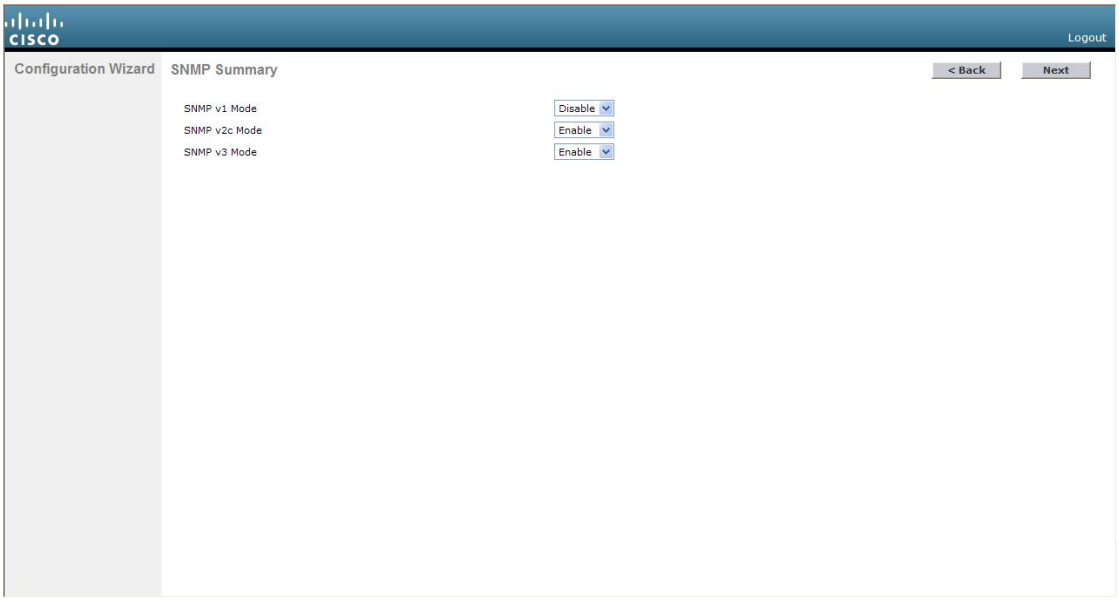
ステップ 4 [User Name] テキスト ボックスに、このコントローラに割り当てる管理者ユーザ名を入力します。 ASCII 文字を最大 24 文字入力できます。 デフォルトのユーザ名は *admin* です。

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。 また、i の代わりに 1、I、! を、o の代わりに 0 を、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、[SNVP 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、[SNVP v3 Mode] ドロップダウン リストから [Disable] を選択します。

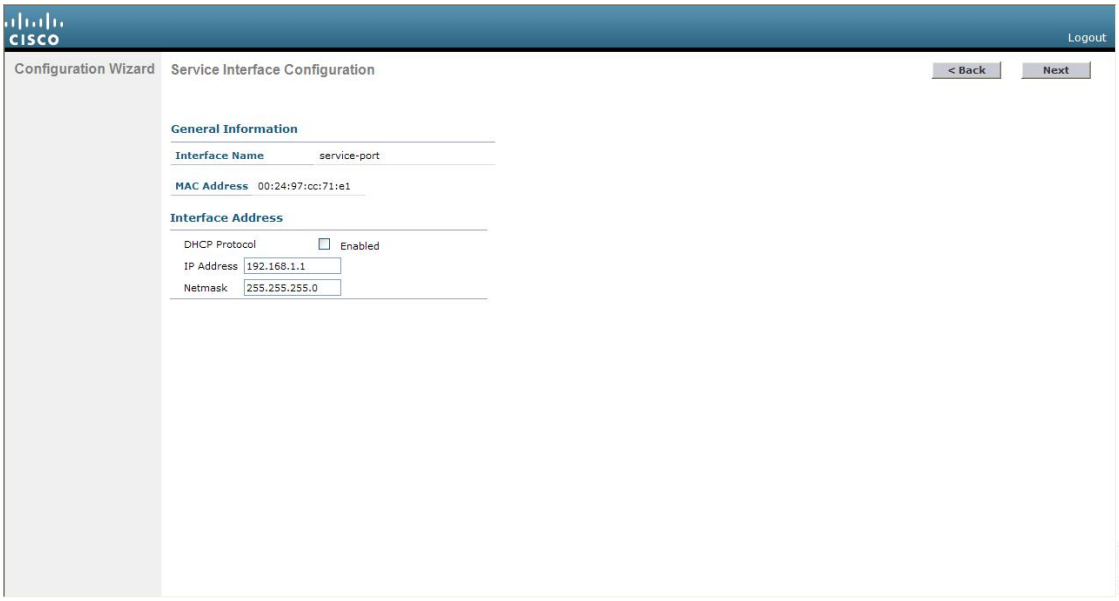
ステップ 10 [Next] をクリックします。

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



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。

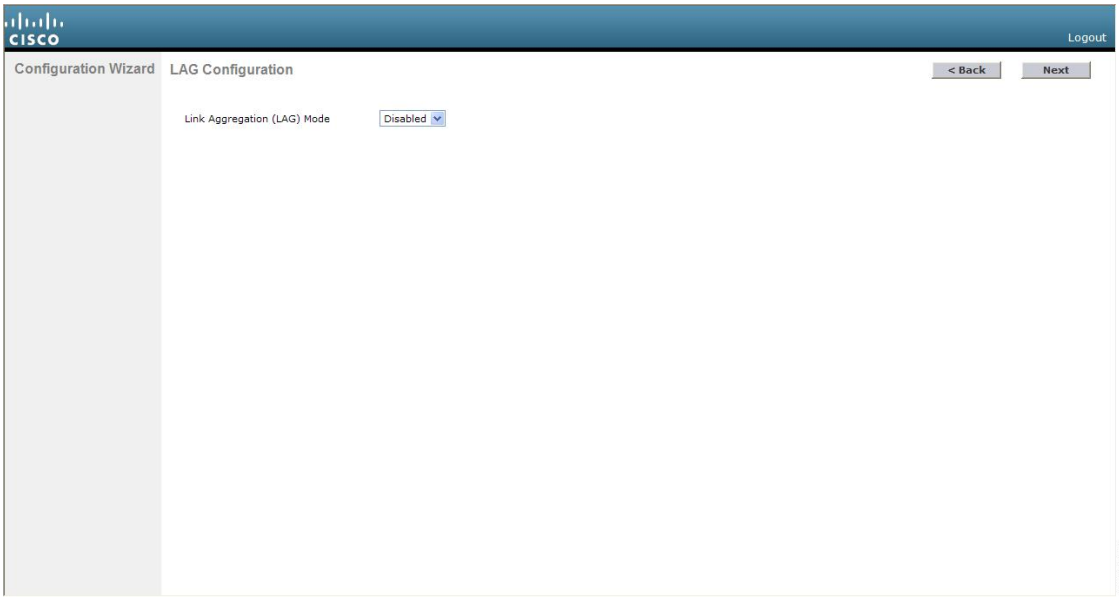
ステップ 13 次のいずれかの操作を行います。

- 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

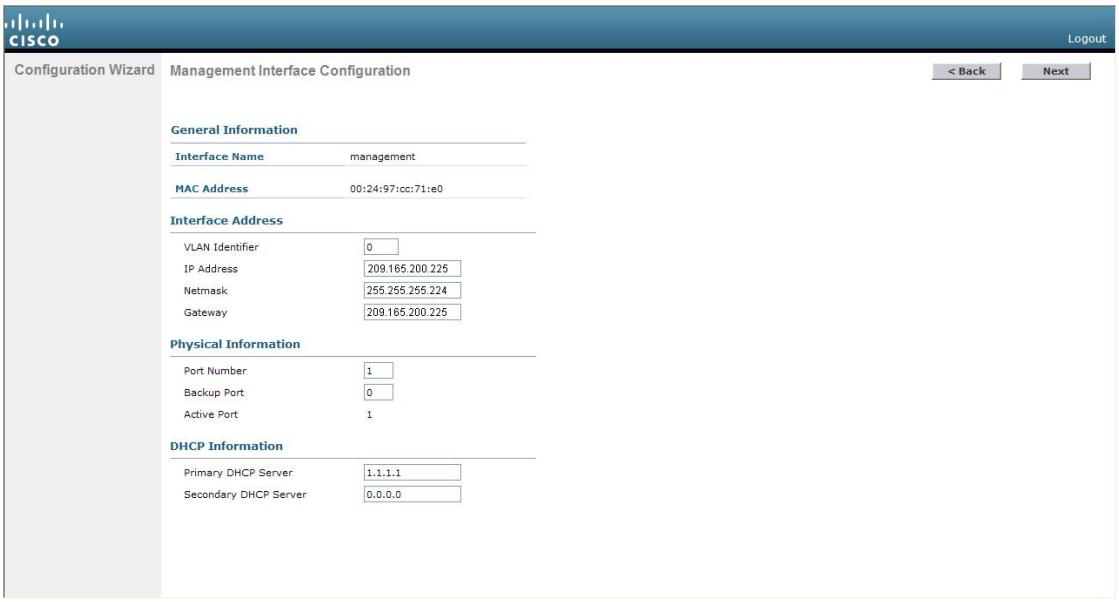


ステップ 15 リンク集約（LAG）を有効にするには、[Link Aggregation (LAG) Mode] ドロップダウン リストから [Enabled] を選択します。 LAG を無効にするには、このテキスト ボックスを [Disabled] のままにします。

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



（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。

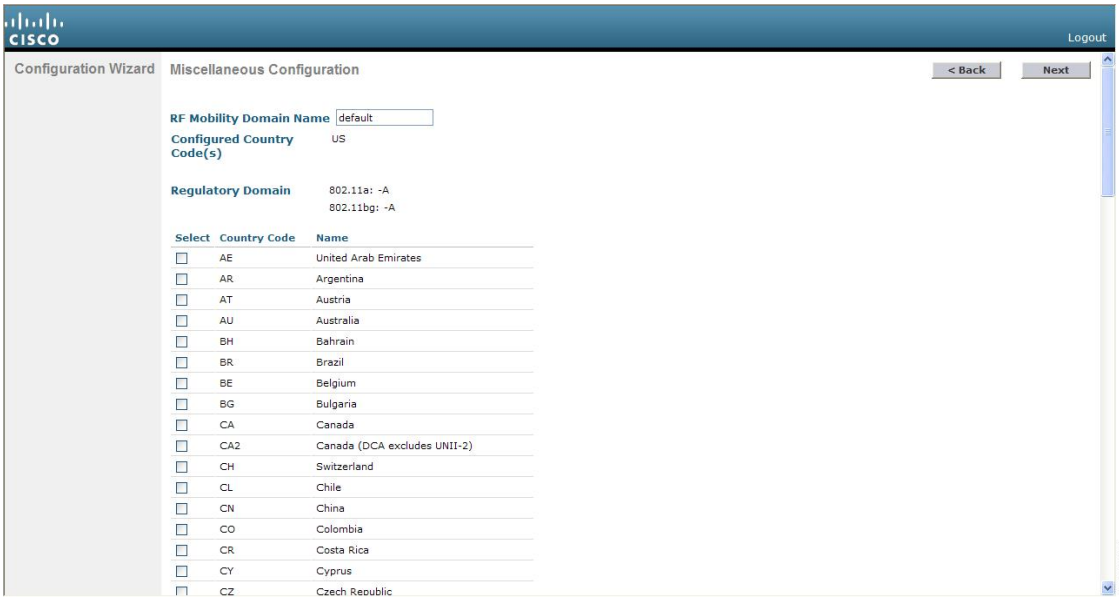
ステップ 25 [Next] をクリックします。 [AP-Manager Interface Configuration] 画面が表示されます。

（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、目的が異なっています。 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 グループはスケー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 グループはスケー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、複数の国番号を選択できます。 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。

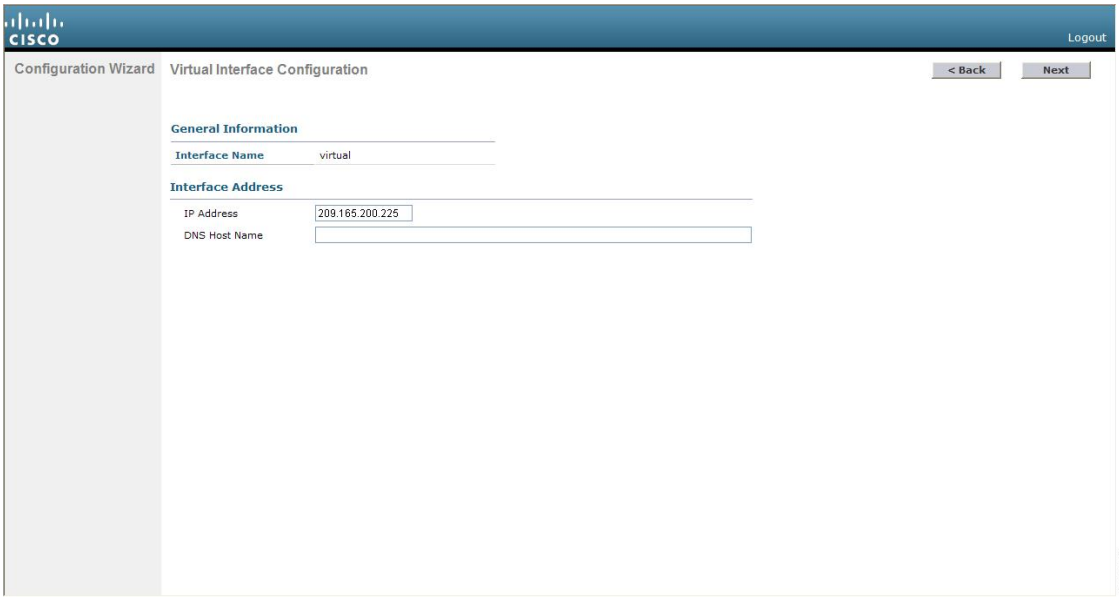
ステップ 31 次のメッセージが表示されたら、[OK] をクリックします。

```
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。

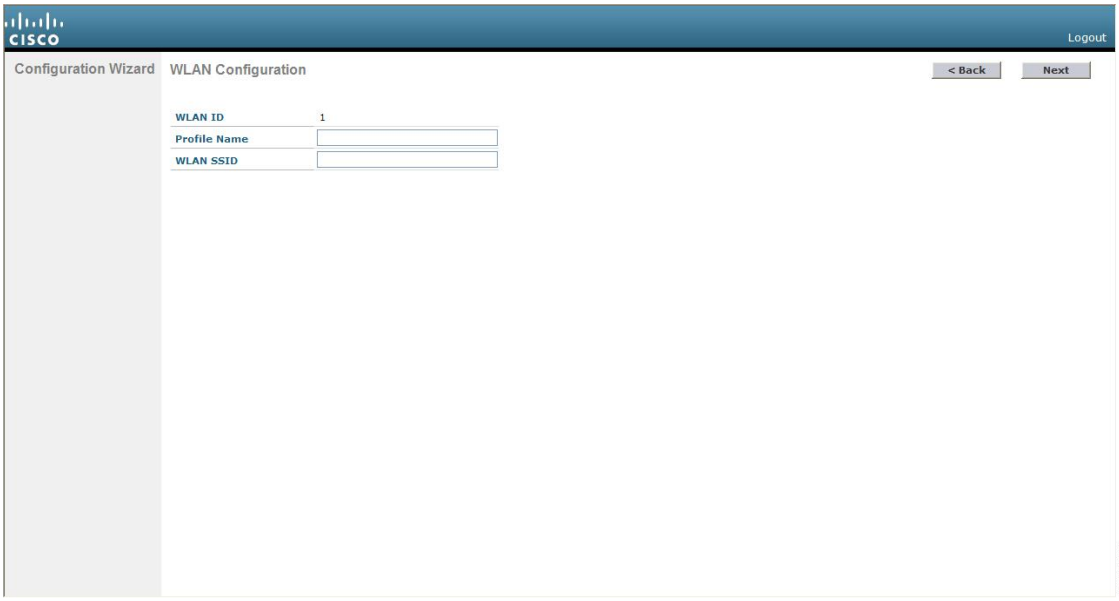
（注） 仮想インターフェイスは、モビリティ管理、DHCP リレー、およびゲスト Web 認証や VPN 終端などレイヤ 3 の組み込みセキュリティをサポートするために使用されます。 同一のモビリティ グループに属するコントローラはすべて、同じ仮想インターフェイス IP アドレスを使用して設定する必要があります。

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。

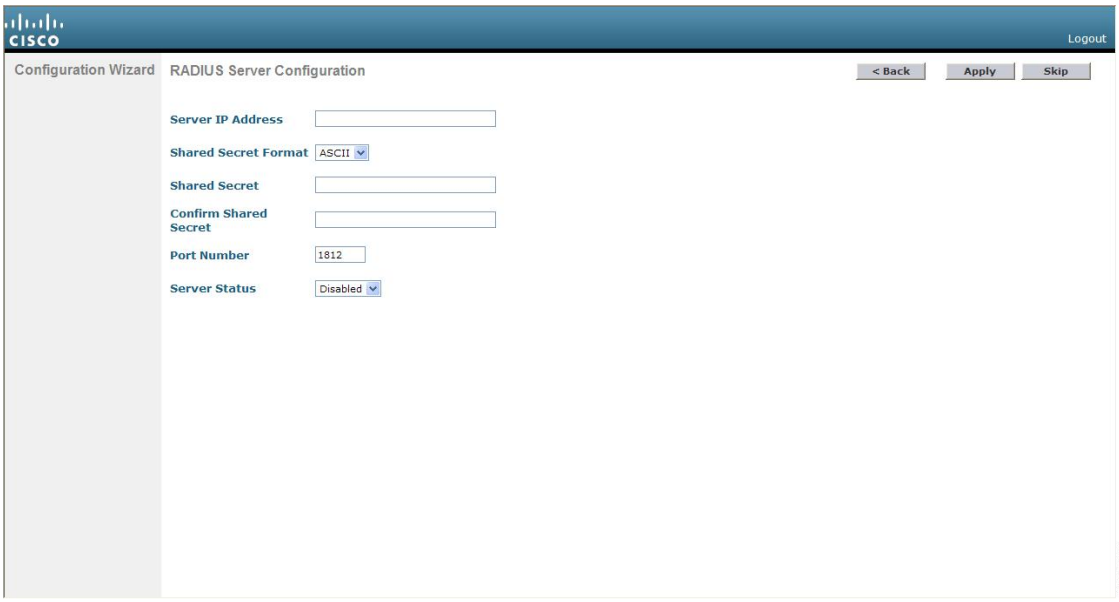
ステップ 37 [Next] をクリックします。

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



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。

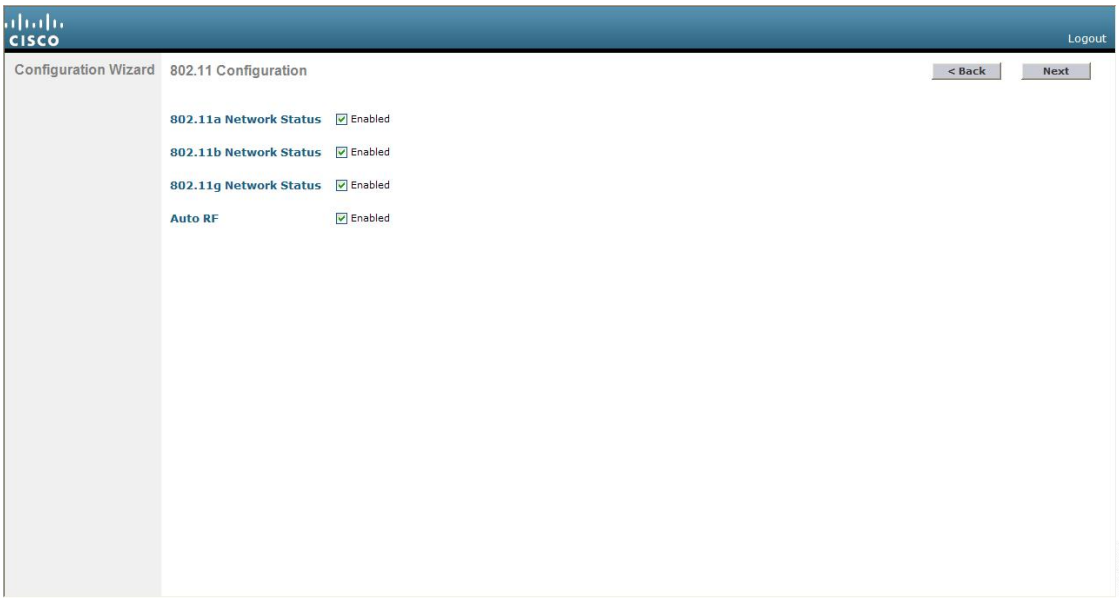
ステップ 41 [Shared Secret] テキスト ボックスと [Confirm Shared Secret] テキスト ボックスに、RADIUS サーバによって使用される秘密キーを入力します。

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



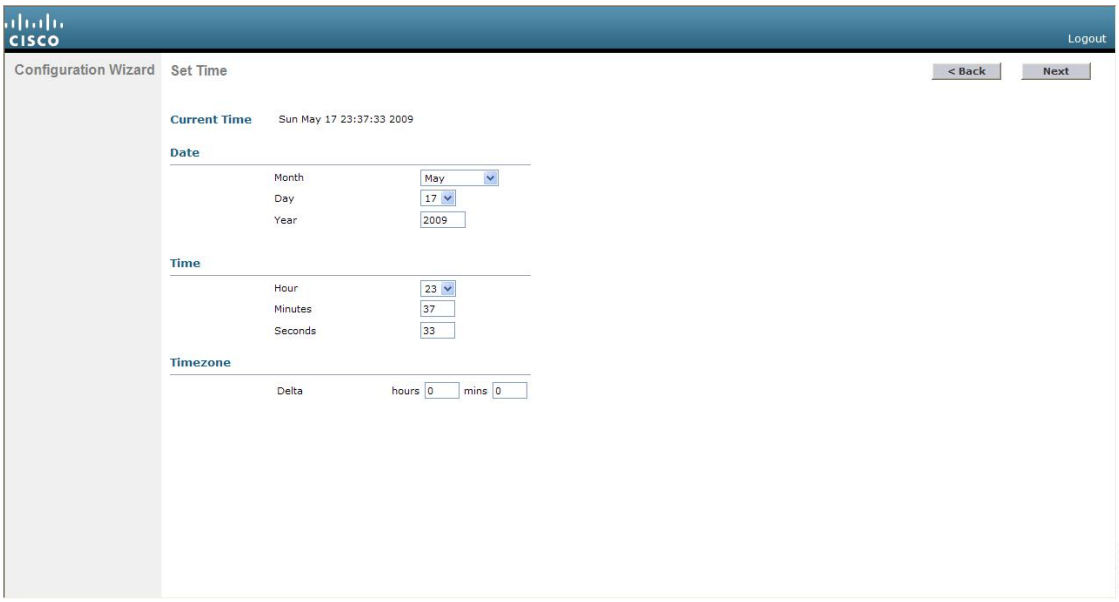
ステップ 45 802.11a、802.11b、および 802.11g の Lightweight アクセス ポイント ネットワークを有効にするには、[802.11a Network Status]、[802.11b Network Status]、および [802.11g Network Status] の各チェックボックスを選択したままにします。 これらのネットワークのサポートを無効にするには、このチェックボックスをオフにします。

ステップ 46 コントローラの Radio Resource Management（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



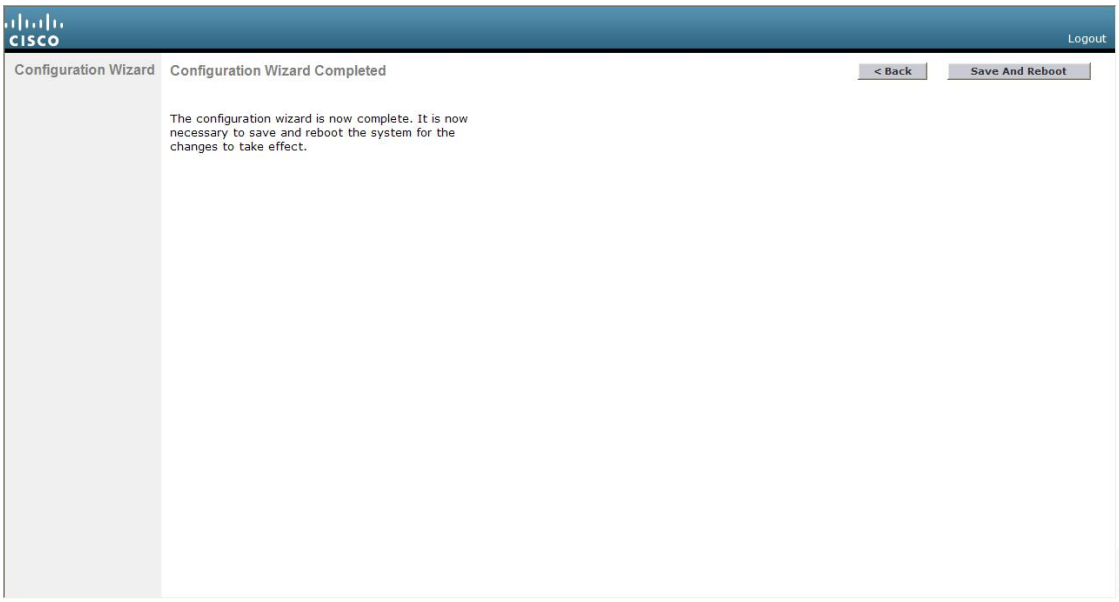
ステップ 48 コントローラのシステム時間を手動で設定するには、現在の日付を Month/DD/YYYY の形式で、現在の時刻を HH:MM:SS の形式で入力します。

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。

その他の関連資料

- コントローラのデフォルト設定へのリセットについて，（217 ページ）
- Radio Resource Management の設定，（825 ページ）
- モビリティ グループの設定，（941 ページ）
- SNMP コミュニティ ストリング，（140 ページ）

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。 また、i の代わりに 1、I、！を、o の代わりに 0 を、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、目的が異なっています。 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 グループはスケー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 グループはスケー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） 使用可能な国番号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、複数の国番号を入力できます。 複数の国番号を入力するには、国番号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 Radio Resource Management（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 23 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。
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 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 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。
- このコントローラ GUI は、Microsoft Internet Explorer バージョン 6.0 SP1 以降および 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 インターフェイスの設定方法については、ポートとインターフェイスの設定，（65 ページ）を参照してください。
- 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 ブロッカを無効にする必要があります。

GUI へのログイン

コントローラの GUI にログインするには、次の手順に従います。

ステップ 1 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。 コントローラの [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

コントローラの GUI からログアウトするには、次の手順に従います。

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 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

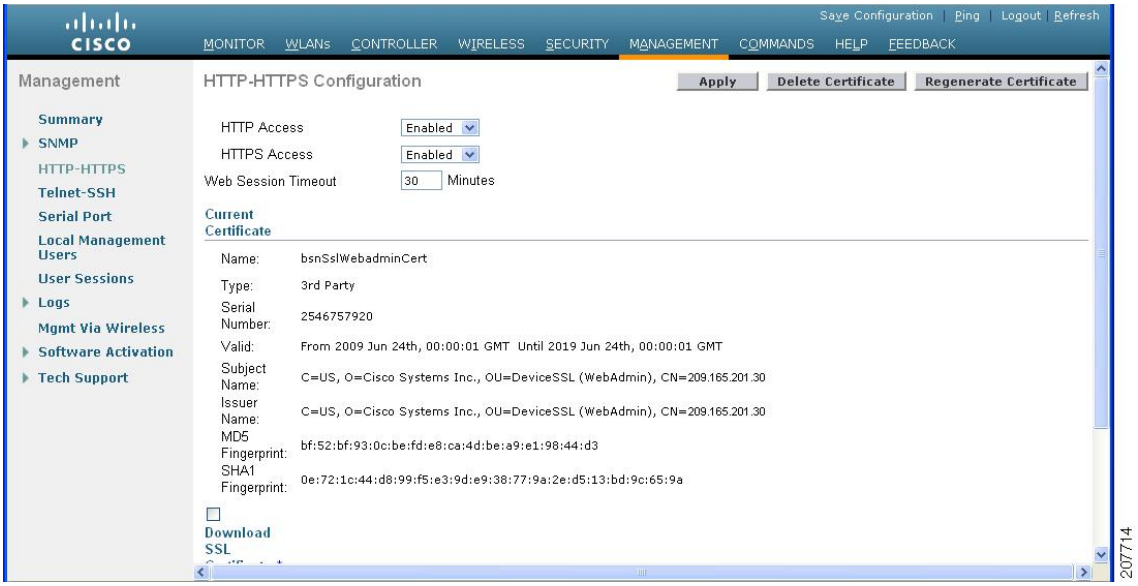
この項では、ディストリビューション システム ポートを Web ポート（HTTP を使用）またはセキュア Web ポート（HTTPS を使用）として有効にする手順について説明します。 HTTPS を有効化すると、GUI との通信を保護できます。 HTTPS は、Secure Socket Layer（SSL）プロトコルを使用して HTTP ブラウザ セッションを保護します。 HTTPS を有効にすると、コントローラは独自の Web アドミニストレーション SSL 証明書を生成して、自動的に GUI に割り当てます。 また、外部で生成された証明書をダウンロードすることもできます。

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] の順に選択して [HTTP Configuration] ページを開きます。

図 *15*：*[HTTP Configuration]* ページ



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 セッションのアクティビティがない場合にタイムアウトするまでの時間（分単位）を入力します。 30 ～ 160 分の範囲内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] をクリックして、変更を確定します。

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 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] をクリックして、変更を保存します。

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 Web 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 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 セキュア Web 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 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 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するには、次のコマンドを入力します。
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 [disabled] です。

ステップ 4 Web 管理に対して SSLv2 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 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 [disabled] です。

ステップ 5 コントローラが証明書を生成したことを確認するには、次のコマンドを入力します。
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 6 （任意）新しい証明書を生成する場合は、次のコマンドを入力します。
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 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 パスワードを不揮発性 RAM（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

外部で生成した SSL 証明書のロード

ここでは、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 WCS と同じ PC 上で実行することはできません。WCS 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。

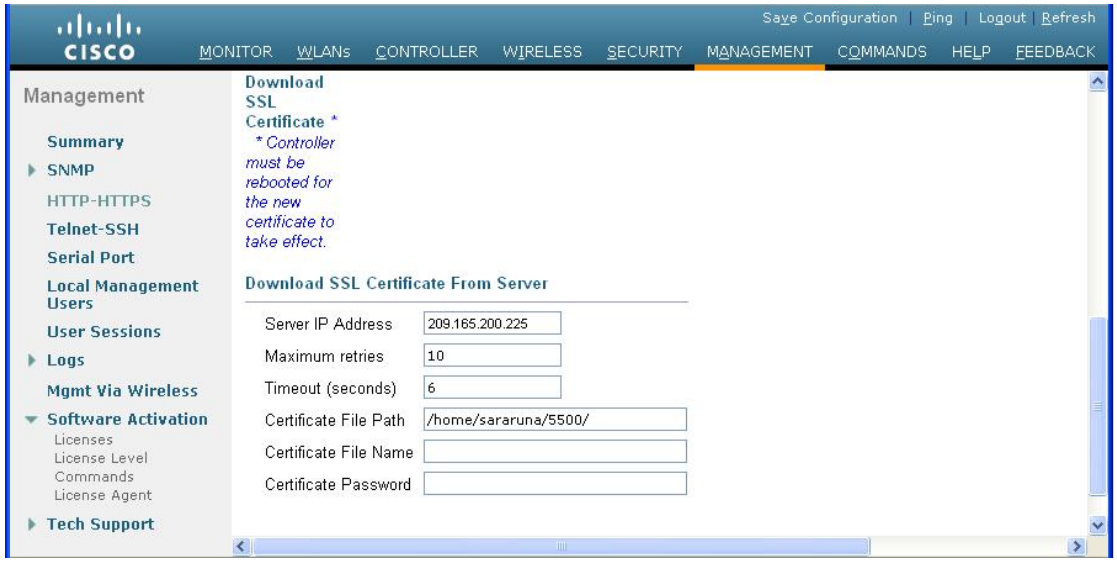
（注） チェーン証明書は Web 認証でのみサポートされています。管理証明書ではサポートされていません。

（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 *16*：*[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（webadmincert_name.pem）。

ステップ 7 （オプション）[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。

ステップ 10 コントローラをリブートして変更内容を有効にするには、[Commands] > [Reboot] > [Reboot] > [Save and Reboot] の順に選択します。

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（webadmincert_name.pem）と呼ばれます。

ステップ 2 webadmincert_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 *webadmincert_name.pem*

ステップ 5 オペレーティング システムが Web アドミニストレーション 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。

リモート イーサネット接続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 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。

```
#(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。

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。

コマンド	アクション
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WCS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情報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ブートをトリガーします。 リブート後に、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*-confg
- *host name*.cfg
- *Base MAC Address*-confg（0011.2233.4455-confg など）
- *serial number*-confg
- ciscowlc-confg
- 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-confg'
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: interation 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-confg'
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-confg'
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-confg'
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
```

その他の関連資料

コントローラにDHCPを設定する方法の詳細は、WLANの使用,（365ページ）を参照してください。

コントローラにTFTPサーバを設定する方法の詳細は、コントローラ ソフトウェアと設定の管理,（745 ページ）を参照してください。

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、設定を変更したい場合は、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）

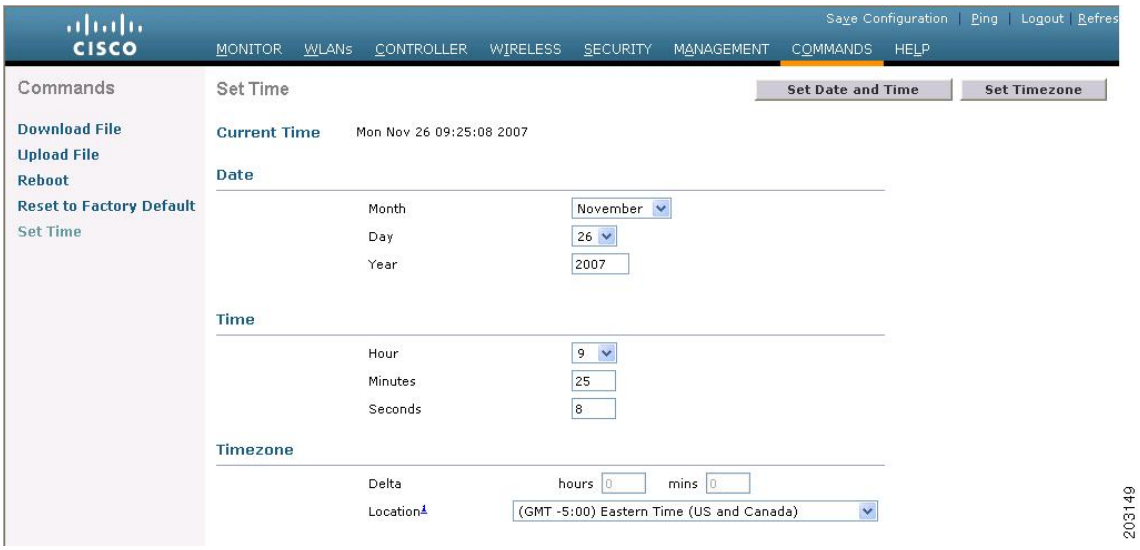
（注） デフォルトでは MD5 が使用されます。

- **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*
- 認証キーを削除するには、次のコマンドを入力します。
  config time ntp key-auth delete *key-index*
- NTP キーのインデックスの一覧を表示するには、次のコマンドを入力します。
  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 *17*：*[Set Time]* ページ



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 コントローラ上の現在の現地日時を GMT で設定するには、次のコマンドを入力します。
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。

- 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するには、次のコマンドを入力します。

  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 日曜から始まり、11 月の第 1 日曜日で終わります。

- 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、次のコマンドを入力します。

  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 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 4 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するには、次のコマンドを入力します。
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。

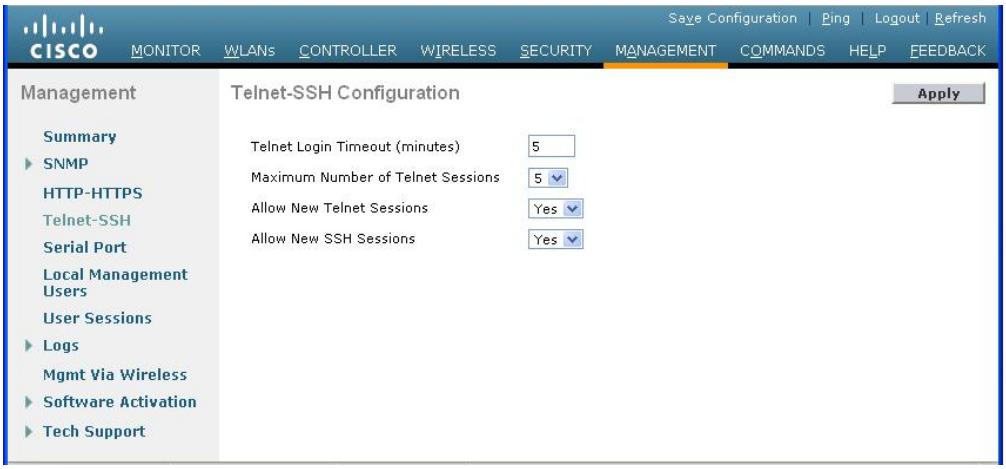
注意事項および制約事項

- 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] の順に選択して [Telnet-SSH Configuration] ページを開きます。

図 *18*：*[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。

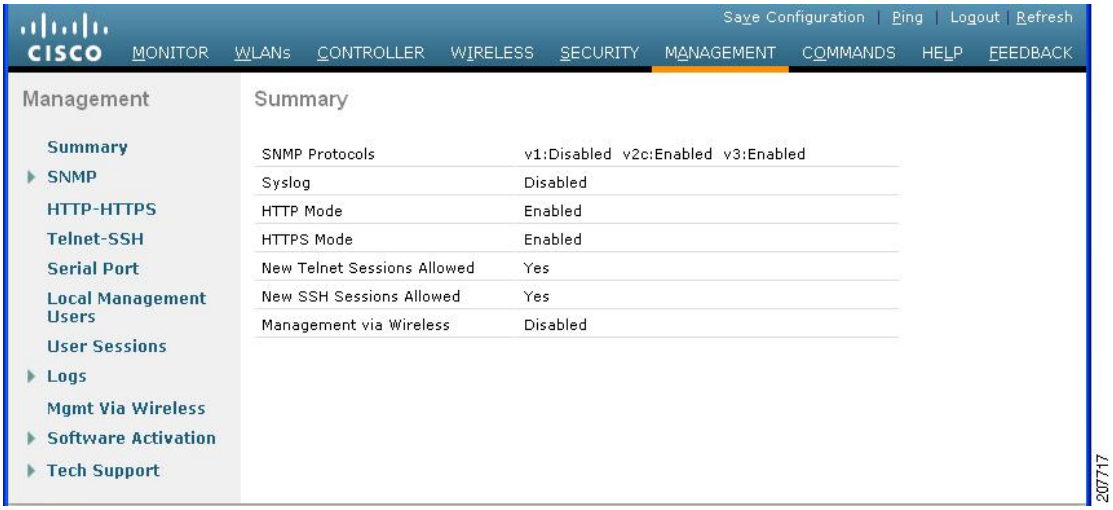
ステップ 5 コントローラ上での新規 SSH セッションを許可する場合は [Allow New SSH Sessions] ドロップダウン リストから [Yes] を選択し、許可しない場合は [No] を選択します。 デフォルト値は [Yes] です。

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 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 *19*：*[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が、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 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するには、次のコマンドを入力します。
config network telnet {**enable** | **disable**}

デフォルト値は [disabled] です。

ステップ 2 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するには、次のコマンドを入力します。
config network ssh {**enable** | **disable**}

デフォルト値はイネーブルです。

ステップ 3 非アクティブの Telnet セッションを終了させるまでの時間（分単位）を指定するには、次のコマンドを入力します。
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 同時 Telnet セッションまたは SSH セッションの最大数を指定するには、次のコマンドを入力します。
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 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 6 Telnet と SSH の設定を表示するには、次のコマンドを入力します。
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 Telnet セッションの設定を表示するには、次のコマンドを入力します。
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 アクティブな Telnet セッションをすべて表示するには、次のコマンドを入力します。
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 アクティブな Telnet セッションをすべて終了させる、または特定の Telnet セッションを終了させるには、次のコマンドを入力します。
config loginsession close {**all** | **session_id**}

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

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」を参照してください。

注意事項および制約事項

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。

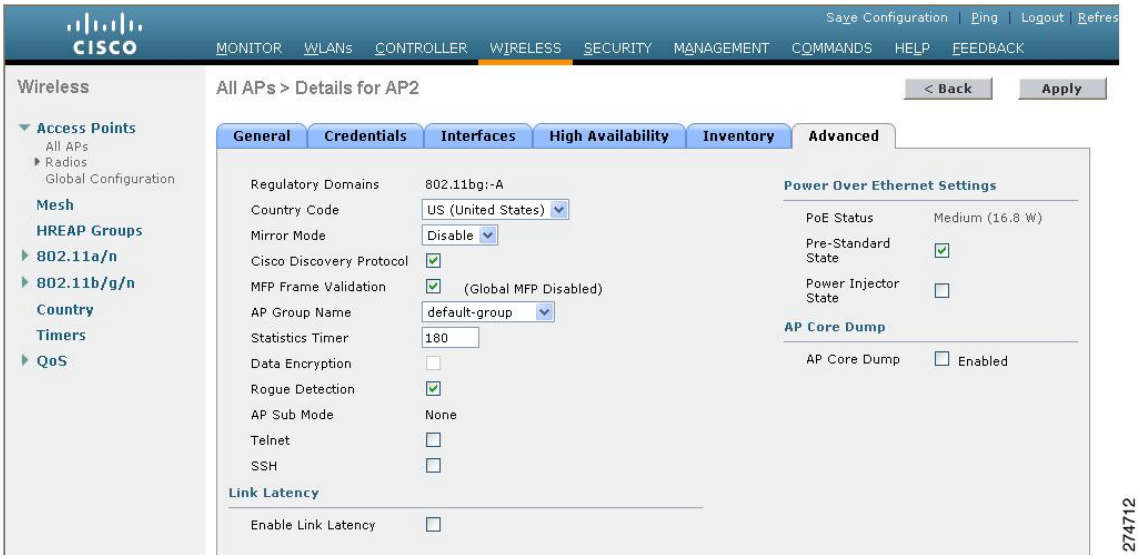
Telnet または SSH を使用したアクセス ポイントのトラブルシューティング（GUI）

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。

図 *20*：*[All APs > Details for]*（*[Advanced]*）ページ



ステップ 4 このアクセス ポイント上での Telnet 接続を有効にするには、[Telnet] チェックボックスをオンにします。デフォルトではオフになっています。

ステップ 5 このアクセス ポイント上での SSH 接続を有効にするには、[SSH] チェックボックスをオンにします。 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。

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 アクセス ポイントで Telnet または SSH の接続を有効にするには、次のコマンドを入力します。
config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

デフォルト値は [disabled] です。

（注） アクセス ポイントで Telnet または SSH の接続を無効にするには、次のコマンドを入力します。
config ap {**telnet** | **ssh**} **disable** *Cisco_AP*

ステップ 2 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 3 アクセス ポイントで Telnet または SSH が有効になってい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 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となるよう、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

ポートとインターフェイスの設定

この章で説明する内容は、次のとおりです。

- ポートとインターフェイスの概要，66 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，67 ページ
- インターフェイスに関する情報，68 ページ
- 管理インターフェイスの設定，70 ページ
- AP マネージャ インターフェイスの設定，73 ページ
- 仮想インターフェイスの設定，76 ページ
- サービス ポート インターフェイスの設定，78 ページ
- 動的インターフェイスの設定，79 ページ
- 動的 AP 管理について，83 ページ
- WLAN について，83 ページ
- ポートの設定（GUI），85 ページ
- ポートのミラーリングの設定，86 ページ
- Cisco 5500 シリーズ コントローラの USB コンソール ポートの使用，88 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，90 ページ
- リンク集約の設定，90 ページ
- 複数の AP マネージャ インターフェイスの設定，94 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，96 ページ
- VLAN Select の設定，98 ページ
- インターフェイス グループの設定，99 ページ
- マルチキャスト最適化，102 ページ

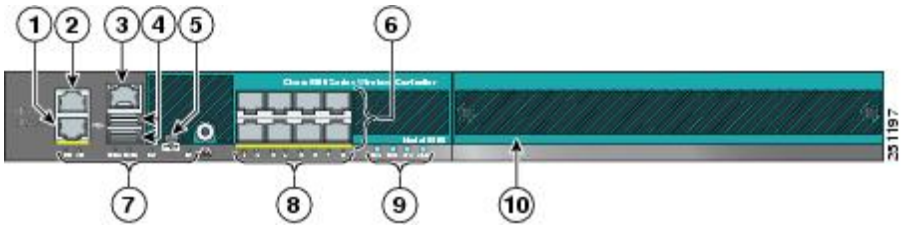
ポートとインターフェイスの概要

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

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 *21*：*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） （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。

注意事項および制約事項

- 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。

- 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イネーブルになります。

- 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的実体です。 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 コントローラおよび Cisco WiSM2 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れば、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。

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。

注意事項および制約事項

- 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 コントローラおよび Cisco WiSM2 では、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。

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

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） サービス ポートが使用中の場合は、サービス ポート インターフェイスとは異なるスーパーネット上に管理インターフェイスが存在する必要があります。

（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（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。

- 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 5500 シリーズ コントローラの場合のみ）

  （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 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。

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

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。

注意事項および制約事項

- 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。
- 7.0.116.0 リリース以降では、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。
- 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

（注） AP マネージャ 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の IP アドレスと異なるものにする必要があります。またこれらの IP アドレスは同じ VLAN および同じサブネット上にある必要があります。セカンダリ サブネットによる動的インターフェイスの設定はサポートされていません。

- 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。

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

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 認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。

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。

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

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。

注意事項および制約事項

- 外部ネットワークから到達できる物理的なサービス ポート インターフェイスを持つのはCisco 5500 シリーズ コントローラのみです。

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 ip-address-of-primary-dhcp- server [*ip-address-of-secondary-dhcp-server*]

- DHCP サーバをディセーブルにするには、次のコマンドを入力します。

  config interface dhcp service-port none

- 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。

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

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 ポートにマッピング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。

注意事項および制約事項

- 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では、タグ付きの VLAN を使用することをお勧めします。
- 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。
- コントローラは、動的インターフェイスとして設定されているサブネットからの送信元アドレスを持つ SNMP 要求には応答しません。

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** *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 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 システム通信用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。

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。

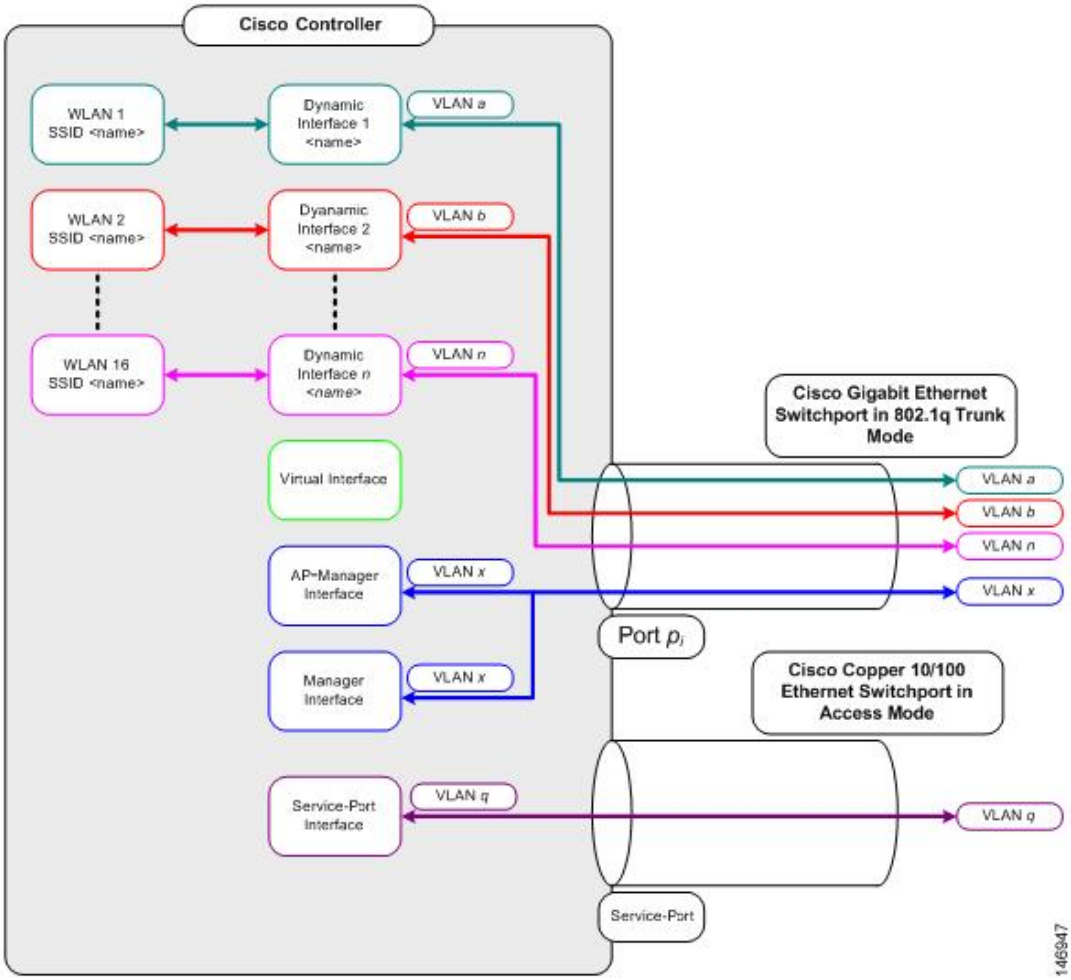
コントローラ ポートごとに別々の動的 AP マネージャ インターフェイスを設定することをお勧めします。

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 *22*：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。

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] の順に選択して、[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。

  （注） Cisco 5500 シリーズ コントローラおよび Cisco Flex 7500 シリーズ コントローラでは、物理モードは常に [Auto] に設定します。

- [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。
- [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。

ステップ 2 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 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 [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 6 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。

ポートのミラーリングの設定

ポートのミラーリングについて

ミラー モードでは、特定のクライアント デバイスまたはアクセス ポイントが起点または終点であるトラフィックをすべて別のポートに複製することができます。 このモードは、ネットワーク

で発生している特定の問題を診断するには便利です。 このポートは接続にいっさい応答しなくなりますので、ミラー モードは使用されていないポートでのみ有効にしてください。

注意事項および制約事項

- コントローラでリンク集約（LAG）が有効になっている場合、ポートのミラーリングはサポートされません。
- ネットワークに問題が発生することがあるので、あるコントローラ ポートから別のコントローラ ポートへのトラフィックのミラーリングはしないでください。

ポート ミラーリングの有効化（GUI）

ステップ 1 [Controller] > [Ports] の順に選択して、[Ports] ページを開きます。

ステップ 2 ミラー モードを有効にする未使用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。

ステップ 3 [Mirror Mode] パラメータを [Enable] に設定します。

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 次のいずれかの操作を行います。

a) コントローラで選択したポートにトラフィックをミラーリングするクライアント デバイスを選択する場合は、[Wireless] > [Clients] を選択して [Clients] ページを開きます。
b) ミラー モードを有効にするクライアントの 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。
c) [Client Details] で、[Mirror Mode] パラメータを [Enable] に設定します。

または

a) コントローラで選択したポートにトラフィックをミラーリングするアクセス ポイントを選択する場合は、[Wireless] > [Access Points] > [All APs] を選択して [All APs] ページを開きます。
b) ミラー 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] ページが表示されます。
c) [Advanced] タブを選択します。
d) [Mirror Mode] パラメータを [Enable] に設定します。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

Cisco 5500 シリーズ コントローラの USB コンソール ポートの使用

Cisco 5500 シリーズ コントローラの USB コンソール ポートは、USB タイプ A/5 ピン ミニ タイプ B ケーブルを使用して PC の USB コネクタに直接接続します。

（注） 4 ピン ミニ タイプ B コネクタは、5 ピン ミニ タイプ B コネクタと混同しやすいです。 これらに互換性はありません。 5 ピン ミニ タイプ B コネクタだけを使用できます。

Microsoft Windows で使用する場合、Cisco Windows USB コンソール ドライバをコンソール ポートに接続されているすべての PC にインストールする必要があります。 このドライバを使用すると、Windows HyperTerminal の動作に影響を与えることなく、USB ケーブルをコンソール ポートから取り外したり、コンソール ポートに接続したりすることができます。

（注） 同時にアクティブにできるのは 1 個のコンソール ポートだけです。 ケーブルを USB コンソール ポートに接続すると、RJ-45 ポートは非アクティブになります。 反対に、USB ケーブルを USB ポートから外すと、RJ-45 ポートはアクティブになります。

USB コンソール OS の互換性

はじめる前に

USB コンソールと互換性があるオペレーティング システムは次のとおりです。

- Microsoft Windows 2000、Windows XP、Windows Vista、Windows 7（Cisco Windows USB コンソール ドライバが必要）
- Apple Mac OS X 10.5.2（ドライバは不要）
- Linux（ドライバは不要）

Cisco Windows USB コンソール ドライバをインストールする手順は、次のとおりです。

ステップ 1 次の手順に従って、USB_Console.inf ドライバ ファイルをダウンロードします。

a) http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875243 をクリックして、Software Center に移動します。
b) [Wireless LAN Controllers] をクリックします。
c) [Standalone Controllers] をクリックします。
d) [Cisco 5500 Series Wireless LAN Controllers] をクリックします。

e) [Cisco 5508 Wireless LAN Controller] をクリックします。
f) USB ドライバ ファイルを選択します。
g) お使いのハード ドライブにファイルを保存します。

ステップ 2 お使いの PC にある USB ポートにタイプ A コネクタを接続します。

ステップ 3 コントローラの USB コンソール ポートにミニ タイプ B コネクタを接続します。

ステップ 4 ドライバを指定するよう要求されたら、お使いの PC の USB_Console.inf ファイルを参照します。 プロンプトに従って、USB ドライバをインストールします。

（注） また、一部のシステムには、追加のシステム ファイルが必要です。 Usbser.sys ファイルは http://support.microsoft.com/kb/918365 からダウンロードできます。

Cisco USB システム管理コンソールの COM ポートの未使用ポートへの変更

はじめる前に

USB ドライバは COM ポート 6 にマッピングされます。 一部のターミナル エミュレーション プログラムは、COM 4 より大きいポート番号のポートを認識しません。 必要に応じて、Cisco USB システム管理コンソールの COM ポートを COM 4 以下のポート番号の未使用ポートに変更する必要があります。

ステップ 1 Windows デスクトップで、[My Computer] を右クリックして、[Manage] を選択します。

ステップ 2 左側のリストから、[Device Manager] を選択します。

ステップ 3 右側のデバイスのリストで、[Ports (COM & LPT)] をダブルクリックします。

ステップ 4 [Cisco USB System Management Console 0108] を右クリックして、[Properties] を選択します。

ステップ 5 [Port Settings] タブをクリックして、[Advanced] ボタンをクリックします。

ステップ 6 [COM Port Number] ドロップダウン リストから、4 以下のポート番号の未使用 COM ポートを選択します。

ステップ 7 [OK] をクリックして保存してから、[Advanced Settings] ダイアログボックスを閉じます。

ステップ 8 [OK] をクリックして保存してから、[Communications Port Properties] ダイアログボックスを閉じます。

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る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。

リンク集約の設定

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。

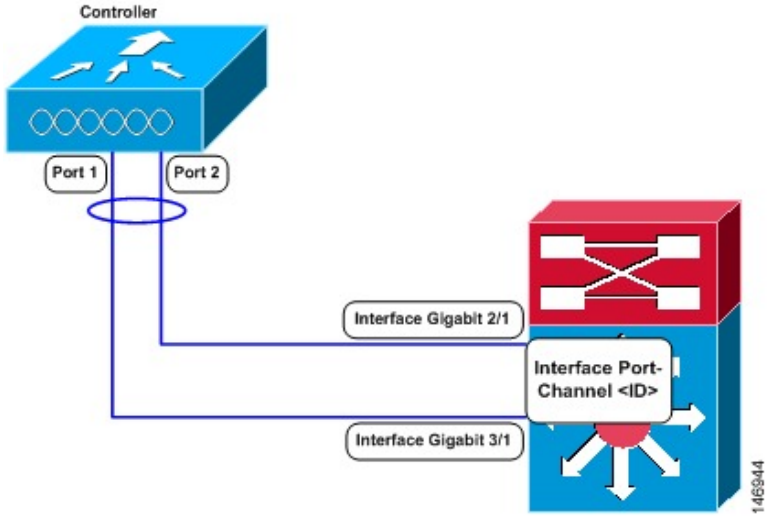
（注） LAG はスイッチ全体でサポートされます。

注意事項および制約事項

- 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の間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ネル ネゴシエーションは行われないため、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 フレームに応答せず、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。
- Catalyst スイッチでのロード バランシングは、すべての IP データグラム フラグメントの終点が単一のコントローラ ポートとなるように設定されている必要があります。 この推奨事項に従わない場合は、アクセス ポイントのアソシエートの問題が発生することがあります。
- Catalyst スイッチのロード バランシングには、**src-dst-ip**を使用することをお勧めします（**port-channel load-balance** *src-dst-ip* コマンドを入力）。
- 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 *23*：*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ブートするまで、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す。

- 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。

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
```

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

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。

注意事項および制約事項

- 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。

- 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。

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 ポイントのリブ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） AP マネージャ インターフェイスのバックアップ ポートは定義しないでください。 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 インターフェイスで障害が発生した場合は、そのインターフェイスを通してコントローラに接続しているすべてのアクセス ポイントが、他の設定済み AP マネージャ インターフェイスに均等に分散されます。

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。

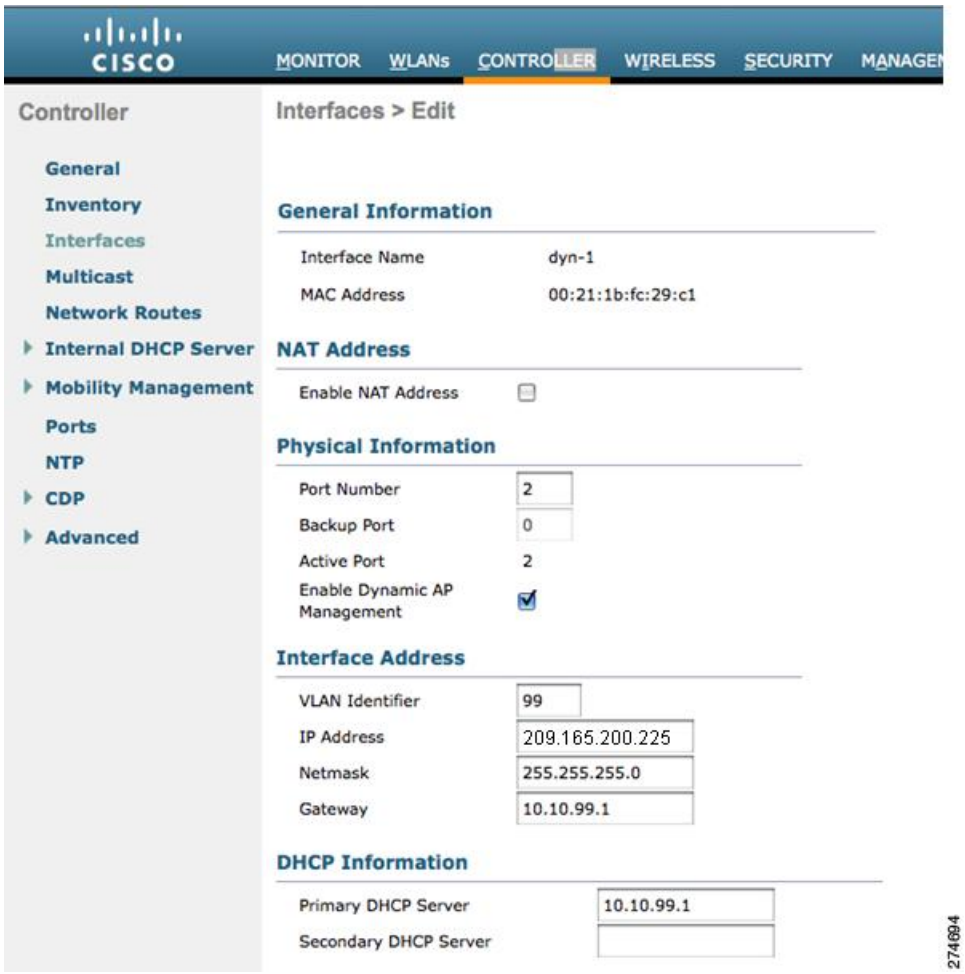
ステップ 4 作成する AP マネージャ インターフェイスそれぞれについて、この手順を繰り返します。

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 コントローラの場合、LAG を使用しないときには、動的 AP マネージャ インターフェイスを 8 つ設定して、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 7 つだけ動的 AP マネージャ インターフェイスを作成し、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。 たとえば次の図は、動的 AP マネー

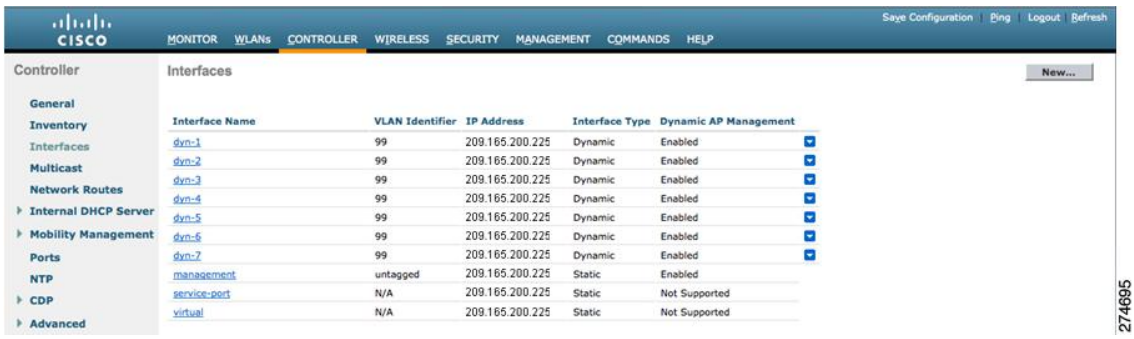
ジャインターフェイスとしてイネーブルにされていて、ポート番号2.に関連付けられた動的インターフェイスを表しています。

図 *24*：動的 *AP* 管理を使用した動的インターフェイスの例



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 *25*：*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



VLAN Select の設定

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、大量の無線クライン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がありません。 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。

注意事項および制約事項

- 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。

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 グループからを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 グループの作成（GUI）

ステップ 1 左のナビゲーション ペインから [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] をクリックして、新規グループを追加します。
[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。

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。

マルチキャスト最適化

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 上に送出されるようにして、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 をイネーブルにします。
[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 4 章

コントローラ設定の構成

この章では、コントローラの設定方法について説明します。

- ライセンスのインストールおよび設定，106 ページ
- ライセンスの再ホスト，118 ページ
- ライセンス エージェントの設定，123 ページ
- 802.11 帯域の設定，126 ページ
- 802.11n のパラメータの設定，130 ページ
- 802.11h のパラメータの設定，134 ページ
- DHCP プロキシの設定，136 ページ
- 管理者のユーザ名とパスワードの設定，137 ページ
- SNMP の設定，139 ページ
- SNMP v3 ユーザのデフォルト値の変更，142 ページ
- アグレッシブ ロード バランシングの設定，144 ページ
- 帯域選択の設定，147 ページ
- 高速 SSID 変更の設定，150 ページ
- 802.3X のフロー制御の有効化，150 ページ
- 802.3 ブリッジの設定，151 ページ
- マルチキャスト モードの設定，152 ページ
- クライアント ローミングの設定，159 ページ
- IP-MAC アドレス バインディングの設定，164 ページ
- Quality of Service の設定，166 ページ
- Quality of Service ロールの設定，169 ページ

- 音声パラメータとビデオ パラメータの設定，172 ページ
- SIP ベースの CAC の設定，187 ページ
- メディア パラメータの設定，188 ページ
- 優先コール番号を使用した音声優先制御の設定，189 ページ
- EDCA パラメータの設定，191 ページ
- Cisco Discovery Protocol の設定，193 ページ
- コントローラと NTP サーバの認証の設定，202 ページ
- RFID タグ追跡の設定，203 ページ
- ロケーション設定の実行および表示，207 ページ
- コントローラのデフォルト設定へのリセット，217 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。

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。

ライセンスに関する注意事項および制限事項

- 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、ライセンスを用意する必要があります。

- 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。 WCS BASE および PLUS ライセンシング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
- 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。 機能が使用できなくなる、あるいは動作しなくなることはありません。
  - 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可キー（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2つの方法のいずれかを使用して PAK を登録します。

- **Cisco License Manager（CLM）**：ライセンスの取得とシスコデバイスへの展開が自動的に行われます。 コントローラの数が 5 台を超える場合は、CLM を使用して PAK の登録とライセンスのインストールを行うことをお勧めします。 CLM では、ライセンスの再ホストや RMA を行うこともできます。

  （注） ライセンスを受けたフィーチャ セットの変更や、評価版 ap-count ライセンスのアクティブ化は、CLM では実行できません。 これらの作業を実行するには、「ap-count 評価ライセンスのアクティブ化」の項の手順に必要があります。それ以外のライセンスに関する作業はすべて CLM で実行できるので、この章の記述のうち、前述の 2 つの項と「ライセンス エージェントの設定」の項以外は無視してもかまいません。コントローラと CLM との通信に HTTP を使用する場合は、も参照してください。

  （注） CLM ソフトウェアのダウンロードおよびユーザ ドキュメントへのアクセスは、次の URL で実行できます。 http://www.cisco.com/go/clm

- **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 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

  以下に類似した情報が表示されます。

```
Administrative statistics
        Install success count:       2
        Install failure count:       0
        Install duplicate count:     0
        Comment add count:           0
        Comment delete count:        0
        Clear count:          0
        Save count:          2
        Save cred count:          0
Client status
        Request success count              2
        Request failure count      0
        Release count              0
        Global Notify count              6
```

- 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

  以下に類似した情報が表示されます。

```
  Feature name       Enforcement  Evaluation  Clear Allowed   Enabled
   base                    yes         yes          yes           yes
   base-ap-count           yes         yes          yes           no
```

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 エージェントのデバッグを設定します。
  debug license agent {**errors** | **all**} {**enable** | **disable**}
- 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。

a) 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。

b) [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。

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「High」、ステータスが「In Use」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。

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 ボックスは、ライセンスが使用中かどうかを表し、[License Priority] テキスト ボックスは各ライセンスの現在の優先度を表します。

（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 ライセンスの使用中の数が、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) base-ap-count 評価ライセンスの優先度を上げるには、次のコマンドを入力します。
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) 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するには、次のコマンドを入力します。
reset system

c) ap-count評価ライセンスの優先度が「高」、ステータスが「使用中」になったことを確認するには、次のコマンドを入力します。
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) ap-count 評価ライセンスの優先度を下げるには、次のコマンドを入力します。
license modify priority *license_name* **low**

b) 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するには、次のコマンドを入力します。
reset system

c) ap-count評価ライセンスの優先度が「低」、ステータスが「非使用中」になったことを確認するには、次のコマンドを入力します。
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。

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別のコントローラに基本ライセンスを移行できます。

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。

評価ライセンスおよび永久ベース イメージ ライセンスは再ホストできません。

（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。

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) ライセンスをコントローラから取り消すには、次のコマンドを入力します。
license revoke *permission_ticket_url*

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

b) 再ホスト チケットを生成するには、次のコマンドを入力します。
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），（110 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。

ライセンス エージェントの設定

ライセンス エージェントの設定について

ネットワークにさまざまなライセンスを持つシスコデバイスが含まれる場合、Cisco License Manager（CLM）を使用して、1 つのアプリケーションによるすべてのライセンスの管理を検討することを推奨します。 CLM は、ネットワーク全体でシスコ ソフトウェアのライセンスを管理する、セキュアなクライアント/サーバ アプリケーションです。

ライセンス エージェントは、コントローラで稼働するインターフェイス モジュールであり、CLM とコントローラのライセンス インフラストラクチャを仲介します。 CLM は、HTTP、Telnet などのさまざまなチャネルを使用してコントローラと通信できます。 通信方法として HTTP を使用する場合、コントローラでライセンス エージェントを有効にする必要があります。

ライセンス エージェントは、CLM から要求を受け取ってライセンス コマンドに変換します。 また、CLM への通知の送信も行います。 ライセンス エージェントは HTTP または HTTPS 経由で

XML メッセージを使用して、要求の受信および通知の送信を行います。 たとえば、CLM は **license install** コマンドを送信します。また、エージェントは、ライセンスの期限が切れると CLM に通知します。

（注） CLM ソフトウェアのダウンロードおよびユーザ ドキュメントへのアクセスは、http://www.cisco.com/go/clm で実行できます。

ライセンス エージェントの設定（GUI）

ステップ 1 [Management] > [Software Activation] > [License Agent] を選択して、[License Agent Configuration] ページを開きます。

ステップ 2 [Enable Default Authentication] チェックボックスをオンにしてライセンス エージェントを有効にします。オンにしなければ、この機能は無効になります。 デフォルト値はオフです。

ステップ 3 [Maximum Number of Sessions] テキスト ボックスに、ライセンス エージェントの最大セッション数を入力します。 有効な範囲は 1 ～ 25 セッションです。

ステップ 4 次の手順に従って、CLM からの要求をリッスンするようにライセンス エージェントを設定します。

a) [Enable Listener] チェックボックスをオンにして、CLM からライセンス要求をライセンス エージェントが受信できるようにします。このチェックボックスをオンにしなければ、この機能は無効になります。デフォルト値はオフです。

b) [Listener Message Processing URL] テキスト ボックスに、ライセンス エージェントがライセンス要求を受け取る URL（たとえば http://209.165.201.30/licenseAgent/custom）を入力します。 [Protocol] パラメータは、URL に HTTP と HTTPS のどちらが必要かを示します。

（注） 使用するプロトコルを指定するには、[HTTP Configuration] ページを使用します。

c) [Enable Authentication for Listener] チェックボックスをオンにして、ライセンス エージェントがライセンス要求を受け取るときに認証を行うようにします。このチェックボックスをオンにしなければ、この機能は無効になります。 デフォルト値はオフです。

d) [Max HTTP Message Size] テキスト ボックスに、ライセンス要求の最大サイズを入力します。 有効な値の範囲は 0 ～ 9999 バイトで、デフォルト値は 0 です。

ステップ 5 次の手順に従って、CLM にライセンス通知を送信するようにライセンス エージェントを設定します。

a) [Enable Notification] チェックボックスをオンにして、ライセンス エージェントが CLM にライセンス通知を送信できるようにします。このチェックボックスをオンにしなければ、この機能は無効になります。 デフォルト値はオフです。

b) [URL to Send the Notifications] テキスト ボックスに、ライセンス エージェントが通知を送信する URL（たとえば http://www.cisco.com/license/notify）を入力します。

c) [User Name] テキスト ボックスに、この URL で通知メッセージを表示するのに必要なユーザ名を入力します。

d) [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 URL で通知メッセージを表示するのに必要なパスワードを入力します。

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、変更を保存します。

ライセンス エージェントの設定（CLI）

ステップ 1 次のコマンドのいずれかを入力して、ライセンス エージェントを有効にします。

- **config license agent default authenticate**：ライセンス エージェントのデフォルト リスナーを有効にします。認証も行います。
- **config license agent default authenticate none**：ライセンス エージェントのデフォルト リスナーを有効にします。認証は行いません。

（注） ライセンス エージェントのデフォルト リスナーを無効にするには、**config license agent default disable** コマンドを入力します。 デフォルト値は [disabled] です。

ステップ 2 次のコマンドを入力して、ライセンス エージェントの最大セッション数を指定します。
config license agent max-sessions *sessions*

sessions パラメータの有効な値の範囲は 1 ～ 25 で、デフォルト値は 9 です。

ステップ 3 次のコマンドを入力して、ライセンス エージェントが CLM からライセンス要求を受信できるようにするとともに、要求を受信する URL を指定します。
config license agent listener http {**plaintext** | **encrypt**} *url* **authenticate** [**none**] [**max-message** *size*] [**acl** *acl*]

size パラメータの有効な範囲は 0 ～ 65535 バイトで、デフォルト値は 0 です。

（注） ライセンス エージェントが CLM からライセンス要求を受信しないようにするには、**config license agent listener http disable** コマンドを入力します。 デフォルト値は [disabled] です。

ステップ 4 次のコマンドを入力して、ライセンス エージェントが CLM にライセンス通知を送信するように設定するとともに、通知を送信する URL を指定します。
config license agent notify *url username password*

（注） ライセンス エージェントが CLM にライセンス通知を送信しないようにするには、**config license agent notify disable** *username password* コマンドを入力します。デフォルト値は [disabled] です。

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 次のコマンドを入力して、ライセンス エージェントのカウンタまたはセッションの統計情報を確認します。
show license agent {**counters** | **sessions**}

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

```
License Agent Counters
Request Messages Received:10: Messages with Errors:1
Request Operations Received:9: Operations with Errors:0
Notification Messages Sent:12: Transmission Errors:0: Soap Errors:0
```

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

```
License Agent Sessions: 1 open, maximum is 9
```

（注） ライセンスエージェントのカウンタまたはセッションの統計情報をクリアするには、**clear license agent** {**counters** | **sessions**} コマンドを入力します。

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（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 の両方が有効になっています。

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 トラフィック専用に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] 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。

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、そこのネットワークに 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 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 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。

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ドバ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、そこのネットワークに 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、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 8 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 9 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 10 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 802.11b 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 11 **save config** コマンドを入力して、変更を保存します。

ステップ 12 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
```

802.11n のパラメータの設定

802.11n の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 レートを使用できるのは、1140、1260、3500、および 3600 シリーズ アクセス ポイントです。このときに、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。

802.11n のパラメータの設定（GUI）

ステップ 1 [Wireless] > [802.11a/n（または 802.11b/g/n）] > [High Throughput (802.11n)] の順に選択して [802.11n (5 GHz または 2.4 GHz) 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。

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（または 802.11b/g/n）Cisco APs > Configure] ページまたは [802.11a/n（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 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、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**}

ステップ 2 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**}

ステップ 3 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。

ステップ 4 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。

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。 次の表は、トラフィック タイプごとに割り当てられる優先レベル（0 ～ 7）の説明です。

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 送信が使用されます。 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**

ステップ 5 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。

ステップ 6 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**}

ステップ 7 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**}

ステップ 8 **save config** コマンドを入力します。

ステップ 9 次のコマンドを入力して、802.11a/n または 802.11b/g/n 帯域の設定を表示します。
show {**802.11a** | **802.11b**}

その他の関連資料

Radio Resource Management（RRM）パラメータの設定と、802.11n アクセス ポイントの無線パラメータの静的割り当ての方法については、Radio Resource Management の設定, （825 ページ）を参照してください。

802.11h のパラメータの設定

802.11h のパラメータの設定について

802.11h では、チャ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 次の手順に従って、802.11a 帯域を無効にします。

a) [Wireless] > [802.11a/n] > [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] をクリックして、変更を適用します。

ステップ 2 [Wireless] > [802.11a/n] > [DFS (802.11h)] の順に選択して [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ネルに切り替えたときに新しいチャネル番号がアナウンスされるようにする場合は、[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 [disabled] です。

ステップ 5 チャネル 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 [disabled] 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 次の手順に従って、802.11a 帯域を有効にします。

a) [Wireless] > [802.11a/n] > [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] をクリックして、変更を適用します。

ステップ 8 [Save Configuration] をクリックして、変更を保存します。

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ネルに切り替えたときの新しいチャ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** | **disable**} *switch_mode*

switch_mode パラメータには 0 または 1 を入力できます。チャネルが実際に切り替えられるまで送信を制限する場合は 0 を入力し、制限しない場合は 1 を入力します。 デフォルト値は [disabled] です。

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

DHCP プロキシの設定

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。 そのため、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部分が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 トンネルを通っ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。

注意事項および制約事項

- DHCP プロキシは、デフォルトで有効になっています。
- 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

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（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 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）

コントローラ CLI を使用して DHCP 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。

config dhcp timeout *seconds*

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と、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

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

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 の設定

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。

ステップ 1 SNMP コミュニティ名を作成するには、**config snmp community create** *name* コマンドを入力します。

ステップ 2 SNMP コミュニティ名を削除するには、**config snmp community delete** *name* コマンドを入力します。

ステップ 3 読み取り専用権限を持つ SNMP コミュニティ名を設定するには、**config snmp community accessmode ro** *name* コマンドを入力します。 読み取りと書き込み権限を持つ SNMP コミュニティ名を設定するには、**config snmp community accessmode rw** *name* と入力します。

ステップ 4 SNMP コミュニティの IP アドレスとサブネット マスクを設定するには、**config snmp community ipaddr** *ip-address ip-mask name* コマンドを入力します。

（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。

ステップ 5 コミュニティ名を有効にするには、**config snmp community mode enable** コマンドを入力します。 コミュニティ名を無効にするには、**config snmp community mode disable** コマンドを入力します。

ステップ 6 トラップの宛先を設定するには、**config snmp trapreceiver create** *name ip-address* コマンドを入力します。

ステップ 7 トラップを削除するには、**config snmp trapreceiver delete** *name* コマンドを入力します。

ステップ 8 トラップの宛先を変更するには、**config snmp trapreceiver ipaddr** *old-ip-address name new-ip-address* コマンドを入力します。

ステップ 9 トラップを有効にするには、**config snmp trapreceiver mode enable** コマンドを入力します。 トラップを無効にするには、**config snmp trapreceiver mode disable** コマンドを入力します。

ステップ 10 SNMP 担当者の名前を設定するには、**config snmp syscontact** *syscontact-name* と入力します。 担当者名には、最大 31 文字の英数字を使用できます。

ステップ 11 SNMP システムの場所を設定するには、**config snmp syslocation** *syslocation-name* コマンドを入力します。 場所の名前には、最大 31 文字の英数字を使用できます。

ステップ 12 **show snmpcommunity** コマンドおよび **show snmptrap** コマンドを使用して、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。

ステップ 13 **show trapflags** コマンドを使用して、各トラップ フラグが有効か無効かを表示します。 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。

ステップ 14 リリース 7.0.116.0 以降では、SNMP エンジン ID も設定できます。 **config snmp engineID** *engine-id-string* コマンドを使用して、SNMP エンジン ID を設定します。

（注） エンジン ID の文字列には、最大 24 文字を使用できます。

ステップ 15 **show engineID** コマンドを使用して、エンジン ID を表示します。

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 プロトコル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 **save config** コマンドを入力して、変更を保存します。

ステップ 8 「public」または「private」コミュニティ ストリングのデフォルト値を変更する必要がまだある場合は、この手順を繰り返します。

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。

アグレッシブ ロード バランシングの設定

アグレッシブなロード 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と、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。

（注） Cisco 600 シリーズ OfficeExtend アクセス ポイントと 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せん。

アグレッシブ ロード バランシングの設定

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 **save config** 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、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

以下に類似した情報が表示されます。

```
Aggressive Load Balancing..................... per WLAN enabling
Aggressive Load Balancing Window.............. 5 clients
Aggressive Load Balancing Denial Count........... 3
Aggressive Load Balancing Uplink Threshold....... 50

Statistics (client-count based)
Total Denied Count............................. 0 clients
Total Denial Sent.............................. 0 messages
Exceeded Denial Max Limit Count................ 0 times
None 5G Candidate Count........................ 0 times
None 2.4G Candidate Count...................... 0 times

Statistics (uplink-usage based)
Total Denied Count............................. 0 clients
Total Denial Sent.............................. 0 messages
Exceeded Denial Max Limit Count................ 0 times
None 5G Candidate Count........................ 0 times
```

```
None 2.4G Candidate Count..................... 0 times
```

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

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ネル干渉も発生します。802.11b/g では、重複しないチャネルが 3 つしかないからです。 これらの干渉の原因を緩和して、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 チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。

注意事項および制約事項

- 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。
- 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。

（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 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応答するための最小 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。

ステップ 9 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、[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 [Save Configuration] をクリックして、変更を保存します。

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。

高速 SSID 変更の設定

高速 SSID 変更の設定について

コントローラ上で Fast SSID Change が有効になっているときは、クライアントは SSID 間で移動することができます。 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、コントローラの通信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。 Fast SSID Change が無効のときは、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 の設定

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 [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。

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 **save config** コマンドを入力して、設定を保存します。

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、**config switchconfig flowcontrol enable** コマンドを入力します。

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。

注意事項および制約事項

- 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。 現在サポートされている 802.3 Raw フレームは、次のフォーマットのものだけです。

  +------------------+--------------------+----------------+------------------------+

  | 宛先 | 送信元 | 合計パケット | ペイロード ..... | MAC アドレス | MAC アドレス | 長 |

  +------------------+--------------------+----------------+------------------------

- 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。
- 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 [disabled] です。

ステップ 3 **save config** コマンドを入力して、設定を保存します。

マルチキャスト モードの設定

マルチキャスト モードの設定について

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。

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、最後のレポータ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。

注意事項および制約事項

- 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 join 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って、マルチキャストの帯域幅は大きくする必要がない場合、単一の Basic レートを設定し、無線セルの端に到達するために十分な低さにします。
- 特定のスループットを達成するために特定のデータ レートでマルチキャスト データを送信する必要がある場合、そのレートを最高の Basic レートとして設定できます。 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。
- Cisco Flex 7500 シリーズ コントローラは、マルチキャスト モードをサポートしません。

マルチキャスト モードの設定

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 [disabled] 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 [disabled] 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 [disabled] 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 [disabled] 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 [disabled] 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 **save config** コマンドを入力して、設定を保存します。

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*

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

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。

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。

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 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] の下の [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

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（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 –80 ～ –90 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ときに必要なアクセス 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 –70 ～ –77 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。

範囲は 1 ～ 10 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（802.11a または 802.11b/g）についてクライアント 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**}

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

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

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............................. ctrl4404
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?>
```

Quality of Service の設定

Quality of Service の設定について

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。 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。

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]（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 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。

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。

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） burst-realtime-rate は average-realtime-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。

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） burst-realtime-rate は average-realtime-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。

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。

ステップ 11 802.11a および 802.11b/g ネットワークを有効にします。
無線ネットワークを有効にするには、[Wireless] > [802.11a/n] 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 802.11a disable network

config 802.11b 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 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 4 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す。

ステップ 5 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 802.11a enable network

config 802.11b enable network

Quality of Service ロールの設定

Quality of Service ロールの設定について

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] をクリックして、変更を確定します。

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。

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。

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） burst-realtime-rate は average-realtime-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。

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 コントローラでのローカル ネットワーク ユーザの設定, （256 ページ）の項の手順に従って、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） burst-realtime-rate は average-realtime-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。

（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
```

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。

- コール アドミッション制御

- 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） CCX は、AP1030 ではサポートされません。

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に 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，（151 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す。 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	Expedited Bandwidth Request を 使用した TSPEC
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しないため、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、リブ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
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、WCS または NCS 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（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] 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] 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 [disabled] 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は、85 % を超えてはなりません。

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 のこのチェックボックスはオフになっています。

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。 最大コール数の制限に達すると、新規コールやローミングイン コールはできなくなります。
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] をクリックして、変更を確定します。

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] 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有効にします。

ステップ 19 [Save Configuration] をクリックして、変更を保存します。

ステップ 20 別の無線帯域（802.11a または 802.11b/g）について音声パラメータの設定をする場合、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 TSM 音声メトリックを表示するには、次のコマンドを入力します。
show [802.11a | 802.11b] cu-metrics *AP_Name*

このコマンドでは、チャ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] 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] 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 [disabled] 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は、85 % を超えてはなりません。
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に SIP CAC を有効にすることはできません。

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 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] 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有効にします。

ステップ 13 [Save Configuration] をクリックして、変更を保存します。

ステップ 14 別の無線帯域（802.11a または 802.11b/g）についてビデオ パラメータの設定をする場合、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いものと想定して、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] または [802.11b/g/n] の順に選択します。 [802.11a/n 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、802.11a または 802.11b/g ネットワークに対する 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 でリブートが必要になったとします。 AP がリブートされた後も、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） 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アクセス ポイントすべての TSM 統計情報をクリアするには、**clear client tsm** {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**} コマンドを入力します。

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 client 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、以下に示す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

注意事項および制約事項

- 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] 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] 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 [disabled] 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 [disabled] 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。

注意事項および制約事項

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

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。 コントローラの GUI または CLI を使用して EDCA パラメータを設定するには、この項の手順に従ってください。

EDCA パラメータの設定

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] 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] 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。 768 ビットは、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 Managment（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] 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] をクリックして、変更を保存します。

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| optimzed-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。 768 ビットは、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 Managment（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 [disabled] 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。

Cisco Discovery Protocol の設定

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。

注意事項および制約事項

- 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す。

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。この機能を無効にする場合は、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す。

  [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**

  show ap cdp neighbors all コマンドを入力すると、次のような情報が表示されます。

```
AP Name                AP IP      Neighbor Name    Neighbor IP       Neighbor Port
--------               --------    -------------    -----------       -------------
AP0013.601c.0a0    10.76.108.123    6500-1         10.76.108.207    GigabitEthernet1/26
AP0013.601c.0b0    10.76.108.111    6500-1         10.76.108.207    GigabitEthernet1/27
AP0013.601c.0c0    10.76.108.125    6500-1         10.76.108.207    GigabitEthernet1/28
```

  show ap cdp neighbors detail all コマンドを入力すると、次のような情報が表示されます。

```
AP Name: AP0013.601c.0a0
AP IP Address: 10.76.108.125
----------------------------------
Device ID: 6500-1
Entry address(es): 10.76.108.207
Platform: cisco WS-C6506-E,  Capabilities: Router Switch IGMP
Interface: Port - 1,  Port ID (outgoing port): GigabitEthernet1/26
Holdtime: 157 sec

Version:
Cisco Internetwork Operating System Software  IOS (tm) s72033_rp Software (s72033_rp-PSV-M),
Version 12.2(18)SXD5, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport
 Copyright (c) 1986-2005 by Cisco Systems, Inc. Compiled Fri 13-Ma
```

（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

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

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。

コントローラと NTP サーバの認証の設定

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 Severs] 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。

RFID タグ追跡の設定

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	—	—	—	—
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ドバ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

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

以下に類似した情報が表示されます。

```
RFID Tag data Collection..................... Enabled
RFID timeout................................. 1200 seconds
RFID mobility................................ Oui:00:14:7e : Vendor:pango
               State:Disabled
```

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。

以下に類似した情報が表示されます。

```
RFID address................................. 00:12:b8:00:20:52
Vendor....................................... G2
Last Heard................................... 51 seconds ago
Packets Received............................. 2
Bytes Received............................... 324
Cisco Type...................................

Content Header
==================
Version...................................... 1
Tx Power..................................... 12 dBm
Channel...................................... 1
Reg Class.................................... 12
Burst Length................................. 1

CCX Payload
===========
Last Sequence Control........................ 0
Payload length............................... 127
```

```
Payload Data Hex Dump

01 09 00 00 00 00 0b 85 52 52 52 02 07 4b ff ff
7f ff ff ff 03 14 00 12 7b 10 48 53 c1 f7 51 4b
50 ba 5b 97 27 80 00 67 00 01 03 05 01 42 34 00
00 03 05 02 42 5c 00 00 03 05 03 42 82 00 00 03
05 04 42 96 00 00 03 05 05 00 00 00 55 03 05 06
42 be 00 00 03 02 07 05 03 12 08 10 00 01 02 03
04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 03 0d 09 03
08 05 07 a8 02 00 10 00 23 b2 4e 03 02 0a 03

Nearby AP Statistics:
      lap1242-2(slot 0, chan 1) 50 seconds ag.... -76 dBm
      lap1242(slot 0, chan 1) 50 seconds ago..... -65 dBm
```

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

以下に類似した情報が表示されます。

```
Total Number of RFID   : 24
----------------- -------- ------------------ ------ ---------------------
     RFID ID      VENDOR       Closest AP      RSSI  Time Since Last Heard
----------------- -------- ------------------ ------ ---------------------
00:04:f1:00:00:03 Wherenet flexconnect               -70      151 seconds ago
00:04:f1:00:00:05 Wherenet flexconnect               -66      251 seconds ago
00:0c:cc:5b:f8:1e Aerosct  flexconnect               -40        5 seconds ago
00:0c:cc:5c:05:10 Aerosct  flexconnect               -68       25 seconds ago
00:0c:cc:5c:06:69 Aerosct  flexconnect               -54        7 seconds ago
00:0c:cc:5c:06:6b Aerosct  flexconnect               -68      245 seconds ago
00:0c:cc:5c:06:b5 Aerosct  cisco1242                 -67       70 seconds ago
00:0c:cc:5c:5a:2b Aerosct  cisco1242                 -68       31 seconds ago
00:0c:cc:5c:87:34 Aerosct  flexconnect               -40        5 seconds ago
00:14:7e:00:05:4d Pango    cisco1242                 -66      298 seconds ago
```

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 タグがクライアント モードである場合、以下に類似した情報が表示されます。

```
------------------  -------- --------- ----------------- ------ ----------------
                                  Heard
   RFID Mac           VENDOR   Sec Ago    Associated AP    Chnl    Client State
------------------  -------- --------- ----------------- ------ ----------------

00:14:7e:00:0b:b1     Pango      35      AP0019.e75c.fef4    1        Probing

When the RFID tag is not in client mode, the above text boxes are blank.
```

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。

ロケーション設定の実行および表示

ロケーション設定の実行および表示について

ここでは、コントローラ CLI からロケーション設定を実行および表示する手順について説明します。

コントローラと Mobility Services Engine の同期

Mobility Services Engine がネットワーク上にインストールされている場合は、コントローラ上で時間帯が設定されていることが必要になります。これは、この 2 つのシステムを正しく同期させるためです。 また、2つのデバイスの時刻が同期されている必要があります。 Mobility Services Engine

が存在しないネットワークであっても、時刻を設定することをお勧めします。 コントローラ上で時刻と日付を設定する手順については、「802.11 帯域の設定」の項を参照してください。

（注） 時間帯はコントローラとロケーション アプライアンスとで異なっていてもかまいませんが、時間帯デルタは GMT を基準として設定されていなければなりません。

ロケーションの設定

ロケーションの設定（CLI）

コントローラは、クライアント デバイスのロケーションを特定するために、対象クライアント周辺のアクセス ポイントから Received Signal Strength Indication（RSSI; 受信信号強度表示）測定値を収集します。 コントローラは、最大 16 台のアクセス ポイントから、クライアント、RFID、および不正なアクセス ポイントのロケーション レポートを取得できます。

ロケーションの精度を高めるために、次のコマンドを入力して、通常のクライアントまたは調整クライアントのパス損失測定（S60）要求を設定します。

config location plm *?*

ここで、*?* は、次のいずれかを示します。

- **client** {**enable** | **disable**} *burst_interval*：通常の、非調整クライアントのパス損失測定要求を有効または無効にします。 *burst_interval* パラメータの有効な値の範囲は 1 ～ 3600 秒で、デフォルト値は 60 秒です。
- **calibrating** {**enable** | **disable**} {**uniband** | **multiband**}：アソシエートされた 802.11a または 802.11b/g 無線上またはアソシエートされた 802.11a/b/g 無線上の調整クライアントのパス損失測定要求を有効または無効にします。

クライアントからプローブが送信される頻度が低い場合や、少数のチャネルに対してしか送信されない場合は、クライアントのロケーションが更新不可能になるか、精度が低下します。 **config location plm** コマンドを実行すると、クライアントは強制的に、すべてのチャネルに対してパケットを送信するようになります。 CCXv4 以上のクライアントがアソシエートすると、コントローラはそのクライアントにパス損失測定要求を送信します。これは、アクセス ポイントが使用している帯域とチャネル（2.4 GHz のみのアクセス ポイントの場合は一般にチャネル 1、6、および 11）で無期限に送信するようクライアントに指示するものです。送信する間隔は設定可能です（たとえば 60 秒）。

ロケーションに関する CLI コマンドは、この他に次の 4 つがありますが、これらのコマンドのデフォルト値は最適な値に設定されているので、変更することはお勧めしません。

- 次のコマンドを入力して、デバイスの種類ごとに RSSI タイムアウト値を設定します。

  config location expiry *?*

  ここで、*?* は、次のいずれかを示します。

- **client** *timeout*：クライアントの RSSI タイムアウト値を設定します。 *timeout* パラメータの有効な値の範囲は 5 ～ 3600 秒で、デフォルト値は 5 秒です。
- **calibrating-client** *timeout*：調整クライアントの RSSI タイムアウト値を設定します。 *timeout* パラメータの有効な値の範囲は 0 ～ 3600 秒で、デフォルト値は 5 秒です。
- **tags** *timeout*：RFID タグの RSSI タイムアウト値を設定します。 *timeout* パラメータの有効な値の範囲は 5 ～ 300 秒で、デフォルト値は 5 秒です。
- **rogue-aps** *timeout*：不正なアクセス ポイントの RSSI タイムアウト値を設定します。 *timeout* パラメータの有効な値の範囲は 5 ～ 3600 秒で、デフォルト値は 5 秒です。

  ロケーションを正確に特定するには、CPU が保持する RSSI が最近のものであることと、その値が大きいことが必要です。 **config location expiry** コマンドを使用すると、古い RSSI 平均値が失効するまでの時間の長さを指定できます。

（注） **config location expiry** コマンドは、使用したり、変更したりしないことをお勧めします。

- 次のコマンドを入力して、デバイスの種類別に RSSI 半減期を設定します。

  config location rssi-half-life *?*

  ここで、*?* は、次のいずれかを示します。

  - **client** *half_life*：クライアントの RSSI 半減期を設定します。 *half_life* パラメータの有効な値は、0、1、2、5、10、20、30、60、90、120、180、または300秒です。デフォルト値は 0 秒です。
  - **calibrating-client** *half_life*：調整クライアントの RSSI 半減期を設定します。 *half_life* パラメータの有効な値は、0、1、2、5、10、20、30、60、90、120、180、または300秒です。デフォルト値は 0 秒です。
  - **tags** *half_life*：RFID タグの RSSI 半減期を設定します。 *half_life* パラメータの有効な値は、0、1、2、5、10、20、30、60、90、120、180、または300秒です。デフォルト値は 0 秒です。
  - **rogue-aps** *half_life*：不正なアクセス ポイントの RSSI 半減期を設定します。 *half_life* パラメータの有効な値は、0、1、2、5、10、20、30、60、90、120、180、または300秒です。デフォルト値は 0 秒です。

    クライアント デバイスの中には、チャネル変更直後は送信電力を下げるものがあるのと、RF は変動しやすいことから、RSSI の値がパケットごとに大きく異なることもあります。 **config location rssi-half-life** コマンドを実行すると、精度を向上させるために、均一でない状態で到着したデータを平均化するための半減期（ハーフ ライフ）を設定することができます。

（注） **config location rssi-half-life** コマンドは、使用したり、変更したりしないことをお勧めします。

- 次のコマンドを入力して、RSSI 測定に関する NMSP 通知しきい値を設定します。

  config location notify-threshold *?*

  ここで、*?* は、次のいずれかを示します。

  - **client** *threshold*：クライアントおよび不正クライアントの NMSP 通知しきい値（dB）を設定します。 *threshold* の有効な値の範囲は 0 ～ 10 dB で、デフォルト値は 0 dB です。
  - **tags** *threshold*：RFID タグの NMSP 通知しきい値（dB）を設定します。 *threshold* の有効な値の範囲は 0 ～ 10 dB で、デフォルト値は 0 dB です。
  - **rogue-aps** *threshold*：不正なアクセス ポイントの NMSP 通知しきい値（dB）を設定します。 *threshold* の有効な値の範囲は 0 ～ 10 dB で、デフォルト値は 0 dB です。

  （注） **config location notify-threshold** コマンドは、使用したり、変更したりしないことをお勧めします。

- 次のコマンドを入力して、RSSI および信号対雑音比（SNR）の値の平均化に使用するアルゴリズムを設定します。

  config location algorithm *?*

  ここで、*?* は、次のいずれかを示します。

  - **simple**：必要とする CPU オーバーヘッドは小さいけれども精度が低い、高速アルゴリズムを指定します。
  - **rssi-average**：精度は高いけれども、必要とする CPU オーバーヘッドも大きいアルゴリズムを指定します。

  （注） **config location algorithm** コマンドは、使用したり、変更したりしないことをお勧めします。

ロケーション設定の表示（CLI）

ロケーション情報を表示するには、次の CLI コマンドを使用します。

- 次のコマンドを入力して、現在のロケーション設定値を表示します。

  show location summary

以下に類似した情報が表示されます。

```
Location Summary

Algorithm used:                          Average
Client
  RSSI expiry timeout:          5 sec
  Half life:          0 sec
  Notify Threshold:          0 db
Calibrating Client
  RSSI expiry timeout:          5 sec
  Half life:          0 sec
Rogue AP
  RSSI expiry timeout:                     5 sec
  Half life:          0 sec
  Notify Threshold:          0 db
RFID Tag
  RSSI expiry timeout:                    5 sec
  Half life:          0 sec
  Notify Threshold:          0 db
```

- 次のコマンドを入力して、特定のクライアントの RSSI テーブルを表示します。

  show location detail *client_mac_addr*

  以下に類似した情報が表示されます。

```
...
[11] AP 00:00:00:00:00:00 :  Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0)
(antenna-B 0), band 0  rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
[12] AP 00:00:00:00:00:00 :  Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0)
(antenna-B 0), band 0  rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
[13] AP 00:00:00:00:00:00 :  Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0)
(antenna-B 0), band 0  rssi (antenna-A -1) (antenna-B 0), snr 0, acceptable 0
[14] AP 00:00:00:00:00:00 :  Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0)
(antenna-B 0), band 0  rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
[15] AP 00:00:00:00:00:00 :  Slot 0 inUse 0, expired 0, Timestamp (antenna-A 0)
(antenna-B 0), band 0  rssi (antenna-A 0) (antenna-B 0), snr 0, acceptable 0
```

- 次のコマンドを入力して、ロケーションベースの RFID 統計を表示します。

  show location statistics rfid

  以下に類似した情報が表示されます。

```
RFID Statistics

Database Full :          0        Failed Delete:          0
Null Bufhandle:          0        Bad Packet:             0
Bad LWAPP Data:          0        Bad LWAPP Encap:        0
Off Channel:             0        Bad CCX Version:        0
Bad AP Info :            0
Above Max RSSI:          0        Below Max RSSI:         0
Invalid RSSI:            0        Add RSSI Failed:        0
Oldest Expired RSSI:     0         Smallest Overwrite:    0
```

- 次のコマンドを入力して、ロケーションベースの RFID 統計をクリアします。

  clear location statistics rfid

- 次のコマンドを入力して、特定の RFID タグまたはデータベース全体のすべての RFID タグをクリアします。

  clear location rfid {*mac_address* | **all**}

- 次のコマンドを入力して、クライアントでロケーション表示（S69）がサポートされているかどうかを表示します。

  show client detail *client_mac*

  ロケーション表示がクライアントでサポートされており、かつロケーションアプライアンス上で有効化されているときは、ロケーションアプライアンスはその位置を要求に応じてクライアントに知らせることができます。 CCXv5 クライアントでは、ロケーション表示は自動的に有効になります。

  以下に類似した情報が表示されます。

```
Client MAC Address.............................. 00:40:96:b2:a3:44
Client Username ................................ N/A
AP MAC Address.................................. 00:18:74:c7:c0:90
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:18:74:c7:c0:9f
Channel......................................... 56
IP Address...................................... 192.168.10.28
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. 5
Client E2E version.............................. No E2E support
Diagnostics Capability.......................... Supported
S69 Capability.................................. Supported
Mirroring....................................... Disabled
QoS Level....................................... Silver
...
```

クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更（CLI）

ネットワーク モビリティ サービス プロトコル（NMSP）によって、Mobility Services Engine とコントローラの間の発信/着信トラフィックに関する通信の管理が行われます。 高い頻度でのロケーション更新を必要とするアプリケーションがある場合は、クライアント、アクティブな RFID タグ、および不正なアクセス ポイント/クライアントの NMSP 通知間隔を 1 ～ 180 秒の範囲内で変更できます。

（注） コントローラと Mobility Services Engine との通信には、TCP ポート 16113 が使用されます。コントローラと Mobility Services Engine の間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開いている（ブロックされていない）ことが必要です。

ステップ 1 次のコマンドを入力して、クライアント、RFID タグ、不正なクライアント/アクセス ポイントの NMSP 通知間隔の値を設定します。*interval* は 1 ～ 180 秒の範囲内の値です。

- **config nmsp notification interval rssi clients** *interval*
- **config nmsp notification interval rssi rfid** *interval*

- **config nmsp notification interval rssi rogues** *interval*

ステップ 2 次のコマンドを入力して、NMSP 通知間隔を表示します。
show nmsp notification interval

以下に類似した情報が表示されます。

```
NMSP Notification Interval Summary

                                RSSI Interval:
 Client.......................................... 2 sec
 RFID............................................ 2 sec
 Rogue AP........................................ 2 sec
 Rogue Client.................................... 2 sec

Spectrum Interval:
 Interferer device............................... 2 sec
```

NMSP 設定の表示（CLI）

NMSP 情報を表示するには、次の CLI コマンドを使用します。

- 次のコマンドを入力して、アクティブな NMSP 接続のステータスを表示します。

  show nmsp status

  以下に類似した情報が表示されます。

```
MSE IP Address    Tx Echo Resp    Rx Echo Req    Tx Data    Rx Data
--------------    ------------    -----------    -------    -------
171.71.132.107           39046          39046             103742          1
```

- 次のコマンドを入力して、NMSP 機能を表示します。

  show nmsp capability

  以下に類似した情報が表示されます。

```
Service                 Subservice
-------                 ----------
RSSI                    Mobile Station, Tags, Rogue,
Spectrum Services       Interferer Devices
Info                    Mobile Station, Rogue,
Statistics              Mobile Station, Tags,
AP Monitor              Subscription
IDS Services            WIPS
```

- 次のコマンドを入力して、NMSP カウンタを表示します。

  show nmsp statistics {**summary** | **connection**}

  値は次のとおりです。

- **summary** を指定すると、一般的な NMSP カウンタが表示されます。
- **connection** を指定すると、その接続固有の NMSP カウンタが表示されます。

show nmsp statistics summary コマンドに対しては、次のような情報が表示されます。

```
NMSP Global Counters

Client Measure Send Fail..................... 0
Send RSSI with no entry...................... 0
APP msg too big.............................. 0
Failed Select on Accept Socket............... 0
Failed SSL write............................. 0
Partial SSL write............................ 0
SSL write returned zero...................... 0
SSL write attempts to want read.............. 0
SSL write attempts to want write............. 0
SSL write got default error.................. 0
SSL write max data length sent............... 0
SSL write max attempts to write in loop...... 0
SSL read returned zero....................... 0
SSL read attempts to want read............... 0
SSL read attempts to want write.............. 0
SSL read got default error................... 0
Failed SSL read - Con Rx buf freed........... 0
Failed SSL read - Con/SSL freed.............. 0
Max records read before exiting SSL read..... 0
Highest Prio Tx Q full....................... 0
Normal Prio Tx Q full........................ 0
Highest Prio Tx Q Sent....................... 0
Normal Prio Tx Q Sent........................ 0
Highest Prio Tx Q count...................... 0
Normal Prio Tx Q count....................... 0
Messages sent by APPs to Highest Prio TxQ.... 0
Max Measure Notify Msg....................... 0
Max Info Notify Msg.......................... 0
Max Highest Prio Tx Q Size................... 0
Max Normal Prio Tx Q Size.................... 0
Max Rx Size.................................. 1
Max Info Notify Q Size....................... 0
Max Client Info Notify Delay................. 0
Max Rogue AP Info Notify Delay............... 0
Max Rogue Client Info Notify Delay........... 0
Max Client Measure Notify Delay.............. 0
Max Tag Measure Notify Delay................. 0
Max Rogue AP Measure Notify Delay............ 0
Max Rogue Client Measure Notify Delay........ 0
Max Client Stats Notify Delay................ 0
Max RFID Stats Notify Delay.................. 0
RFID Measurement Periodic.................... 0
RFID Measurement Immediate................... 0
SSL Handshake failed......................... 0
NMSP Rx detected con failure................. 0
NMSP Tx detected con failure................. 0
NMSP Tx buf size exceeded.................... 0
NMSP Tx Invalid msg id ...................... 0
Reconnect Before Conn Timeout................ 0
Rogue AP Info Changed DB Full................ 0
Rogue AP Meas Changed DB Full................ 0
Rogue Client Info Changed DB Full............ 0
Rogue Client Meas Changed DB Full............ 0
```

show nmsp statistics connection コマンドを入力すると、アクティブな接続のそれぞれについて、次のような情報が表示されます。

```
NMSP Connection Counters

MSE IP: 171.71.132.107
```

```
 Connection status:     UP
 Tx message count                        Rx message count
 ----------------                        ----------------
 WLC Capability:        1                MSE Capability:          0
 Service Subscr Rsp:    1                Service Subscr Req:      1
 Measure Rsp:           0                Measure Req:             0
 Measure Notify:        0
 Info Rsp:              0                Info Req:                0
 Info Notify:           0
 Stats Rsp:             0                Stats Req:               0
 Stats Notify:          0
 Loc Req:               0                Loc Rsp:                 0
 Loc Subscr Req:        0                Loc Subscr Rsp:          0
                                         Loc Notify:              0
 Loc Unsubscr Req:      0                Loc Unsubscr Rsp:        0
 AP Monitor Rsp:        0                AP Monitor Req:          0
 AP Monitor Notify:     64677
 IDS Get Rsp:           0                IDS Get Req:             0
IDS Notif:             0
 IDS Set Rsp:           0                IDS Set Req:             0
```

- 次のコマンドを入力して、コントローラ上のアクティブなモビリティ サービスを表示します。

  show nmsp subscription {**summary** | **detail** | **detail** *ip_addr*}

  値は次のとおりです。

  - **summary** を指定すると、コントローラが加入しているすべてのモビリティ サービスが表示されます。
  - **detail** を指定すると、コントローラが加入しているすべてのモビリティ サービスの詳細が表示されます。
  - **detail** *ip_addr* を指定すると、特定の IP アドレスが加入しているモビリティ サービスだけの詳細が表示されます。

  show nmsp subscription summary コマンドの場合は、次のような情報が表示されます。

```
Mobility Services Subscribed:

 Server IP               Services
 ---------               --------
 1.4.93.31               RSSI, Info, Statistics
```

  show nmsp subscription detail *ip_addr* コマンドの場合は、次のような情報が表示されます。

```
Mobility Services Subscribed by 1.4.93.31

Services                Sub-services
--------                ------------
RSSI                    Mobile Station, Tags,
Info                    Mobile Station,
Statistics             Mobile Station, Tags,
```

- 次のコマンドを入力して、すべての NMSP 統計をクリアします。

  clear nmsp statistics

NMSP のデバッグについて

NMSP 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。

- 次のコマンドを入力して、NMSP デバッグ オプションを設定します。

  debug nmsp *?*

  ここで、*?* は、次のいずれかを示します。

  - **all** {**enable** | **disable**}：すべての NMSP メッセージのデバッグを有効または無効にします。
  - **connection** {**enable** | **disable**}：NMSP 接続イベントのデバッグを有効または無効にします。
  - **detail** {**enable** | **disable**}：NMSP 詳細イベントのデバッグを有効または無効にします。
  - **error** {**enable** | **disable**}：NMSP 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。
  - **event** {**enable** | **disable**}：NMSP イベントのデバッグを有効または無効にします。
  - **message** {**tx** | **rx**} {**enable** | **disable**}：NMSP 送信/受信メッセージのデバッグを有効または無効にします。
  - **packet** {**enable** | **disable**}：NMSP パケット イベントのデバッグを有効または無効にします。

- 次のコマンドを入力して、NMSPインターフェイス イベントのデバッグを有効または無効にします。

  debug dot11 nmsp {**enable** | **disable**}

- 次のコマンドを入力して、IAPP NMSP イベントのデバッグを有効または無効にします。

  debug iapp nmsp {**enable** | **disable**}

- 次のコマンドを入力して、RFID NMSP メッセージのデバッグを有効または無効にします。

  debug rfid nmsp {**enable** | **disable**}

- 次のコマンドを入力して、アクセス ポイント監視NMSPイベントのデバッグを有効または無効にします。

  debug service ap-monitor nmsp {**enable** | **disable**}

- 次のコマンドを入力して、wIPS NMSP イベントのデバッグを有効または無効にします。

  debug wips nmsp {**enable** | **disable**}

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

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

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 5 章

VideoStream の設定

この章の内容は、次のとおりです。

- VideoStream について，219 ページ
- 注意事項および制約事項，219 ページ
- VideoStream の設定，220 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、無線でブロードキャスト フレームをユニキャスト ストリームに変換することで、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。

注意事項および制約事項

- 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。
- コントローラ ソフトウェアのバージョンが一致していないと、最新リリースにコントローラ ソフトウェアをアップグレードする必要があります。
- 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 は、Cisco Aironet 3600、3500、1260、1250、1240AG、1140、1130AG、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

VideoStream（GUI）の設定

ステップ 1 次の手順に従って、マルチキャスト機能を有効にします。

a) [Multicast Direct Feature] チェックボックスをオンにして、マルチキャスト ダイレクト機能を有効にします。 デフォルト値は [disabled] 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 ストリームを再 join する必要があります。

b) [Session Message Config] で [Session announcement State] を選択してセッション アナウンス メカニズムを有効にします。 この機能が有効な場合、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。

c) [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。

d) [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。

e) [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。

f) [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。

g) [Apply] をクリックして、変更を確定します。

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。

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、予想される最大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 リストから次のオプションの 1 つを選択して、リソース予約コントロール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ッション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（オプション）。

a) [Wireless] > [802.11a/n] 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（オプション）。

（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] 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 [disabled] 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] 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。

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 [disabled] 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] 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 [disabled] 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 Phy Rate] フィールドにクライアントへの最低伝送データ レートを入力します。 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%)] フィールド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 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] または [802.11b/g/n] > [Network] の順に選択します。

b) [802.11a/n（または 802.11b/g/n）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 または 802.11b/g 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 6 章

セキュリティ ソリューションの設定

この章では、無線LANのセキュリティ ソリューションについて説明します。 この章の内容は、次のとおりです。

- Cisco Unified Wireless Network Solution セキュリティ，228 ページ
- RADIUS の設定，230 ページ
- TACACS+ の設定，245 ページ
- 最大ローカル データベース エントリの設定，255 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，256 ページ
- パスワード ポリシーの設定，259 ページ
- LDAP の設定，261 ページ
- ローカル EAP の設定，266 ページ
- SpectraLink 社の NetLink 電話用システムの設定，277 ページ
- RADIUS NAC サポートの設定，279 ページ
- 無線による管理機能の使用，282 ページ
- 動的インターフェイスによる管理機能，283 ページ
- DHCP オプション 82 の設定，284 ページ
- アクセス コントロール リストの設定と適用，286 ページ
- 管理フレーム保護の設定，294 ページ
- クライアント除外ポリシーの設定，299 ページ
- Identity ネットワーキングの設定，301 ページ
- AAA Override の設定，305 ページ
- 不正なデバイスの管理，308 ページ
- 不正なアクセス ポイントの分類，315 ページ

- Cisco TrustSec SXP の設定，333 ページ
- Cisco Intrusion Detection System の設定，337 ページ
- IDS シグニチャの設定，341 ページ
- wIPS の設定，352 ページ
- Wi-Fi Direct クライアント ポリシーの設定，360 ページ
- Web 認証プロキシの設定，361 ページ
- 意図的な悪用の検出，364 ページ

Cisco Unified Wireless Network Solution セキュリティ

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。

注意事項および制約事項

Layer 2 Security

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、アカウンティング）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認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、アカウンティング（AAA）サーバで機能します。

RADIUS の設定

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 User Datagram Protocol（UDP; ユーザ データグラム プロトコル）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 で受信アカウンティ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 アカウンティ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 アカウンティング サーバを異なる地域に配置することができます。 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。

注意事項および制約事項

RADIUS サーバのサポート

- RADIUS 認証サーバおよびアカウンティング 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 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

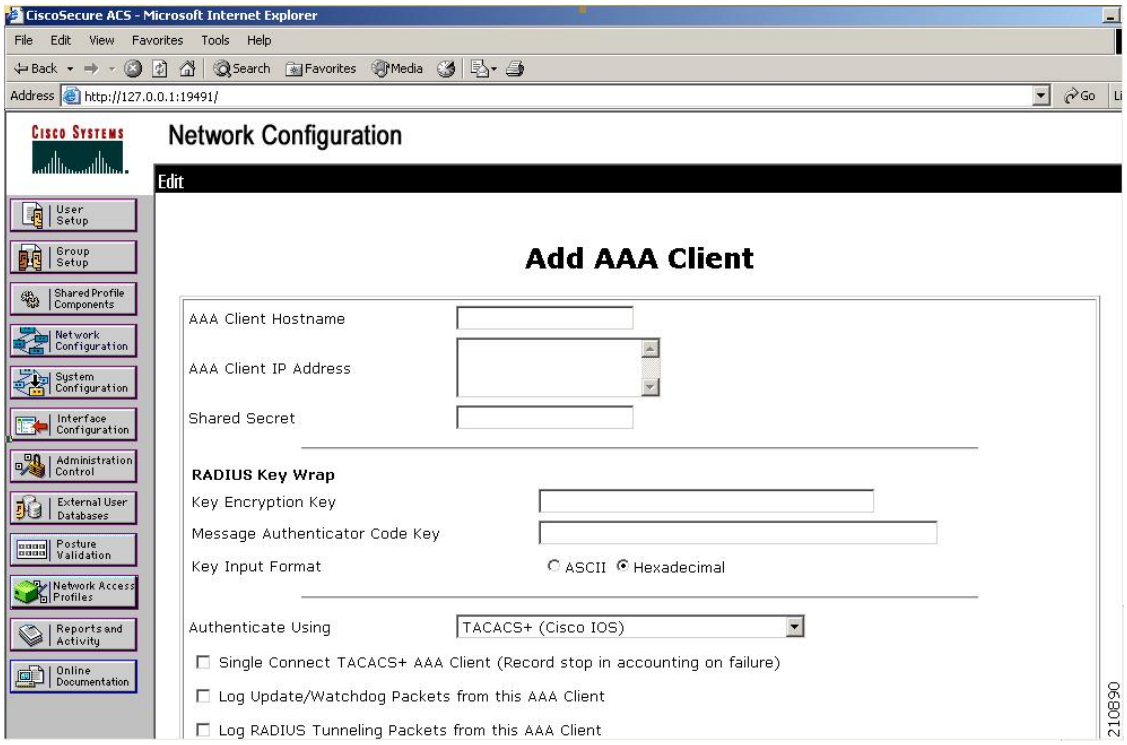
プライマリ RADIUS サーバ（最も低いサーバインデックスを持つサーバ）は、コントローラの最優先サーバであるとみなされます。プライマリ サーバが応答しなくなると、コントローラは、次にアクティブなバックアップ サーバ（低い方から 2 番目のサーバインデックスを持つサーバ）に切り替えます。 コントローラは、プライマリ RADIUS サーバが回復して応答可能になるとそのサーバにフォールバックするように設定されているか、使用可能なバックアップ サーバの中からより優先されるサーバにフォールバックするように設定されていない限り、このバックアップ サーバを引き続き使用します。

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 *26* : *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認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 サーバをアカウンティ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ティング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。

図 *27*：*[RADIUS Authentication Servers]* ページ

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　[Call Station ID Type] ドロップダウン リストから、[IP Address]、[System MAC Address]、または [AP MAC Address] を選択して、送信側の IP アドレス、システム MAC アドレス、または AP 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。

ステップ 4　[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 5　[Apply] をクリックして、変更を確定します。 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 6 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 7 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 8 [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 9 [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 10 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、Key Encryption Key（KEK）または Message Authentication Code Key（MACK）の AES キー ラップ キーを指定します。
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 11 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、アカウンティング用のデフォルト値は 1813 です。

ステップ 12 [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 13 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 14 [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 15 [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（またはアカウンティング）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。

ステップ 16 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 17 [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 18 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す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。 768 ビットは、デフォルト値です。
- [AES CBS]：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、Cipher Block Chaining（CBC; 暗号ブロック連鎖）モードで 128 ビットのデータ パスを使用します。

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。

ステップ 19 [Apply] をクリックして、変更を確定します。

ステップ 20 [Save Configuration] をクリックして、変更を保存します。

ステップ 21 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 22 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。 768 ビットは、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。

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 プロー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] にプローブ間隔値（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 モードでのプロー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 23 [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 24 [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 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。

RADIUS の設定（CLI）

ステップ 1 次のコマンドを入力して、送信側の IP アドレス、システム MAC アドレス、または AP 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 {**ip_address**, **mac_address**, **ap_mac_address**, **ap_macaddr_ssid**}

（注） デフォルトは MAC アドレスです。

（注） IPv6-only クライアントには callStation IdType を使用しないでください。

ステップ 2 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ティング 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）。 768 ビットは、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）。

ステップ 3 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**} *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** {**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。

ステップ 4　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。

ステップ 5 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 6 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。

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、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。

ステップ 9 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 サーバと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。

ステップ 10 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。

ステップ 11 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**}

ステップ 12 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*

アクセス ポイントによって送信される RADIUS 認証属性

この表に RADIUS 認証属性を示します。この認証属性は、Access-Request パケットおよび Access-Accept パケットで Lightweight アクセス ポイントからクライアントに送信されます。

表 *6*：*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

属性 ID	説明
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type[4]
12	Framed-MTU
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 *7* : ***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 *8* : ***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 *9* : ***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 *10* : ***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

属性 ID	説明
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
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name

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 *11*：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

属性 ID	説明
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）
64	Tunnel-Type
65	Tunnel-Medium-Type
81	Tunnel-Group-ID

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 *12*：*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ティング用に予約
15	Failed 用に予約

TACACS+ の設定

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と、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、TACACS+ 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、およびアカウンティング 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。

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。

注意事項および制約事項

- 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 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。

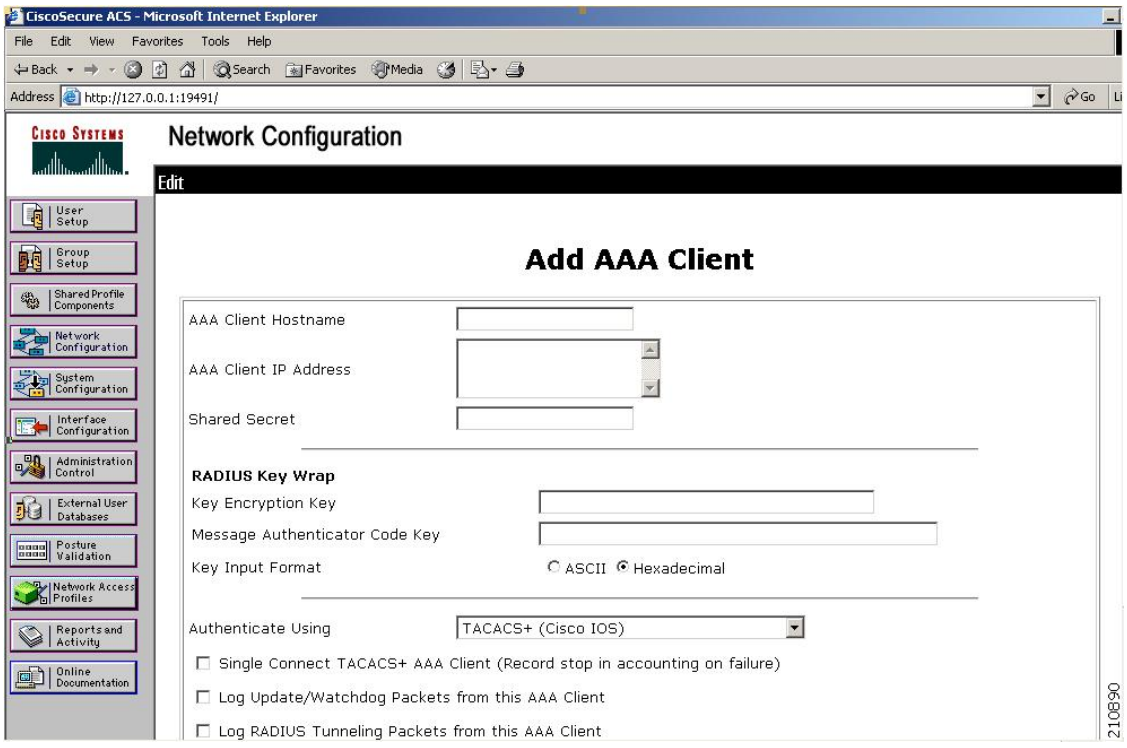
- 再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックしたりする場合には、TACACS+ 認証サーバ、認可サーバ、およびアカウンティング サーバの再送信のタイムアウト値を増やすことをお勧めします。 デフォルトの再送信のタイムアウト値は 2 秒です。この値は最大 30 秒まで増やすことができます。

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 *28*：*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 [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。 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*x*=*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+ サーバを認可用に設定する場合は、[Authorization] を選択します。
- TACACS+ サーバをアカウンティング用に設定する場合、[Accounting] をクリックします。

（注） 認証、許可、アカウンティング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。 アカウンティングの設定は任意です。

[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、または 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。

ステップ 13 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 14 [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 15 [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 16 [Apply] をクリックして、変更を確定します。

ステップ 17 [Save Configuration] をクリックして、変更を保存します。

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+ 認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+ 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

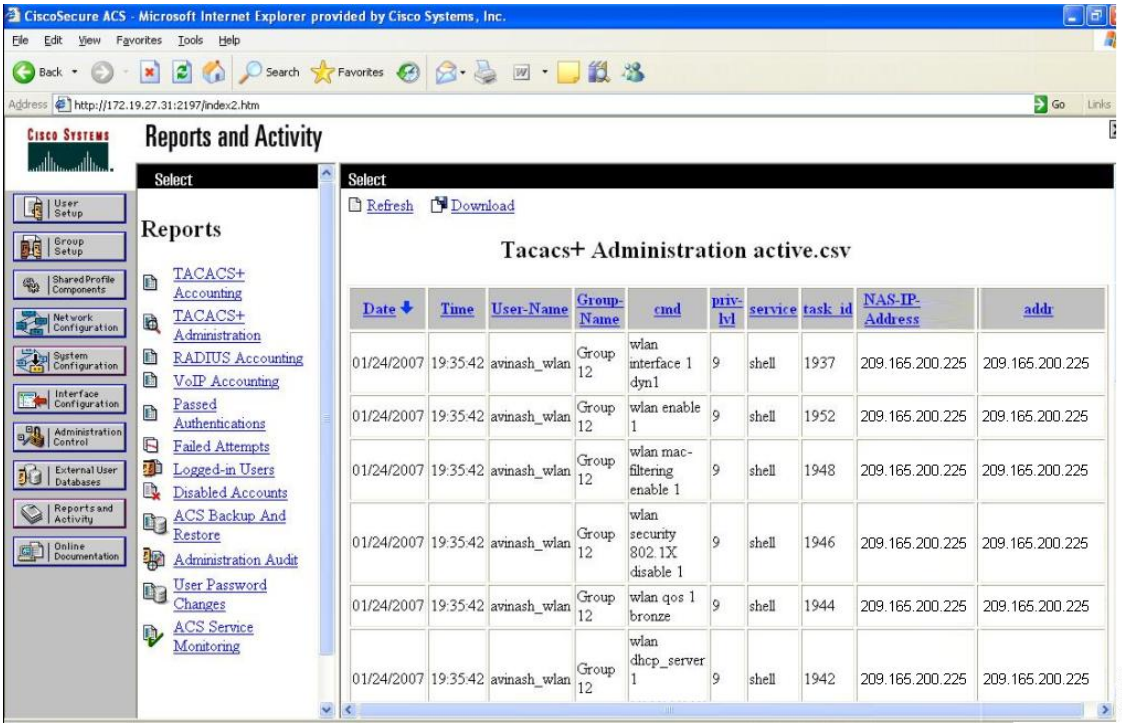
TACACS+ 管理サーバのログの表示

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 *29* : *CiscoSecure ACS* の *[TACACS+ Administration .csv]* ページ



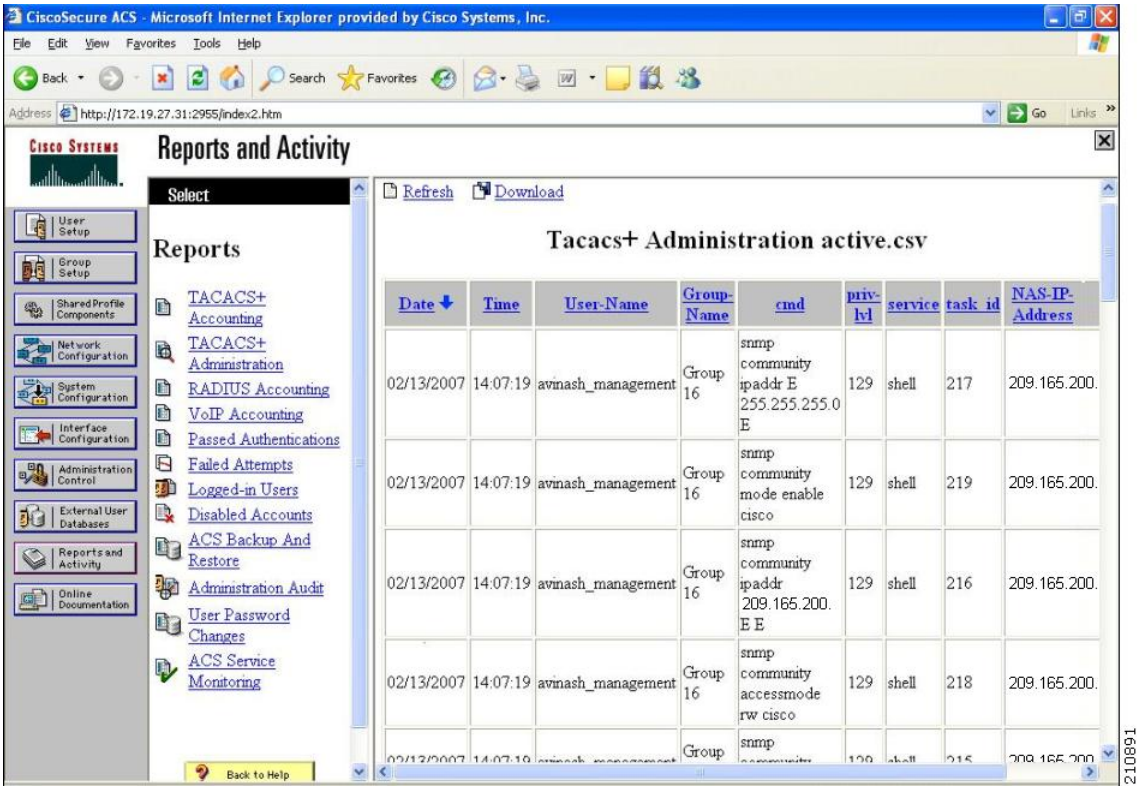
このページは、次の情報を表示します。

- 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、ユーザが **snmp community ipaddr** *ip_address subnet_mask community_name* というコマンドを入力したとします。このとき、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 *30*：*CiscoSecure ACS* の *[TACACS+ Administration .csv]* ページ



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

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 ポイント認可リスト 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

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

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。

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*：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。

- 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

その他の関連資料

ローカル ネットワーク ユーザの設定の詳細については、ローカル EAP の設定，（266 ページ）を参照してください。

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

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）

ステップ 1 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-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アント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。

ステップ 2 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-check ...........Enabled
          consecutive-check ....Enabled
          default-check .......Enabled
          username-check ......Enabled
```

LDAP の設定

この項では、Lightweight Directory Access Protocol（LDAP）サーバを、RADIUS データベースやローカル ユーザ データベースに類似したバックエンド データベースとして設定する方法について説明します。

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。

（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 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 [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 [disabled] です。

ステップ 6 [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 7 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 8 [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、
o=*corporation*.com
または

dc=*corporation*,dc=com

ステップ 9 [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 10 [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 11 [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 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。

ステップ 14 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 15 （オプション）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。

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*： 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 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、認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。
- （オプション）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
```

- **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
```

- **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**}

その他の関連資料

LEAP の設定方法の詳細については、ローカル EAP の設定, （266 ページ）を参照してください。

ローカル EAP の設定

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。

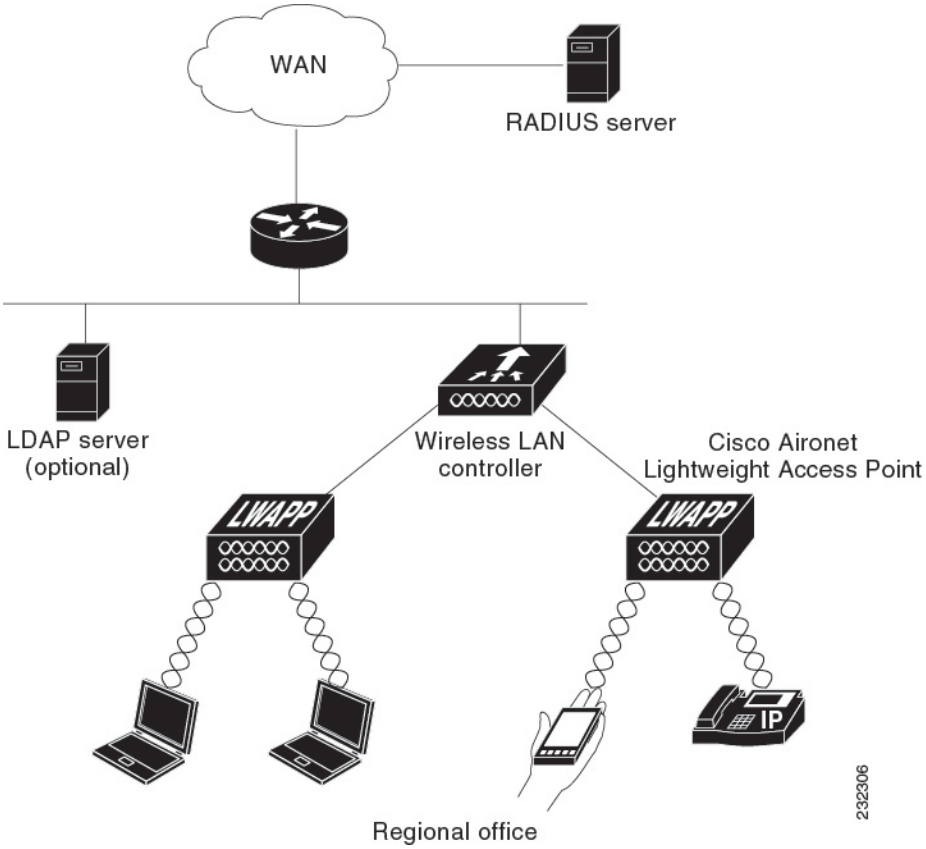
（注） LDAPバックエンドデータベースでは、ローカルEAP方式として、EAP-TLS、EAP-FAST/GTC、および PEAPv1/GTC がサポートされます。 LEAP、EAP-FAST/MSCHAPv2、および PEAPv0/MSCHAPv2 もサポートされていますが、平文のパスワードを返すようにLDAPサーバが設定されている場合にのみサポートされます。

（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 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 番めの 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 番めの RADIUS サーバを試行し、次に 4 番めの 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 *31*：ローカル *EAP* の例



注意事項および制約事項

AP602 OEAP では、EAP プロファイル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。

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) 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。

c) 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。

d) [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。

a) [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。

c) [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。

d) [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。

e) [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。

f) [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。

g) [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。

h) [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。

i) [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。

j) [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。

k) [Apply] をクリックして、変更を確定します。

ステップ 6 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 7 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 8 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) [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。
e) [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。
f) 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。
g) [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。

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、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 7 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 8 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 9 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 10 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 11 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 12 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 .............................. 436973636f000000000000000000000000
     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 13 （オプション）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
```

その他の関連資料

証明書と PAC のインポートの手順については、コントローラ ソフトウェアと設定の管理，（745 ページ）の項を参照してください。

コントローラのローカル ネットワーク ユーザの設定手順については、コントローラでのローカル ネットワーク ユーザの設定，（256 ページ）の項を参照してください。

LDAP の設定手順については、LDAP の設定，（261 ページ）の項を参照してください。

SpectraLink 社の NetLink 電話用システムの設定

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、ここには、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、短いプリアンブルが無効になっていることを示しています。

Enhanced Distributed Channel Access（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。

RADIUS NAC サポートの設定

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（LWA）の場合、コントローラが Web 認証ログイン ページを表示し、ここでユーザ名とパスワードが検証されます。クライアントの資格情報が検証されると、制限付き ACL を使用する ISE サーバと URL がクライアントに送信されます。

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。

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 *13*：*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	Yes	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

注意事項および制約事項

- 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。 RADIUS NAC によるローカル Web 認証を使用している場合は、レイヤ 3 Web 認証も有効にする必要があります。
- ローカル Web 認証では、Web 認証の優先順位を RADIUS として設定しなければなりません。
- 設定されたアカウンティング 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ティング 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、アカウンティング サーバを柔軟に設定できます。 Dot1x 認証を有効に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が検証されます。
- 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 WLAN2 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。

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*

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

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

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

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、ユーザにログオン 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による管理機能の有効化（CLI）

次のコマンドを入力します。

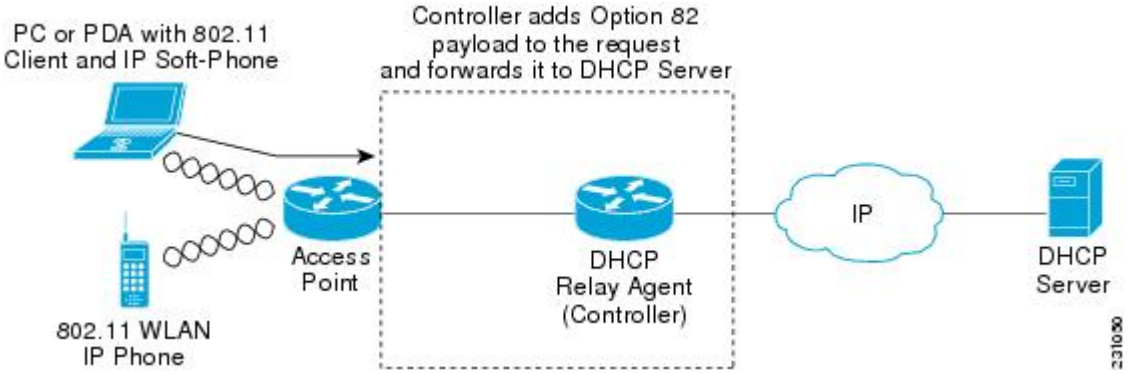
config network mgmt-via-dynamic-interface {enable | disable}

DHCP オプション 82 の設定

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。 具体的には、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 要求にオプション 82 情報を追加してから DHCP サーバに転送するように、コントローラを設定することができます。

図 *32*：*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。

注意事項および制約事項

- 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**

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。
- 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。

```
Interface Name................................. dynamic
MAC Address.................................... e0:5f:b9:46:9f:af
IP Address..................................... 9.4.46.13
IP Netmask..................................... 255.255.255.0
IP Gateway..................................... 9.4.46.1
External NAT IP State.......................... Disabled
External NAT IP Address........................ 0.0.0.0
VLAN........................................... 46
Quarantine-vlan................................ 0
NAS-Identifier................................. test
Active Physical Port........................... LAG (13)
Primary Physical Port.......................... LAG (13)
Backup Physical Port........................... Unconfigured
DHCP Proxy Mode................................ Global
Primary DHCP Server............................ 9.1.0.100
Secondary DHCP Server.......................... Unconfigured
DHCP Option 82................................. Disabled
ACL............................................ Unconfigured
mDNS Profile Name.............................. Unconfigured
AP Manager..................................... No
Guest Interface................................ No
L2 Multicast................................... Enabled
```

その他の関連資料

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。

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

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。

注意事項および制約事項

- 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。
- ACL はコントローラ上で直接設定されるか、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。

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、ネットワーキング 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す。

（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**

以下に類似した情報が表示されます。

```
ACL Counter Status        Enabled
-------------------------------------
ACL Name                   Applied
------------------------ -----------
acl1                          Yes
acl2                          Yes
acl3        Yes
```

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*
以下に類似した情報が表示されます。

```
      Source         Destination           Source Port Dest Port
I Dir  IP Address/Netmask IP Address/Netmask Prot    Range  Range      DSCP  Action Counter
- --- ----------------- ----------------- ---- ----------- -------- ----- ------ -------
1 Any  0.0.0.0/0.0.0.0     0.0.0.0/0.0.0.0     Any       0-65535    0-65535   0     Deny       0
2 In   0.0.0.0/0.0.0.0     200.200.200.0/          6         80-80       0-65535  Any   Permit
0
```

```
        255.255.255.0

DenyCounter :     0
```

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と、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、int 3 というインターフェイス名を作成しようとすると、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。 int 3 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。

- 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

管理フレーム保護の設定

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 はまた、フィッシング インシデントの効果的かつ迅速な検出/報告手段を提供します。

  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。
- 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はネットワーク タイム プロトコル（NTP）で同期化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す。 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 ポイント認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。

注意事項および制約事項

- インフラストラクチャ MFP はグローバル設定です。 旧リリースには、WLAN 向けの MFP インフラストラクチャ保護、および AP 向けの MFP インフラストラクチャ検証を有効または無効にするオプションがありました。 今後、これらのオプションを GUI または CLI で使用することはできません。
- インフラストラクチャ MFP とクライアント MFP の両方がサポートされています。
- 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。
- 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す。
- 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。

a) [WLANs] を選択します。

b) 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。

c) [Advanced] を選択します。 [WLANs > Edit]（[Advanced]）ページが表示されます。

d) [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。

e) [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。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。

- [Infrastructure Protection] フィールドは、インフラストラクチャ MFP が個別の WLAN に対して有効化されているかどうかを示します。
- [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の例は、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。

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）

ステップ 1 [Security] > [Wireless Protection Policies] > [Client Exclusion Policies] の順に選択して、[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。

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
```

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

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。

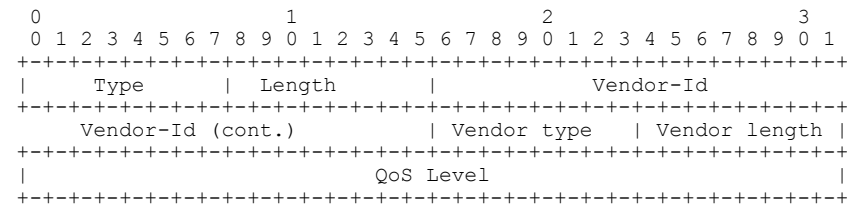
オペレーティング システムのローカル MAC フィルタ データベースは、インターフェイス名を含むように拡張されました。これにより、クライアントを割り当てるインターフェイスをローカル MAC フィルタで指定できるようになりました。 別の RADIUS サーバも使用できますが、その RADIUS サーバは [Security] メニューを使用して定義する必要があります。

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。

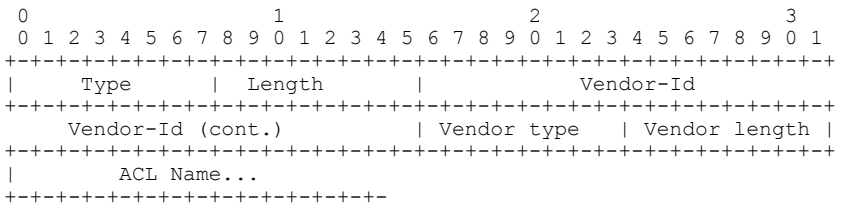
この属性は、スイッチング ファブリック内、および無線経由のモバイル クライアントのトラフィックに適用される QoS レベルを示しています。 この例は、QoS-Level 属性フォーマットの要約を示しています。 テキスト ボックスは左から右に伝送されます。



- 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：
  - 0 – Bronze（バックグラウンド）
  - 1 - Silver（ベストエフォート）
  - 2 – Gold（ビデオ）
  - 3 – Platinum（音声）

ACL-Name

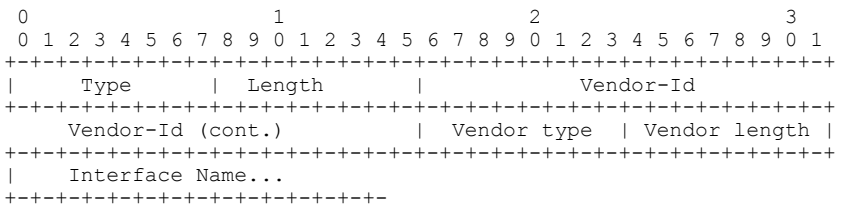
この属性は、クライアントに適用される ACL 名を示します。 ACL-Name 属性形式の要約を次に示します。 テキスト ボックスは左から右に伝送されます。



- 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。



- 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

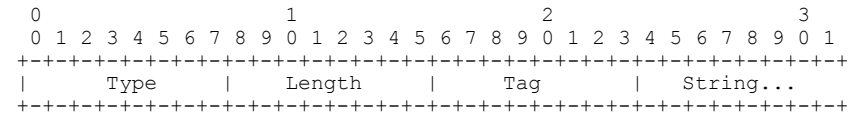
（注） この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

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。



- Type – 81（Tunnel-Private-Group-ID 用）
- Length – >= 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）この属性が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、アカウンティング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プ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、サプ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ときは、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、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。

AAA Override の設定

AAA Override について

WLAN の Allow 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、QoS、および ACL を適用できます。

注意事項および制約事項

- 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。
- 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。

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] タブを選択して、[WLANs > Edit]（[Advanced]）ページを開きます。

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 [disabled] 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。

AAA Override の設定（CLI）

config wlan aaa-override {**enable** | **disable**} *wlan_id*

wlan_id には、1 ～ 16 の ID を入力します。

不正なデバイスの管理

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 Clear To Send（CTS; クリア ツー センド）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この CTS フレームが送信され、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 セキュリティ侵犯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。

不正なデバイスの検出

コントローラは、すべての近隣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およびクライアントに関する情報を自動的に検出して収集します。 コントローラで不正なアクセス ポイントが検出されると、Rogue Location Discovery Protocol（RLDP; 不正ロケーション検出プロトコル）を使用して、不正なアクセス ポイントがネットワークに接続されているかどうかが判定されます。

コントローラは、すべてのアクセスポイント上で、またはmonitor（リッスン専用）モードに設定されたアクセス ポイント上のみ、のいずれかでRLDPを使用できるように設定できます。 この後者のオプションでは、輻輳している RF 空間での不正なアクセス ポイントを簡単に自動検出できるようになります。そして、不要な干渉を生じさせたり、通常のデータ アクセスポイント機能に影響を与えたりすることなく、モニタリングを行えるようになります。 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、コントローラでは常にRLDP動作に対してモニタ アクセス ポイントが選択されます。 ネットワーク上に不正があるとRLDPで判断された場合は、検出された不正を手動で封じ込め処理を行うことも、自動的に封じ込め処理を行うこともできます。

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。

不正阻止の操作は、次の 2 通りの方法で実行されます。

- 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 ポイントを阻止するために、この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。

個々の不正阻止フレームには、一連のユニキャスト アソシエーション解除および認証解除フレームの送信が含まれます。

注意事項および制約事項

- 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ネル 157 または 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。

- ローカルおよび FlexConnect モードのアクセスポイントは、アソシエートされたクライアントに対して機能するように設計されており、オフチャネルのスキャンに費やす時間は比較的短くなります。アクセス ポイントが各チャネル上で費やす時間は約 50 ミリ秒です。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 または 60 秒などに短縮して、無線がオフチャ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 ポイントが各チャネル上で費やす時間は約 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（モニタ モード アクセス ポイントの場合、無線チャネルごとに 6 台）に制限します。
- RLDP は、オープン認証用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 BSSID を使用する不正アクセス ポイント（ビーコンで SSID を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 ポイントだけを検出します。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 チャネルのモニタ モードであるときには機能します。
- 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、コントローラからそのメッシュ AP のアソシエーションは解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。

WCS の相互作用と不正の検出

WCS ソフトウェア リリース 5.0 以降でも、ルール ベースの分類がサポートされています。WCS では、コントローラ上で設定された分類ルールが使用されます。次のイベント後に、コントローラから WCS にトラップが送信されます。

- 最初に不明なアクセス ポイントが Friendly に移動した場合に、不正の状態が Alert であると、コントローラから WCS にトラップが送信されます。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移動した場合、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 WCS 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 必要なアクセス 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）。 ただしコントローラ ソフトウェア リリース 6.0 以降では、[All APs > Details for]（[Advanced]）ページで [Rogue Detection] チェックボックスを選択または選択解除すると、個々のアクセス ポイントに対して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] を選択して、[Rogue Policies] ページを開きます。

ステップ 3 [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 ポイント上で RLDP を無効にします。 768 ビットは、デフォルト値です。
- [All APs]：すべてのアクセス ポイント上で RLDP を有効にします。
- [Monitor Mode APs]：モニタ モードのアクセス ポイント上でのみ RLDP を有効にします。

ステップ 4 [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 5 必要に応じて、[Validate Rogue Clients Against AAA] チェックボックスをオンにし、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かどうかを検証します。 デフォルト値はオフです。

ステップ 6 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、アドホック不正の検出および報告を有効にします。 デフォルト値はオンです。

ステップ 7 [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 8 [Rogue Detection Minimum RSSI] テキスト ボックスに、不正に必要な最小 RSSI 値を入力します。これは、AP が不正を検出し、コントローラで不正エントリが作成されるために必要な値です。 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 9 [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。 これによって、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。この機能は、モニタ モードの AP のみに適用されます。

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
- 一時的な不正エントリをコントローラで回避できる
- 一時的な不正への不要なメモリ割り当てを回避できる

ステップ 10 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、次のチェックボックスをオンにします。それ以外の場合は、これらのチェックボックスをオフ（デフォルト値）のままにしておきます。

注意 次のパラメータのいずれかを有効にすると、「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。

- [Auto Containment Level]：ドロップダウン リストから値を選択して、自動阻止レベルを設定します。デフォルトは 1 です。
- [Auto Containment only for monitor mode APs]：監視モードのアクセス ポイントだけを自動阻止に使用したい場合、このチェックボックスをオンにします。
- [Rogue on Wire]：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。
- [Using Our SSID]：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。 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。 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 ネットワークを自動的に阻止します。 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 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。

不正検出の設定（CLI）

ステップ 1 必要なアクセス 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）。ただしコントローラ ソフトウェア リリース 6.0 以降では、次のコマンドを入力すると、個々のアクセス ポイントに対して不正の検出を有効または無効にできます。
config rogue detection {**enable** | **disable**} *Cisco_AP command.*

（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、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 ポイントに対して 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 ポイントに対してのみ 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 ポイントに対して RLDP を無効にします。

ステップ 3 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 の有効な値の範囲は 240 ～ 3600 秒（両端の値を含む）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 4 次のコマンドを入力して、アドホック不正の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 5 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 6 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 パラメータの有効範囲は 10 ～ 300 秒で、デフォルト値は 10 秒です。

（注） この機能は、モニタ モードの AP のみに適用されます。

ステップ 7 次のコマンドを入力して、不正に必要な最小RSSI値を指定します。これは、APが不正を検出し、コントローラで不正エントリが作成されるために必要な値です。
config rogue detection min-rssi *rssi in dBm*

rssi in dBm パラメータの有効範囲は –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 8 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 パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。

（注） この機能は、監視モードの AP のみに適用されます。

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
- 一時的な不正エントリをコントローラで回避できる
- 一時的な不正への不要なメモリ割り当てを回避できる

ステップ 9 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 次のコマンドのいずれかを入力すると、「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 alart** コマンドを入力します。

- **configure rogue auto-containment level {1 - 4}**：1 ～ 4 の値を入力して、自動阻止レベルを設定します。デフォルトは 1 です。
- **config rogue auto-contain level 1** *monitor_mode_ap_only*：監視モードのアクセス ポイントだけを自動的に阻止します。

ステップ 10 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**：特定の曜日に RLDP をスケジュールします。 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

  （注） RLDP スケジュールを設定すると、それ以降、つまり設定が保存されたあと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 11 次のコマンドを入力して、変更を保存します。
save config

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

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、または Unclassified に分類して表示するルールを作成できます。

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、未分類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、およびUnclassified）にそのルールが適用されます。

（注） ルール ベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。

（注） 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。

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るようになります。
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 *14*：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	• Internal：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Friendly、Internal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。 • External：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Friendly、External 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。 • Alert：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 Alert に移動されます。
Malicious	• Alert：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 Alert に移動されます。 • Threat：未知（管理対象外）のアクセスポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：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。 • Contained Pending：未知（管理対象外）のアクセス ポイントが Contained 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。

ルールベースの分類タイプ	不正の状態
Unclassified	• Pending：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 Pending 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が判定されます。 • Alert：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 Alert に移動されます。 • Contained：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。 • Contained Pending：未知（管理対象外）のアクセス ポイントが Contained 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。

コントローラ ソフトウェア リリース 5.0 以降にアップグレードした場合、不正なアクセス ポイントの分類と状態は次のように再設定されます。

- Known から Friendly、Internal
- Acknowledged から Friendly、External
- Contained から Malicious、Contained

前述のように、コントローラでは、ユーザ定義のルールに基づいて未知（管理対象外）のアクセス ポイントの分類タイプと不正の状態が自動的に変更されます。もしくは、未知（管理対象外）のアクセス ポイントを本来とは異なる分類タイプと不正の状態に手動で変更することができます。

表 *15*：設定可能な分類タイプ/不正の状態の推移

From	To
Friendly（Internal、External、Alert）	Malicious（Alert）
Friendly（Internal、External、Alert）	Unclassified（Alert）
Friendly（Alert）	Friendly（Internal、External）
Malicious（Alert、Threat）	Friendly（Internal、External）
Malicious（Contained、Contained Pending）	Malicious（Alert）
Unclassified（Alert、Threat）	Friendly（Internal、External）

From	To
Unclassified（Contained、Contained Pending）	Unclassified（Alert）
Unclassified（Alert）	Malicious（Alert）

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。

a) [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。
b) [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。 名前にはスペースを含めないでください。
c) [Rule Type] ドロップダウン リストから [Friendly] または [Malicious] を選択して、このルールと一致する不正なアクセス ポイントを Friendly または Malicious に分類します。
d) [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 リストから [Friendly] または [Malicious] を選択して、このルールと一致する不正なアクセス ポイントを Friendly または Malicious に分類します。
c) [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。 768 ビットは、デフォルト値です。

d) 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。

e) [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） WCS では、このオプションを「オープン認証」と呼びます。

- [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ので、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。

f) [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 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] をクリックして、変更を確定します。

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。 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

[Friendly Rogue APs] ページ、[Malicious Rogue APs] ページ、および [Unclassified Rogue APs] ページには、不正なアクセス ポイントの MAC アドレスと SSID、チャネル番号、不正なアクセス ポイントに接続されたクライアントの数、不正なアクセス ポイントが検出された無線の数、および不正なアクセス ポイントの現在のステータスなどの情報が表示されます。

（注） データベースから既知の不正を削除するには、WLC UI へ移動して不正の状態を [Alert Unknown] に変更し、[Save Configuration] をクリックします。 その不正が存在しなくなると、20 分後にデータベースから消去されます。

（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、削除対象に該当するチェックボックスをオンにし、[Remove Selected] をクリックします。

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。未分類のアクセス 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。

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 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 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] をクリックして、変更を保存します。

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。

ステップ 18 [Apply] をクリックして、変更を確定します。

ステップ 19 [Save Configuration] をクリックして、変更を保存します。

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、WCS ユーザが WCS マップに手動で追加し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、WCS 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 WCS にトラップを送信します。 WCS は、Autonomous アクセス ポイント リストでこのアクセス ポイントを発見すると、このアクセス ポイントを不正無視リストに追加するようコントローラにコマンドを送信します。 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 WCS から Autonomous アクセス ポイントを削除すると、WCS はこのアクセス ポイントを不正無視リストから削除するようにコントローラにコマンドを送信します。

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*
後からこのルールの優先順位を変更し、それに伴ってリスト内の他のルールの順番を変更する場合は、**config rogue rule priority** *priority rule_name* コマンドを入力します。 後から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、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 3 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*

ステップ 4 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*

- **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。
- **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、{**all** | *condition_type} condition_value rule_name* コマンドを入力します。

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 6 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 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、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
以下に類似した情報が表示されます。

```
Priority Rule Name   State         Type             Match   Hit Count
-------- ----------- --------  ------------ ------ ---------
1        Rule1           Disabled     Friendly      Any   0
2        Rule2           Enabled      Malicious     Any   339
3        Rule3           Disabled     Friendly      Any   0
```

ステップ 9 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*

以下に類似した情報が表示されます。

```
Priority..................................... 2
Rule Name.................................... Rule2
State........................................ Enabled
Type......................................... Malicious
Match Operation.............................. Any
Hit Count.................................... 352
Total Conditions............................. 6
Condition 1
    type..................................... Client-count
    value.................................... 10
Condition 2
    type..................................... Duration
    value (seconds).......................... 2000
Condition 3
    type..................................... Managed-ssid
    value.................................... Enabled
Condition 4
    type..................................... No-encryption
    value.................................... Enabled
Condition 5
    type..................................... Rssi
    value (dBm).............................. -50
Condition 6
    type..................................... Ssid
    SSID Count............................... 1
    SSID 1................................... test
```

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
  以下に類似した情報が表示されます。

```
Rogue Location Discovery Protocol..... Enabled
Rogue AP timeout..... 1200

MAC Address        Classification     # APs  # Clients  Last Heard
-----------------  ------------------ -----  ---------  ----------------------
00:0a:b8:7f:08:c0  Friendly           0      0          Not Heard
00:0b:85:01:30:3f  Malicious          1      0          Fri Nov 30 11:30:59 2007
00:0b:85:63:70:6f  Malicious          1      0          Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf  Malicious                 1      0     Fri Nov 30 11:23:12 2007
...
```

- 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

  以下に類似した情報が表示されます。

```
Number of APs..... 1

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- --------------------------
00:0a:b8:7f:08:c0  Internal           1      0               Tue Nov 27 13:52:04 2007
```

- 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

  以下に類似した情報が表示されます。

```
Number of APs..... 264

MAC Address        State              # APs # Clients Last Heard
-----------------  ------------------ ----- --------- ----------------------
00:0b:85:01:30:3f  Alert              1     0         Fri Nov 30 11:20:01 2007
00:0b:85:63:70:6f  Alert              1     0         Fri Nov 30 11:20:14 2007
00:0b:85:63:cd:bf  Alert              1     0         Fri Nov 30 11:23:12 2007
00:0b:85:63:cd:dd  Alert              1     0         Fri Nov 30 11:27:03 2007
00:0b:85:63:cd:de  Alert              1     0         Fri Nov 30 11:26:23 2007
00:0b:85:63:cd:df  Alert                 1   0     Fri Nov 30 11:26:50 2007
...
```

- 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

  以下に類似した情報が表示されます。

```
Number of APs.................................. 164

MAC Address        State              # APs # Clients Last Heard
-----------------  -----------------  ----- --------- -----------------------
00:0b:85:63:cd:bd  Alert              1   0         Fri Nov 30 11:12:52 2007
00:0b:85:63:cd:e7  Alert              1   0         Fri Nov 30 11:29:01 2007
00:0b:85:63:ce:05  Alert              1   0         Fri Nov 30 11:26:23 2007
00:0b:85:63:ce:07 Alert                 1    0    Fri Nov 30 11:26:23 2007
...
```

- 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*

  以下に類似した情報が表示されます。

```
Rogue BSSID.................................... 00:1d:70:59:95:9d
Rogue Radio Type............................... 802.11a
State.......................................... Alert
First Time Rogue was Reported.................. Tue Sep 21 09:57:08 2010
Last Time Rogue was Reported................... Tue Sep 21 10:00:56 2010
Rogue Client IP address........................ Not known
Reported By
    AP 1
        MAC Address............................ 68:ef:bd:e1:fd:30
        Name................................... AP5475.d074.48e4
        RSSI................................... -80 dBm
        SNR.................................... 18 dB
        Channel................................ 40
        Last reported by this AP............... Tue Sep 21 10:00:56 2010
```

- 次のコマンドを入力して、特定の802.11a/n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*

  以下に類似した情報が表示されます。

```
Number Of Slots................................ 2
AP Name........................................ AP2
MAC Address.................................... 00:1b:d5:13:39:74
  Radio Type................................... RADIO_TYPE_80211a
  Noise Information
    Noise Profile.............................. PASSED
    Channel 36.................................  -80 dBm
    Channel 40.................................  -78 dBm
    ...
  Interference Information
    Interference Profile....................... PASSED
```

```
    Channel 36.................................  -81 dBm @  8 % busy
    Channel 40.................................  -66 dBm @  4 % busy
   ...
Rogue Histogram (20/40_ABOVE/40_BELOW)
 Channel 36................................. 21/ 1/ 0
    Channel 40.................................  7/ 0/ 0
    ...
```

- 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*

  以下に類似した情報が表示されます。

```
MAC Address         State               # APs      Last Heard
-----------------  ------------------ ----- -------------------------
00:bb:cd:12:ab:ff     Alert      1  Fri Nov 30 11:26:23 2007
```

- 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

  以下に類似した情報が表示されます。

```
Validate rogue clients against AAA.............. Disabled

MAC Address        State              # APs Last Heard
-----------------  ------------------ ----- ----------------------
00:0a:8a:7d:f5:f5  Alert              1     Mon Dec  3 21:56:36 2007
00:18:ba:78:c4:44  Alert              1     Mon Dec  3 21:59:36 2007
00:18:ba:78:c4:d1  Alert              1     Mon Dec  3 21:47:36 2007
00:18:ba:78:ca:f8  Alert                 1    Mon Dec  3 22:02:36 2007
...
```

- 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*

  以下に類似した情報が表示されます。

```
Rogue BSSID..................................... 00:0b:85:23:ea:d1
State........................................... Alert
First Time Rogue was Reported................... Mon Dec  3 21:50:36 2007
Last Time Rogue was Reported.................... Mon Dec  3 21:50:36 2007
Rogue Client IP address......................... Not known
Reported By
    AP 1
        MAC Address............................. 00:15:c7:82:b6:b0
        Name.................................... AP0016.47b2.31ea
        Radio Type.............................. 802.11a
        RSSI.................................... -71 dBm
        SNR..................................... 23 dB
        Channel................................. 149
```

```
        Last reported by this AP..... Mon Dec  3 21:50:36 2007
```

- 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

  以下に類似した情報が表示されます。

```
Detect and report Ad-Hoc Networks..... Enabled

Client MAC Address  Adhoc BSSID         State          # APs    Last Heard
------------------  ------------------  ----------- -------  ------------------------
00:bb:cd:12:ab:ff     super     Alert    1   Fri Nov 30 11:26:23 2007
```

- 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*

  以下に類似した情報が表示されます。

```
Adhoc Rogue MAC address..... 02:61:ce:8e:a8:8c
Adhoc Rogue BSSID..... 02:61:ce:8e:a8:8c
State..... Alert
First Time Adhoc Rogue was Reported..... Tue Dec 11 20:45:45 2007
Last Time Adhoc Rogue was Reported..... Tue Dec 11 20:45:45 2007
Reported By
    AP 1
        MAC Address..... 00:14:1b:58:4a:e0
        Name..... AP0014.1ced.2a60
        Radio Type..... 802.11b
        SSID..... rf4k3ap
        Channel..... 3
        RSSI..... -56 dBm
        SNR..... 15 dB
        Encryption..... Disabled
        ShortPreamble..... Disabled
        WPA Support..... Disabled
  Last reported by this AP..... Tue Dec 11 20:45:45 2007
```

- 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

  以下に類似した情報が表示されます。

```
MAC Address
------------------
10:bb:17:cc:01:ef
```

（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）」のステップ *20* 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。
- 次のコマンドを入力して、変更を保存します。
  save config

Cisco TrustSec SXP の設定

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、およびレポーティング 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 ボーダレス 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 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。

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。

注意事項および制約事項

- 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。
- コントローラは常にスピーカー モードで動作します。
- 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。
- 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。
- 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。

- 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

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 Cisco TrustSec SXP を有効にするには、[SXP State] ドロップダウン リストから [Enabled] を選択します。

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] をクリックして、変更を確定します。

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
```

Cisco Intrusion Detection System の設定

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 IDS センサーをリストに追加するには、[New] をクリックします。 [CIDS Sensor Add] ページか表示されます。

ステップ 3 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。 [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。

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 HTTPS ポートの番号を設定します。 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 [disabled] 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] をクリックして、変更を保存します。

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。

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 （オプション）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 [disabled] 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。 そのあと、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

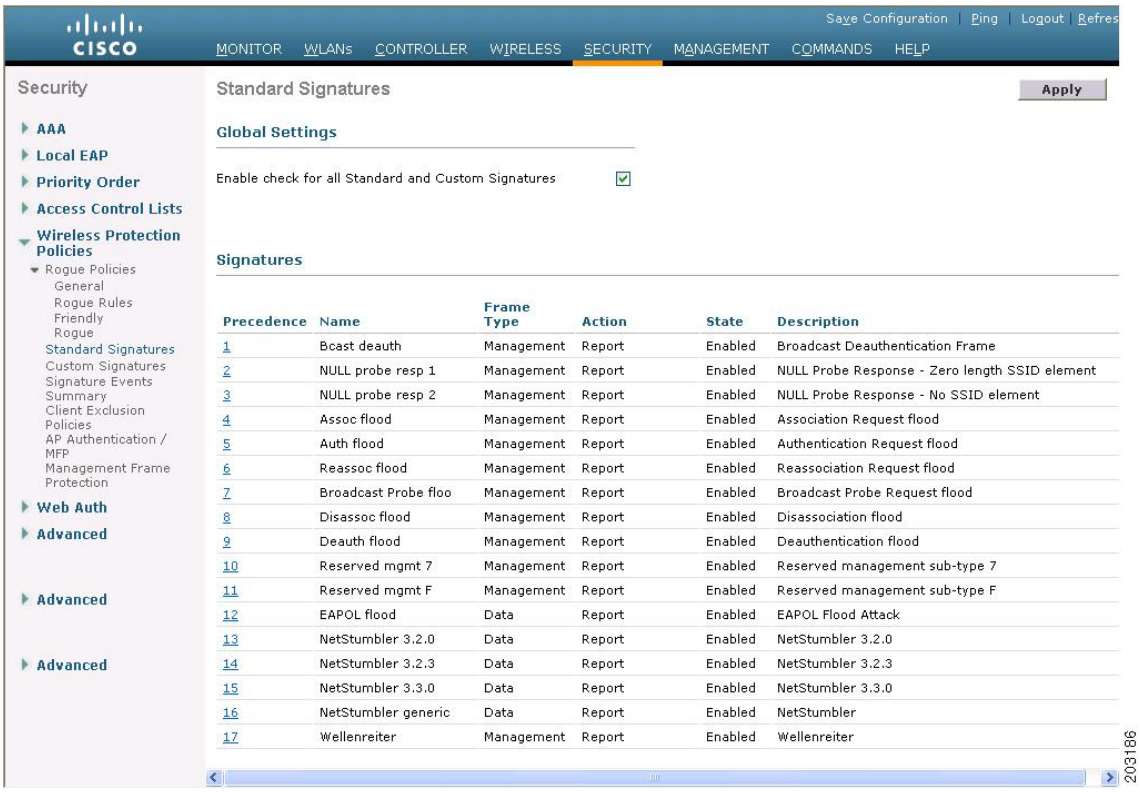
IDS シグニチャの設定

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。

[Standard Signatures] ページに示すように、シスコではコントローラ上で 17 の標準シグニチャをサポートしています。

図 *33*：*[Standard Signatures]* ページ



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認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 プローブ応答シグニチャ**：NULL プロー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 プロー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 プロー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 プロー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）

- **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。 コントローラではトラップが生成され、WCS に転送されます。

  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 サーバと WCS 内蔵 TFTP 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 サーバは Cisco WCS と同じコンピュータ上で実行できません。

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 秒当たりの一致パケットの数
- 攻撃が検出されたチャネル上のアクセス 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）にするには、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

  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
```

（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

  以下に類似した情報が表示されます。

```
Signature-ID..................................... 1
Precedence....................................... 1
Signature Name................................... Bcast deauth
Type............................................. standard
FrameType........................................ management
State............................................ enabled
Action........................................... report
Tracking......................................... per Signature and Mac
Signature Frequency.............................. 50 pkts/interval
Signature Mac Frequency.......................... 30 pkts/interval
Interval......................................... 1 sec
Quiet Time....................................... 300 sec
Description...................................... Broadcast Deauthentication Frame
Patterns:
                0(Header):0x00c0:0x00ff
       4(Header):0x01:0x01
```

- 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

  以下に類似した情報が表示されます。

```
Precedence Signature Name            Type      # Events
---------- ------------------    -----      -----------
1    Bcast deauth         Standard     2
2    NULL probe resp 1   Standard        1
```

- 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

  以下に類似した情報が表示されます。

```
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type........................................... Standard
Number of active events..................... 2
```

```
Source MAC Addr      Track Method     Frequency   No. APs  Last Heard
-----------------  ------------    --------- -------- ------------------------
00:01:02:03:04:01  Per Signature      4                3   Tue Dec 6 00:17:44 2005
00:01:02:03:04:01  Per Mac               6     2   Tue Dec 6 00:30:04 2005
```

- 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

  以下に類似した情報が表示されます。

```
Source MAC..................................... 00:01:02:03:04:01
Precedence..................................... 1
Signature Name................................. Bcast deauth
Type........................................... Standard
Track.......................................... Per Mac
Frequency...................................... 6
Reported By
 AP 1
  MAC Address.............................. 00:0b:85:01:4d:80
  Name..................................... Test_AP_1
  Radio Type............................... 802.11bg
  Channel.................................. 4
  Last reported by this AP................. Tue Dec 6 00:17:49 2005
 AP 2
  MAC Address.............................. 00:0b:85:26:91:52
  Name..................................... Test_AP_2
  Radio Type............................... 802.11bg
  Channel.................................. 6
  Last reported by this AP................. Tue Dec 6 00:30:04 2005
```

wIPS の設定

wIPS について

シスコの適応型 Wireless Intrusion Prevention System（wIPS）は、無線の脅威の検出およびパフォーマンスの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。 シスコの適応型 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。

シスコの適応型 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ートが解除され、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（Enhanced Local Mode）アクセス ポイント、または単に 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

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ネルを監視し、そのチャ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。

表 *16*：*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 アソシエーション	bsnDot11StationAssociate
	802.11 ディスアソシエーション	bsnDot11StationDisassociate
	802.11 認証解除	bsnDot11StationDeauthenticate
	802.11 認証失敗	bsnDot11StationAuthenticateFail
	802.11 アソシエーション失敗	bsnDot11StationAssociateFail
	Exclusion	bsnDot11StationBlacklisted

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
自動 RF プロファイル トラップ	Load Profile	bsnAPLoadProfileFailed
	Noise Profile	bsnAPNoiseProfileFailed
	Interference Profile	bsnAPInterferenceProfileFailed
	Coverage Profile	bsnAPCoverageProfileFailed
自動 RF 更新トラップ	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

（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。 それらのトラップはそれほど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。 したがって、コントローラで生成される上記以外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。

注意事項および制約事項

- リリース 7.0.116.0 以降では、標準のローカル モードまたは FlexConnect モードのアクセス ポイントが拡張され、Wireless Intrusion Prevention System（wIPS）機能のサブセットが装備されています。 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 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。

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ネルのみ
- DCA：動的チャネル割り当て（DCA）アルゴリズムによって使用されるチャネルセットのみ（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*
  以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 3
Cisco AP Name.................................... AP1131:46f2.98ac
...
AP Mode ......................................... Monitor
Public Safety ................................... Disabled  Disabled
AP SubMode ...................................... WIPS
```

...

- 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ネル スキャンを表示します。
  show ap monitor-mode summary
  以下に類似した情報が表示されます。

```
AP Name           Ethernet MAC           Status           Scanning Channel List
-----------------  -------------------- ----------  ------------------------
AP1131:46f2.98ac       00:16:46:f2:98:ac          wIPS              1, 6, NA, NA
```

- 次のコマンドを入力して、WCS から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
  以下に類似した情報が表示されます。

```
Policy Name.............. Default
Policy Version.......... 3
```

- 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
  以下に類似した情報が表示されます。

```
Policy Assignment Requests............ 1
Policy Assignment Responses........... 1
Policy Update Requests................ 0
Policy Update Responses............... 0
Policy Delete Requests................ 0
Policy Delete Responses............... 0
Alarm Updates......................... 13572
Device Updates........................ 8376
Device Update Requests................ 0
Device Update Responses............... 0
Forensic Updates...................... 1001
Invalid WIPS Payloads................. 0
Invalid Messages Received............. 0
NMSP Transmitted Packets.............. 22950
NMSP Transmit Packets Dropped......... 0
NMSP Largest Packet................... 1377
```

- 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

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

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。

注意事項および制約事項

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）

- 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うには、次のコマンドを使用します。
  - **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

Web 認証プロキシの設定

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 リダイレクト ポートは、CPU ACL では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。なぜなら、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 ブラウザには、次の 3 種類のインターネット設定をユーザが指定できます。

- 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。ブラウザでこの設定が有効になると、ワイヤレス クライアントは設定されたポートで宛先プロキシ サーバの IP 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。 ユーザは事実上、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 クライアントが Web 認証された WLAN ネットワークに入った場合、そのクライアントは 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と、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（JavaScipt 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] メニューから [Enabled] を選択して、Web 認証プロキシを有効にします。

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、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。
- Web 認証プロキシ設定の現在のステータスを表示するには、次のいずれかのコマンドを入力します。
  - **show network summary**
  - **show running-config**

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 7 章

WLAN の使用

この章の内容は、次のとおりです。

- WLAN について，366 ページ
- 注意事項および制約事項，366 ページ
- WLAN の作成，369 ページ
- WLAN の検索（GUI），372 ページ
- WLAN ごとのクライアント カウントの設定，372 ページ
- DHCP の設定，374 ページ
- DHCP スコープの設定，379 ページ
- WLAN の MAC フィルタリングの設定，382 ページ
- ローカル MAC フィルタの設定，382 ページ
- 無効なクライアントのタイムアウトの設定，383 ページ
- インターフェイスへの WLAN の割り当て，384 ページ
- DTIM period の設定，384 ページ
- ピアツーピア ブロッキングの設定，387 ページ
- レイヤ 2 セキュリティの設定，390 ページ
- Static WEP と Dynamic WEP の両方をサポートする WLAN の設定，397 ページ
- Sticky PMKID キャッシュの設定，401 ページ
- CKIP の設定，403 ページ
- セッション タイムアウトの設定，406 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，408 ページ
- Web 認証を使用したレイヤ 3 セキュリティの設定，409 ページ

- キャプティブ バイパスの設定，412 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，413 ページ
- WLAN への QoS プロファイルの割り当て，415 ページ
- QoS Enhanced BSS の設定，418 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，422 ページ
- Key Telephone System-Based CAC の設定，427 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，430 ページ
- シームレスな IPv6 モビリティの設定，432 ページ
- Cisco Client Extensions の設定，437 ページ
- リモート LAN の設定，439 ページ
- AP グループの設定，441 ページ
- RF プロファイルの設定，448 ページ
- 802.1X 認証を使用した Web リダイレクトの設定，455 ページ
- NAC アウトオブバンド統合の設定，460 ページ
- パッシブ クライアントの設定，465 ページ
- クライアント プロファイルの設定，469 ページ
- WLAN ごとの RADIUS 送信元サポートの設定，471 ページ
- リモート LAN の設定，473 ページ

WLAN について

この機能により、ネットワーク管理者は 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 には識別子である（1～512）WLAN ID、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している各アクセス ポイントに対して最大 16 の WLAN を公開しますが、管理しやすくするため、最大 512 の WLAN を作成し、これらの WLAN を異なるアクセス ポイントに選択的に公開する（アクセス ポイント グループを使用）ことができます。

異なるサービス セット ID（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。

注意事項および制約事項

- 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、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。
- コントローラでは、同じ SSID の WLAN を区別するために、異なる属性が使用されます。
  - WLAN ID が 17 よりも小さい場合、同じ SSID と同じ L2 ポリシーを持つ WLAN は作成できません。
  - ID が 17 よりも大きい 2 つの WLAN が、同じ SSID と同じ L2 ポリシーを持つ場合は、別の AP グループに WLAN を追加できます。

（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。

- 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。

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いる必要があります。 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。

- CKIP
- 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 WPA（Wi-Fi Protected Access）/TKIP（Temporal Key Integrity Protocol）でそれぞれ設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES でそれぞれ設定することができます。

- 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 バリアント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。

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 の作成

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英数字 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 に対する最大 32 文字の英数字を入力します。

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。

（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。

（注） 有線ゲスト ユーザ用にゲスト LAN を作成する場合は、有線ゲスト アクセスの設定（CLI），（818 ページ）セクションの手順に従ってください。

- 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。

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 カウントの設定について

WLAN に接続できるクライアントの数に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に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 クライアントの数に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。

注意事項および制約事項

- 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。

（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（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、[Maximum Allowed Clients] テキスト ボックスに入力します。
プラットフォームごとのサポートされるクライアントの最大数については、「注意事項および制約事項,（372 ページ）」の項を参照してください。

ステップ 4 [Apply] 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*

各 WLAN の AP 無線ごとの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] をクリックして、変更を確定します。

各 WLAN の AP 無線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、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 設定されているアソシエートされたクライアントの最大数を表示するには、show 802.11a コマンドを使用します。

DHCP の設定

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 10 台以下のアクセス 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、DNS、またはプ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。

（注） クライアントが認証解除または削除された場合、DHCP Required 状態が原因でトラフィックが適切に転送されない場合があります。 この問題に対処するには、DHCP Required 状態が常に無効になるようにします。

（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 Assignment

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が推奨されます。

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。 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はプライマリおよびセカンダリ DHCP サーバに設定でき、サービス ポート インターフェイスは DHCP サーバを有効または無効にするように設定できます。

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は、すべての WLAN を DHCP Addr. 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。

また、DHCP Addr. Assignment Required を無効に設定して WLAN を作成できます。 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。 プライマリおよびセカンダリ DHCP サーバを定義する必要はありません。 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。

注意事項および制約事項

- 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。

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, （65 ページ）」の項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 [disabled] です。

（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。

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 [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] をクリックして、変更を保存します。

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）

- **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。

DHCP スコープの設定

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を求められる場合、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、それぞれある範囲の IP アドレスを指定する複数の 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 が定義された後、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できます。

注意事項および制約事項

最大 16 の DHCP スコープを設定できます。

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
```

WLAN の MAC フィルタリングの設定

WLAN の MAC フィルタリングについて

クライアント認可または管理者認可に 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。

ローカル MAC フィルタの設定

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。 GUI または CLI を使用して MAC フィルタを設定できます。

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。

注意事項および制約事項

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。

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ディセーブルになります。

- 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。

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。

DTIM period の設定

DTIM period について

802.11a/n ネットワークおよび 802.11b/g/n ネットワークの場合、Lightweight アクセス ポイントは、Delivery Traffic Indication Map（DTIM）と同期する一定間隔でビーコンをブロードキャストします。 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、802.11a/n または 802.11b/g/n のネットワークのビーコン期間が 100ms で DTIM 値が 1 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 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。 ブロードキャスト フレームおよびマルチキャスト フレームの頻度を考慮して、VoIP を含むアプリケーションに適したいずれかの設定を使用できます。

ただし、802.11a/n または 802.11b/g/n のすべてのクライアントで省電力モードが有効になっている場合は、DTIM 値を最大 255 まで設定できます（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 255 回のビーコンで 1 回送信）。 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、ビーコン周期が 100 ms で DTIM 値が 100 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 10 秒おきに送信するので、省電力クライアントを再起動してブロードキャストとマルチキャストをリッスンするまでのスリープ時間が長くなり、結果的にバッテリ寿命が長くなります。

（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 単位時間（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。 このため、たとえば、100 ミリ秒に設定されたビーコン期間は、実際には、104 ms のビーコン期間になります。

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。 省電力クライアントをサポートしている 802.11a/n ネットワークおよび 802.11b/g/n ネットワークでは、DTIM 値を小さく設定することを推奨します。

コントローラ ソフトウェア リリース 5.0 以降では、特定の WLAN 上の 802.11a/n および 802.11b/g/n 無線ネットワークの DTIM 期間を設定できます。 以前のソフトウェア リリースでは、DTIM period は無線ネットワークごとにのみ設定され、WLAN ごとに設定できませんでした。 この変更により、各 WLAN に異なる DTIM period を設定できるようになりました。 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。

注意事項および制約事項

コントローラ ソフトウェアをリリース 5.0 以降にアップグレードすると、無線ネットワークに対して設定されていた DTIM 期間が、そのコントローラのすべての既存の WLAN にコピーされます。

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] をクリックして、変更を確定します。

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 の下の 802.11a/n 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] をクリックして、変更を確定します。

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] をクリックして、変更を保存します。

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 上の 802.11a/n または 802.11b/g/n の無線ネットワークのいずれかに 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*

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........................................... Enabled
...
DTIM period for 802.11a radio.................... 1
DTIM period for 802.11b radio.................... 1
Local EAP Authentication..................... Disabled
...
```

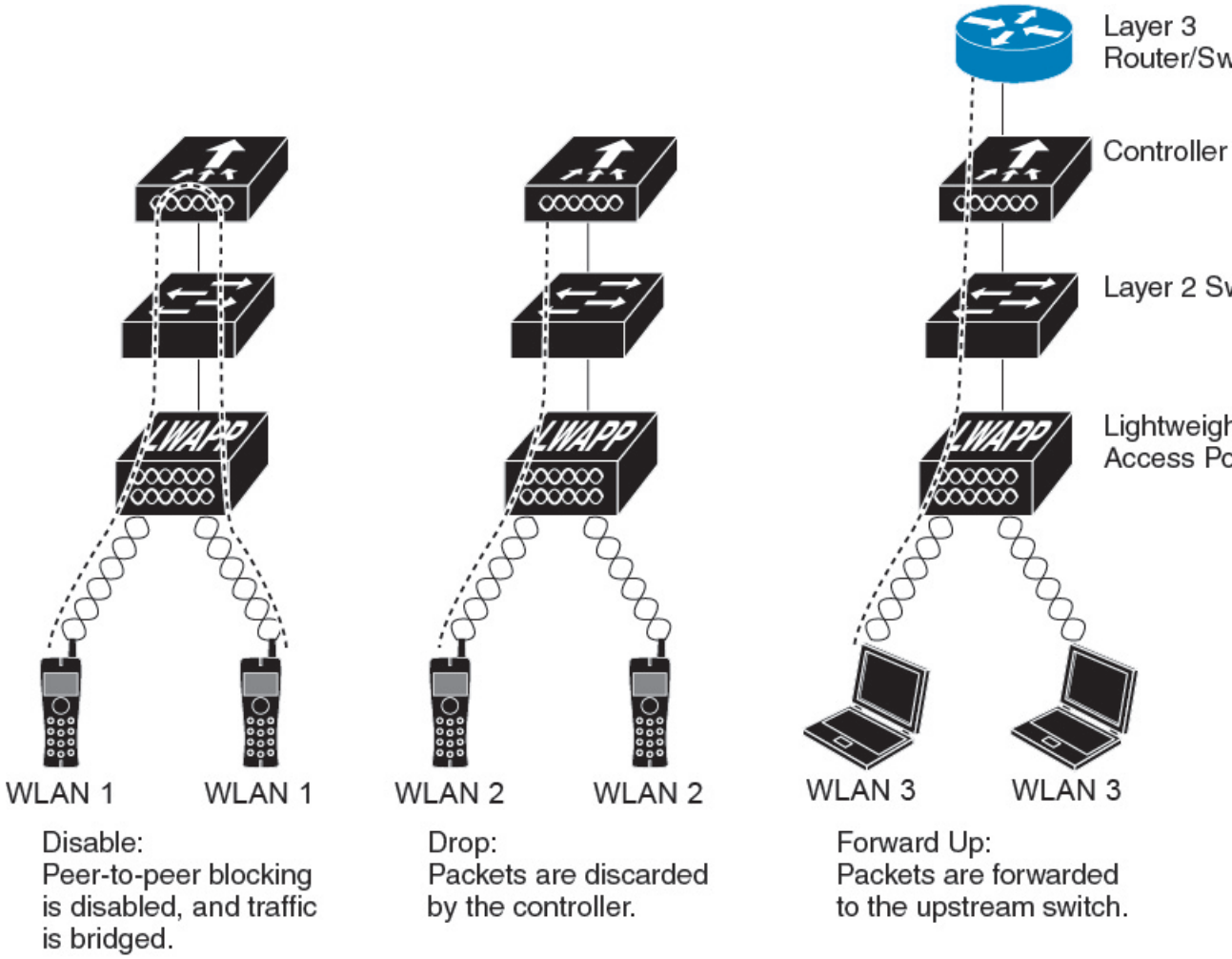
ピアツーピア ブロッキングの設定

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。 トラフィックがダイレクトされる方法をより詳細に制御することもできます。 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。

図 *34*：ピアツーピア ブロッキングの例



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。

注意事項および制約事項

- 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。 768 ビットは、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
```

レイヤ 2 セキュリティの設定

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 動的キーおよび認可の設定（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。

- 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 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。

注意事項および制約事項

- 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。
- 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、無線および Over-the-DS DS 方式の両方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プ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、同じ名前で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*

Static WEP と Dynamic WEP の両方をサポートする WLAN の設定

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 のアクセス ポイントはいずれも、ビーコンとプローブ応答で WPA1、WPA2、および 802.1X/PSK/CCKM/ 802.1X+CCKM 情報要素を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。

注意事項および制約事項

- 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 リリース 4.2 以降では、CCX バージョン 1 ～ 5 をサポートしています。 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。

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。

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 を選択できます。

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

以下に類似した情報が表示されます。

```
PMK-CCKM Cache
                            Entry
Type        Station         Lifetime   VLAN Override        IP Override
------  ------------------- --------   ------------------   ---------------
CCKM    00:07:0e:b9:3a:1b   150                              0.0.0.0
```

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

Sticky PMKID キャッシュの設定

sticky PMKID キャッシュについて

リリース 7.2 以降のリリースから、コントローラは sticky PMKID キャッシュ（SKC）をサポートします。 sticky PMKID キャッシュにより、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。

PKC（Proactive Key Caching）とも呼ばれる SKC では、クライアントは Pairwise Master Key Security Association（PMKSA）に対して各 Pairwise Master Key（PMK）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。

注意事項および制約事項

- 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 PMKID キャッシュの設定（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 Sticky PMKID キャッシュを有効にするには、次のコマンドを入力します。
config wlan security wpa wpa2 skc-cache enable *wlan_id*

デフォルトで、Sticky PMKID キャッシュ（SKC）は無効であり、Opportunistic PMKID キャッシュ（OKC）は有効です。

（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

CKIP の設定

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

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

セッション タイムアウトの設定（GUI）

[Session Timeout] テキスト ボックスに、300 ～ 86400 秒の値を入力して、クライアント セッションの期間を指定します。 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 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。 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 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
...
```

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。

注意事項および制約事項

- 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）

- **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

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。

注意事項および制約事項

- 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。 802.1X での使用はサポートされていません。
- 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、次の状況で、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。
- 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。

その他の情報

Web 認証の使用の詳細については、「ユーザ アカウントの管理」を参照してください。

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 [disabled] 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 ユーザの数が多い場合、または DHCP プールの IP アドレスが限れられている場合、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*

以下に類似した情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... cj
Network Name (SSID).............................. cj
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Network Admission Control

  NAC-State...................................... Disabled
  Quarantine VLAN................................ 0
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. 1800 seconds
CHD per WLAN..................................... Enabled
Webauth DHCP exclusion........................... Disabled
Interface........................................ management
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required............... Disabled
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
...
```

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

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。 このメカニズムを使用すると、ユーザは、インターネットにアクセスするために資格情報を入力する必要がある場合に、Web ブラウザを起動できます。実際の認証は、デバイスが新規の SSID に接続するたびに、バックグラウンドで行われます。

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 webauth 代行受信をトリガーします。 この代行受信によって webauth プロセスが発生し、プロセスは正常に完了します。 webauth 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。

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 検出を実行することなく、webauth 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）

- **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。

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

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，（382 ページ）」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
```

WLAN への QoS プロファイルの割り当て

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値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 *17*：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 Profile	AVVID 802.1p	IEEE 802.11e UP
ネットワーク制御	56（CS7）	Platinum	7	7
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

AVVID トラフィック タイプ	AVVID IP DSCP	QoS Profile	AVVID 802.1p	IEEE 802.11e UP
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）

まだ設定していない場合は、QoS プロファイルの設定（GUI），（166 ページ）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。

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。

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） burst-realtime-rate は average-realtime-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。

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） burst-realtime-rate は average-realtime-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。

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。

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 **save config** コマンドを入力します。

ステップ 3 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
...
```

QoS Enhanced BSS の設定

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ネル使用率をワイヤレス デバイスに通知できます。 チャ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が判断されます。 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。

  - Call Admission Control（CAC; コール アドミッション制御）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ドバ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ドバ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。

注意事項および制約事項

- 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 ユーザの方が多い場合に、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。

Cisco 7921 および 7920 Wireless IP Phone を使用する際の追加のガイドライン

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。

その他の情報

load-based の CAC の詳細および設定の手順は、「コントローラ設定の構成」を参照してください。

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。 768 ビットは、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*

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 WCS にレポートできます。 VoIP スヌーピングおよびレポートは、WLAN ごとに有効または無効にできます。

VoIP MSA スヌーピングが有効であると、この WLAN をアドバ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 WCS 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。 WCS は、失敗した VoIP コールに関する情報を [Events] ページに表示します。

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 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 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] または [802.11b/g/n] の順に選択して、[802.11a/n（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 *18*：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。
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。

エラー コード	整数型	説明
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。
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。

エラーコード	整数型	説明
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。

Key Telephone System-Based CAC の設定

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ビティ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。

注意事項および制約事項

- 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す。
- 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。

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**

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。

注意事項および制約事項

- 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。
- 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。
- 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

シームレスな IPv6 モビリティの設定

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。

注意事項および制約事項

- 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。

- 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。

- 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。
- IPv6 をグローバルにイネーブルまたはディセーブルにするには、次のコマンドを入力します。

  config ipv6 {**enable** | **disable**}

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 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。

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）

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 ネットワーク宛ての 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] 値に達した後にのみ実行されます。 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）

config ipv6 neigbhor-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 タイマーの設定（GUI）

ステップ 1 [Controller] > [IPv6] > [Neighbor Binding Timers] ページを選択します。

ステップ 2 次のタイマーを設定します。

- [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 [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。

ネイバー バインディング タイマーの設定（CLI）

config ipv6 neighbor-binding timers {down-lifetime | reachable-lifetime | stale-lifetime} {enable | disable}.

Cisco Client Extensions の設定

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、優れた電源管理などの、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。

注意事項および制約事項

- コントローラ ソフトウェアのリリース 4.2 以降では、CCX バージョン 1 ～ 5 をサポートしています。これにより、コントローラおよびそのアクセス ポイントは、CCX をサポートするサードパーティ製のクライアントデバイスと無線で通信できるようになります。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。 ただし、WLAN ごとに特定の CCX の機能を設定することができます。 この機能は、Aironet 情報要素（IE）です。
- 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番号などを含む）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。
- 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。

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）

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*

リモート LAN の設定

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。

注意事項および制約事項

- 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。
- 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 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、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す。

リモート LAN の設定

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*

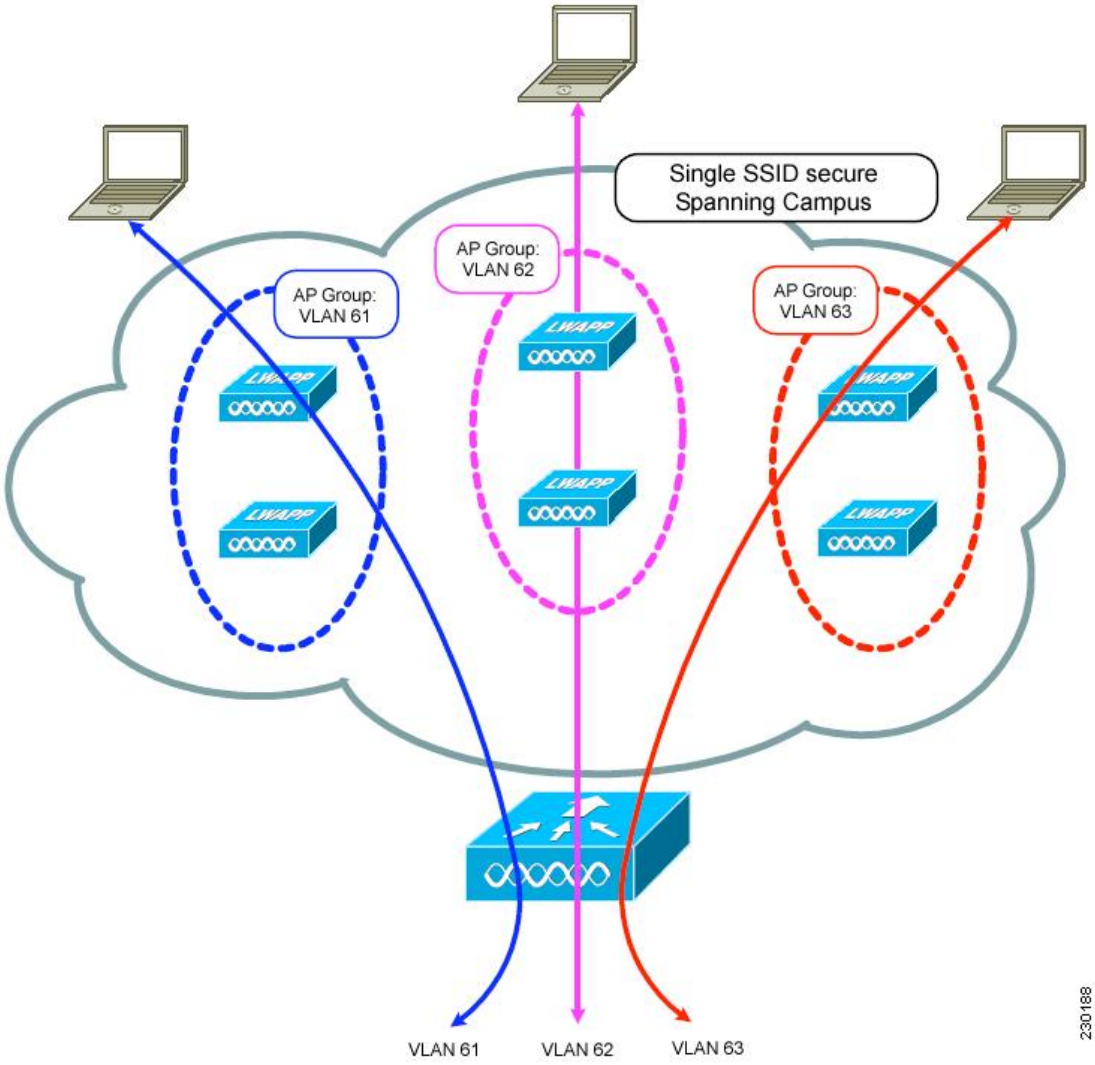
AP グループの設定

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、その WLAN にアソシエートされたすべてのユーザは、同じサブネットまたはVLAN上にあります。 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 *35*：アクセス ポイント グループ



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。 無線 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。

前述の図の例では、コントローラはアクセス ポイント間のローミングをレイヤ 3 ローミング イベントとして内部で処理します。 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 ポイントがコントローラに 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。

注意事項および制約事項

- 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す。 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。
- 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。
- 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。

  （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。

- 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。

- 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。

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と、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。

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。 NAC 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。

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 [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と、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 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

  以下に類似した情報が表示されます。

```
Site Name..................................... AP2
Site Description.............................. Access Point 2

WLAN ID          Interface          Network Admission Control
-------         -----------        --------------------------
 1         management           Disabled
 2        management           Disabled
 3        management          Disabled
 4        management           Disabled
 9        management           Disabled
 10     management           Disabled
 11     management           Disabled
 12     management           Disabled
 13     management           Disabled
 14     management           Disabled
 15     management           Disabled
 16     management           Disabled
 18     management           Disabled

AP Name Slots AP Model        Ethernet MAC     Location Port Country Priority GroupName
------- ---- -------------- ----------------- -------- ---- -------- -------- ---------
AP1242    2   AP1242AG-A-K9  00:14:1c:ed:23:9a default   1        US            1  AP2
...
```

- 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*

  以下に類似した情報が表示されます。

```
Site Name..................................... AP3
```

```
Site Description................................ Access Point 3

WLAN ID          Interface          BSSID
-------         ------------        -------------------
 10      management        00:14:1b:58:14:df
```

- 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*

  以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 166
Cisco AP Name.................................. AP2
...
Station Configuration
      Configuration ............................. AUTOMATIC
      Number Of WLANs ........................... 2
...
```

- 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**}

RF プロファイルの設定

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、802.11b/g/n 無線または 802.11a/n 無線に対して作成されます。 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ライブされたすべての 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ル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。

注意事項および制約事項

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 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。
- 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。
- 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。
- 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。
- 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。
- AP が割り当てられている AP グループは削除できません。

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。

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す。
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しきい値は 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) プローブに応答する条件となる、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*

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

- **config wlan apgroup profile-mapping** {**add** | **delete**} *ap-group-name rf-profile-name*

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

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。

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 ごとのアカウンティング サーバの無効化（GUI）

（注） アカウンティング サーバを無効にすると、すべてのアカウンティ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 に有用です。

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
```

NAC アウトオブバンド統合の設定

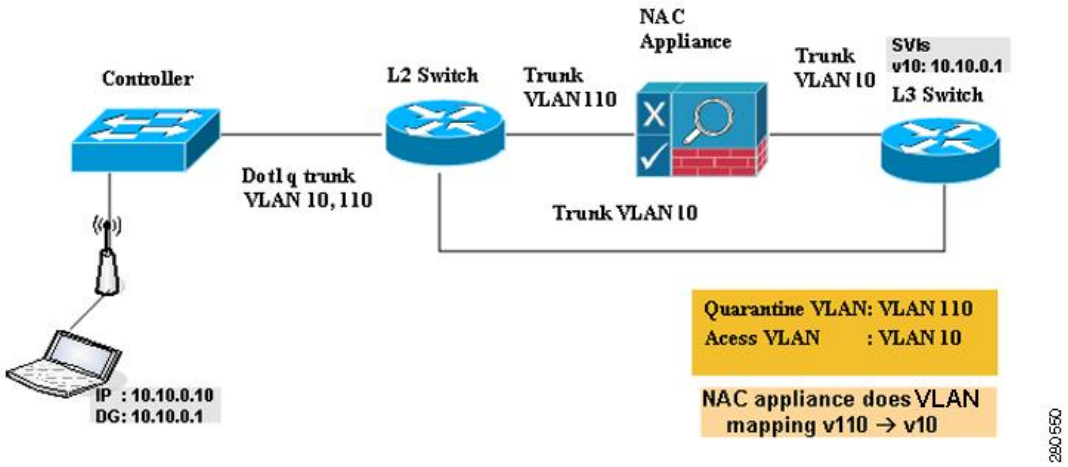
NAC アウトオブバンド統合について

Cisco NAC アプライアンス（Cisco Clean Access（CCA）とも呼ばれます）は、ネットワーク管理者がユーザにネットワークへの接続を許可する前に、有線および無線経由のユーザ、リモートのユーザおよびそのマシンを認証、承認、評価、感染修復する Network Admission Control（NAC）製品です。 Cisco 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の隔離 - 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 *36* : ***NAC*** アウト オブ バンド統合の例



注意事項および制約事項

- 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。
- 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 インタフェースとして同一の 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 つならば、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ので、ポスチャ検証を再度実行する必要があります。
- 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 アウトオブバンド統合は、WLAN AAA Override 機能では使用できません。

- 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） 設定手順については、Cisco NAC アプライアンス設定ガイドを参照してください。http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html

- 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の設定

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。

a) [Controller] > [Interfaces] の順に選択して、[Interfaces] ページを開きます。
b) [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。
c) [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。
d) [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。
e) [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。
f) [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の隔離 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。

g) 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。

h) [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。

a) [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 apgroup 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。

パッシブ クライアントの設定

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。

注意事項および制約事項

- 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 クライアントの設定（GUI）

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 モードをイネーブルにする必要があります。

マルチキャスト-マルチキャスト モードの有効化（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 [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。 768 ビットは、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] をクリックして、変更を確定します。

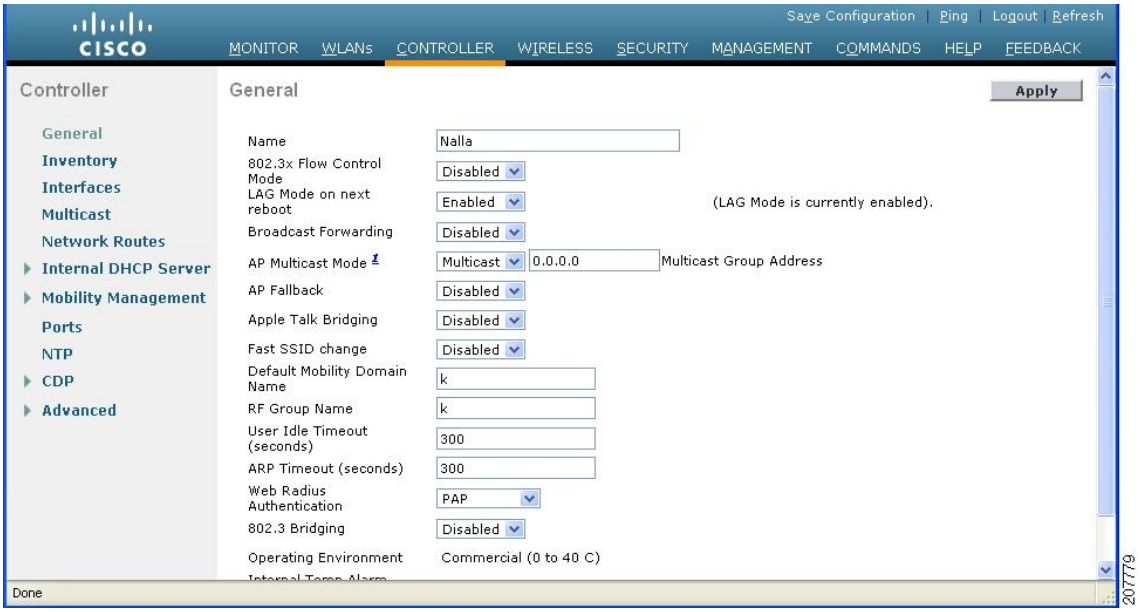
ステップ 6 [Multicast] をクリックして、グローバル マルチキャスト モードを有効にします。

マルチキャスト-マルチキャスト モードの有効化（GUI）

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 モードをイネーブル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。

図 *37*：*[Controller] > [General]* ページ



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。 768 ビットは、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] をクリックして、変更を確定します。

ステップ 6 [Multicast] をクリックして、グローバル マルチキャスト モードを有効にします。

コントロールでのグローバル 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 [disabled] 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 [disabled] 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

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。

注意事項および制約事項

- 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。
- 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。
- 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 のアカウンティング 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ティング 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。
- 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。

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 [Client Profiling] 領域では、次のことを実行できます。

a) DHCP に基づいてクライアントをプロファイルするには、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ァイルするには、HTTP Profiling 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] をクリックします。

クライアント プロファイルの設定（CLI）

- DHCP に基づいて WLAN のクライアント プロファイルを有効、または無効にするには、次のコマンドを入力します。

  config wlan profiling radius dhcp {**enable** | **disable**} *wlan-id*

- HTTP、または DHCP、あるいはその両方に基づいた WLAN のクライアント プロファイルを有効、または無効にするには、次のコマンドを入力します。

  config wlan 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。

- 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**}

WLAN ごとの RADIUS 送信元サポートの設定

WLAN ごとの RADIUS 送信元サポートについて

デフォルトでは、コントローラは、管理インターフェイス上の IP アドレスからすべての RADIUS トラフィックを送信します。つまり、WLAN にグローバル リストではなく、特定の RADIUS サーバが設定されている場合でも、使用される Identity は管理インターフェイスの IP アドレスです。

ユーザ別の WLAN フィルタリングを実行する場合は、APMAC:SSID 形式になるように RFC 3580 によって設定された 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 L3 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、ネットワーク アクセス プロファイルなどで役立ちます。

この機能を通常の RADIUS トラフィック送信元や、アドレス送信元として管理インターフェイスを使用する一部の WLAN、および WLAN ごとの動的インターフェイスを使用するその他の WLAN に統合することができます。

注意事項および制約事項

- コントローラは、選択されたインターフェイスからトラフィックを送信するだけなので、新規の Identity に適切なルール フィルタリングを実装するタスクは、認証サーバ（RADIUS）が行います。
- callStationID は、802.1x RADIUS RFC 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
```

リモート LAN の設定

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。

注意事項および制約事項

- 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。
- 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 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、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す。

リモート LAN の設定

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 8 章

Lightweight アクセス ポイントの制御

この章で説明する内容は、次のとおりです。

- アクセス ポイント通信プロトコル，478 ページ
- アクセス ポイントの検索，486 ページ
- アクセス ポイント無線の検索，492 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，494 ページ
- アクセス ポイントの認証の設定，497 ページ
- 組み込みアクセス ポイントの設定，501 ページ
- 自律アクセス ポイントの Lightweight モードへの変換，503 ページ
- OfficeExtend アクセス ポイントの設定，527 ページ
- Cisco ワークグループ ブリッジの使用，547 ページ
- Cisco 以外のワークグループ ブリッジの使用，553 ページ
- バックアップ コントローラの設定，555 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，560 ページ
- アクセス ポイントの再送信間隔および再試行回数の設定，563 ページ
- 国番号の設定，565 ページ
- アクセス ポイントの -J 規制ドメインから -U 規制ドメインへの移行，571 ページ
- 日本での W56 帯域の使用，574 ページ
- 動的周波数選択，575 ページ
- アクセス ポイントでの RFID トラッキングの最適化，577 ページ
- プローブ要求フォワーディングの設定，579 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，580 ページ

- リンク テストの実行，581 ページ
- リンク遅延の設定，584 ページ
- TCP MSS の設定，587 ページ
- Power over Ethernet の設定，588 ページ
- 点滅する LED の設定，594 ページ
- クライアントの表示，595 ページ
- アクセス ポイントの LED 状態の設定，598 ページ

アクセス ポイント通信プロトコル

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 1260 および 3500 シリーズ アクセス ポイントは唯一の例外であり、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。

注意事項および制約事項

- 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。
- 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 アクセス ポイントはソフトウェアによる暗号化で DTLS データ暗号化をサポートし、1040、1140、1250、1260、2600、3500 および 3600 シリーズ アクセス ポイントはハードウェアによる暗号化で DTLS データ暗号化をサポートします。

- 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の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 イメージを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、WiSM2、WLC2：デフォルトでは、これらのプラットフォームには、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。
- 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、WISM2 および Cisco 2500 シリーズ コントローラを使用するすべてのお客様は、データ DTLS を有効にする必要があります。

Cisco 5500 シリーズ コントローラ用 DTLS イメージを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。

注意 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。
- RMAed コントローラはそれらの LDPE イメージで使用できます。 LDPE イメージを持つこのようなコントローラは、LDPE 以外のイメージに変換できません。 回避策として、LDPE 以外のイメージと同等の DTLS ライセンスをインストールする必要があります。

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。ライセンスの取得およびインストール方法の詳細については、「コントローラ設定の構成」の項を参照してください。

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。

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 [disabled] 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。

注意事項および制約事項

- 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。 以前のソフトウェア リリースでは、アクセス ポイントがコントローラに通知し、セッションを終了せずに変更された IP アドレスで継続されていました。
- 1100 および 1300 シリーズ アクセス ポイントをコントローラに接続する前に、ソフトウェア リリース 4.0.155.0 以降のリリースをコントローラにインストールする必要があります。 1120 および 1310 アクセス ポイントは、ソフトウェア リリース 4.0.155.0 以前ではサポートされていません。
- ディスカバリ プロセスでは、1140 および 3500 シリーズ アクセス ポイントは、シスコ CAPWAP コントローラに対するクエリーのみを送信します。 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 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。
- 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。

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

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

[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 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 つまたは複数をオンにして、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 つまたは複数をオンにして、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、1130AG、1140、1240AG、1250、1260、3500、および AP801 AP802 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 はスペクトラム インテリジェンスをサポートし、AP1260 はスペクトラム 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。

- [Certificate Type]：次のチェックボックスの 1 つまたは複数をオンにして、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 ポイントの認可」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オンにして、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オンにして、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 *38*：*[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 *19*：インターフェイス パラメータの詳細

ボタン	説明
AP 名	アクセス ポイントの名前。
Link Speed	干渉の速度（Mbps 単位）。
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。

ボタン	説明
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。
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。

ボタン	説明
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 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]（または [802.11b/g/n]） > [Radios] > [Details] の順に選択して、[802.11a/n（または [802.11b/g/n]）Radios] ページを開きます。
- [Wireless] > [Access Points] > [Radios] > [802.11a/n]（または [802.11b/g/n]）の順に選択して、[802.11a/n（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 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 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 つまたは複数をオンにして、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 ポイントをリブート、または無線の CleanAir 機能をディセーブル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 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。

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

Cisco IOS アクセス ポイントには、工場出荷時にデフォルトのイネーブル 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** および **debug** コマンドを実行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 コマンドを実行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。

注意事項および制約事項

- 5.0 以前のコントローラ ソフトウェア リリースでは、現在、コントローラに接続されているアクセス ポイントについてのみ、アクセス ポイント イネーブル パスワードを設定できます。 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、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。
- また、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、アクセス ポイントをコントローラに join した後で、アクセス ポイントによりコンソール ポートのセキュリティが有効化され、このアクセス ポイントのコンソール ポートにログインしようとすると、必ずユーザ名とパスワードを求めるプロンプトが表示されます。 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 ソフトウェア リリース 5.0 以降のこれらの機能は、1100 シリーズを除く、Lightweight モードに変換されたアクセス ポイントすべて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。
- 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。 そうしないと、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くなることがあります。 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、コントローラ CLI で、**clear ap config** *Cisco_AP* コマンドを入力します。 コマンドを入力しても、アクセス ポイントの固定 IP アドレスはクリアされません。 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。

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、およびイネーブル 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。 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、oscic、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は使用しないでください。

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イネーブル 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、およびイネーブル 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 （オプション）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、およびイネーブル 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、イネーブル 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。
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、およびイネーブル 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 （オプション）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、およびイネーブル 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

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

AP Name       Slots     AP Model          Ethernet MAC     Location       Port  Country
--------     ------ ------------------- ----------------- ---------------- ----  -------
FlexConnect     2   AIR-AP1131AG-N-K9 00:13:80:60:48:3e  default location  1     US
```

（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す。

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... FlexConnect
...
AP User Mode..................................... AUTOMATIC
AP User Name..................................... globalap
```

（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。

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

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。

注意事項および制約事項

- 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。
- 現在コントローラに join している、また、今後 join す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。 必要に応じて、このグローバル認証設定よりも優先される、独自の認証設定を特定のアクセス 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 ポイントの認証の設定

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。

a) [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
b) 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。
c) [Credentials] タブをクリックして [All APs > Details for]（Credentials）ページを開きます。
d) [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。
e) [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る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。
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 dot1xuser add username *user* **password** *password* **all**
（注） *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を含む。 - どの言語の単語でもない。

ステップ 2 （オプション）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 dot1xuser add username *user* **password** *password Cisco_AP*

（注） *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 dot1xuser 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 （オプション）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 dot1xuser 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
```

（注） グローバルな認証が設定されていない場合、[Global AP Dot1x 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 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す。

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 0
Cisco AP Name.................................... FlexConnect
...
AP Dot1x User Mode............................... AUTOMATIC
AP Dot1x User Name............................... globalDot1x
...
```

（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、[AP Dot1x User 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**

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

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。

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 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。

- 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** コマンドが正常に動作しない場合は、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。
- 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。

その他の関連資料

- 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

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

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 ポイントの Lightweight モードへの変換の手順については、『*Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode*』を参照してください。 このマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

注意事項および制約事項

- 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。
- 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。 以前のリリースでは、無線ごとに 8 の BSSID と、アクセス ポイントごとに合計 8 の無線 LAN がサポートされました。 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。
- 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。

- 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。

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 ポイントがリブートするまで待ち、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 が赤色に変わったら（約 20 ～ 30 秒かかります）、MODE ボタンを放します。

ステップ 8 アクセス ポイントがリブートしてすべての LED が緑色に変わった後、ステータス LED が緑色に点滅するまで待ちます。

ステップ 9 アクセス ポイントがリブートしたら、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 ポイントの認可

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 サーバに認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 ポイントの認可

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 日よりも前に出荷された 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 ポイントの認可

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、ハッシュ検証はイネーブルです。 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 のハッシュ検証をディセーブルにすると、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。 APS 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 キー検証をイネーブルにするには、[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 ポイントの認可

RADIUS サーバによって、MIC を使用してアクセス ポイントを認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 ポイントを認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 ポイントの認可の前に、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、強力に認証されます。

（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 ポイントの認可

独自の公開鍵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。

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 ポイントをプロビジョン リストに追加します。

（注） アクセス ポイントをプロビジョン 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 C*xxxx-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 ポイントの認可（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 ポイントを認可する際に 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 ポイントを認可する際に 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。

a) [Add] をクリックして、[Add AP to Authorization List] 領域にアクセスします。

b) [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。

c) [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。

d) [Add] をクリックします。 アクセス ポイントが認可リストに表示されます。

（注） アクセス ポイントを認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 ポイントの認可（CLI）

ステップ 1 次のコマンドを入力して、アクセス ポイントの認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**}}

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**}}

ステップ 3 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認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**

ステップ 4 次のコマンドを入力して、アクセス ポイントの認可リストを表示します。
show auth-list

以下に類似した情報が表示されます。

```
Authorize MIC APs against Auth-list or AAA ..... disabled
Authorize LSC APs against Auth-List ..... disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate..... no
  AP with Locally Significant Certificate..... no
```

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、リブ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 WCS 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 WCS 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 ポイントのリブ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 *20*：*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
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

アクセス ポイント	VCI 文字列
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 無線インターフェイスの MAC アドレスです。

（注） 802.11 無線インターフェイスの 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

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.
```

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 リストから、[TFTP] または [FTP] を選択します。

ステップ 4 [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 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、ファイルをコントローラから TFTP または FTP サーバに転送します。

- **transfer upload mode** {**tftp** | **ftp**}
- **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 [AP Core Dump] 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 reset-button {**enable** | **disable**} {*ap-name* | **all**}

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。

a) [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。
b) [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。
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。

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 ポイントのスタティック 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。

a) 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作ることで、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。

OfficeExtend アクセス ポイントの設定

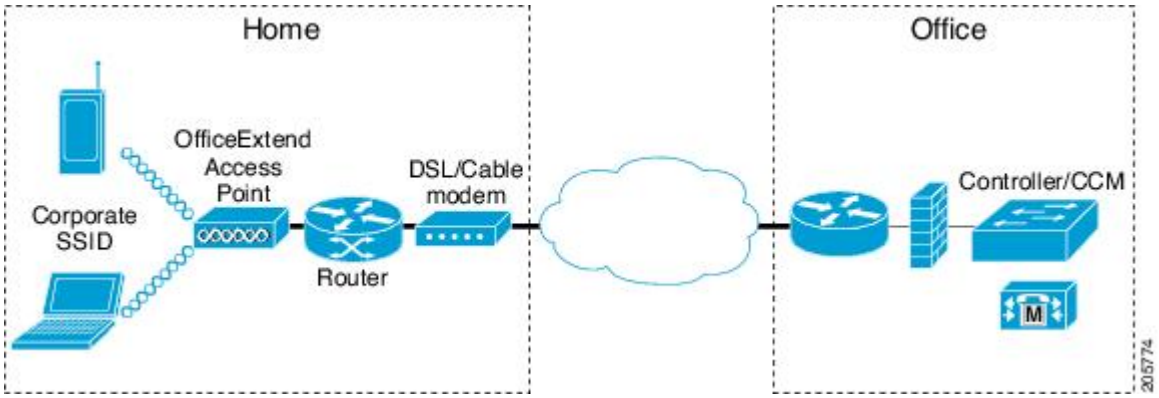
OfficeExtend アクセス ポイントについて

OfficeExtend アクセス ポイントは、リモート ロケーションにおけるコントローラからアクセス ポイントへの安全な通信を提供し、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 600 シリーズ OfficeExtend アクセス ポイント上で永続的にイネーブルです。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 *39*：一般的な *OfficeExtend* アクセス ポイント セットアップ



（注） OfficeExtendアクセス ポイントは、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 デバイスを越えて動作するよう設計されています。 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。 コントローラ ソフトウェア リリース 7.2 以降のリリースでは、NAT デバイスの後方に OfficeExtend アクセス ポイントを 3 台まで展開できます。 以前のコントローラ リリースでは、1 台のデバイスしかサポートされていませんでした。

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、OfficeExtend アクセス ポイントとして動作するように設定できます。

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） Cisco 600 シリーズ OfficeExtend アクセス ポイントは、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 デバイスを越えて動作するよう設計されています。 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。 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、単一の NAT デバイスの後方に単一の OfficeExtend アクセス ポイントのみを展開できます。

（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 *40* : *OEAP* モード

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。

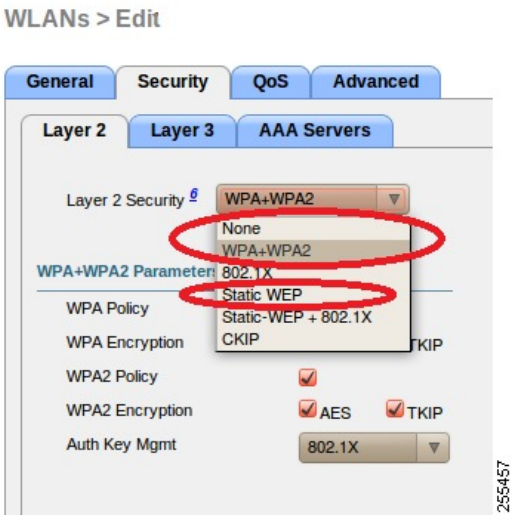
600 シリーズ OfficeExtend アクセス ポイントに対する WLAN のセキュリティ設定

WLAN でセキュリティを設定（図 41：WLAN レイヤ 2 セキュリティ設定, （531 ページ）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 *41*：*WLAN* レイヤ *2* セキュリティ設定



[Security] タブ（図 42：WLAN のセキュリティ設定 - 認証キー管理, （532 ページ）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 *42*：*WLAN* のセキュリティ設定 - 認証キー管理

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 *43* : *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 *44* : *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 *45* : *OEAP* シリーズに対する互換性のあるセキュリティ設定

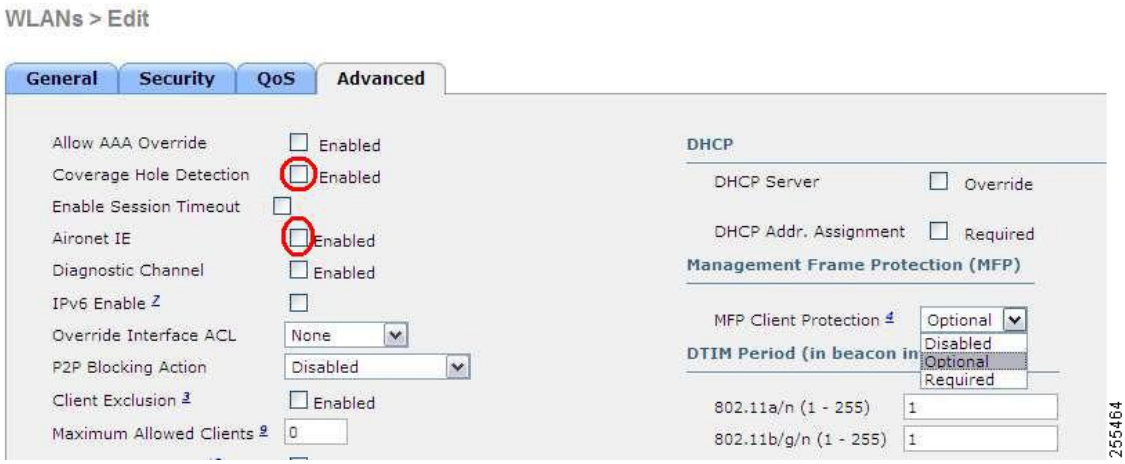
図 *46* : *OEAP* シリーズに対する互換性のあるセキュリティ設定

QoS 設定はサポートされています（図 47 : OEAP 600 に対する QoS の設定, （535 ページ）を参照）が、CAC 設定はサポートされていないので、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。

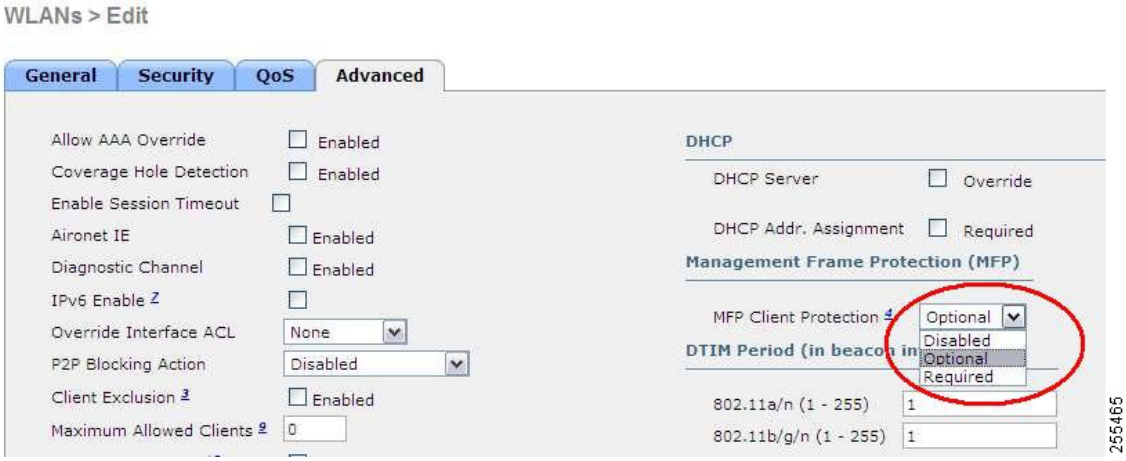
（注） Aironet IE は有効にしないでください。 このオプションはサポートされていません。

図 *47* : *OEAP 600* に対する *QoS* の設定



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 *48* : *OEAP* シリーズ アクセス ポイントに対する *MFP* の設定



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

600 シリーズ OfficeExtend アクセス ポイントで提供される WLAN コントローラ WLAN では、一度に 15 ユーザのみ接続が許可され、16 番目のユーザは最初のクライアントのいずれかが認証解除になるか、コントローラでタイムアウトが発生するまで認証できません。 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。

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 *49*：*OEAP 600* シリーズ *AP* に対するリモート *LAN* の設定

[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 *50*：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 *51*：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 *52*：*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 *53*：*OEAP 600 AP* のチャネル幅

その他の注意事項

600 シリーズ OfficeExtend アクセス ポイントは、単一の AP 導入向けに設計されているので、600 シリーズ OfficeExtend 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。

コントローラで 802.11a/n 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、600 シリーズ OfficeExtend アクセス ポイント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。

（注） 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。

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 アクセス ポイントでは、LSC はサポートされません。

1. ローカルで有効な証明書（LSC）を使用して OfficeExtend アクセス ポイントを認可する手順は、LSC を使用したアクセス ポイントの認可に示されています。
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 ポイントのみがコントローラに join 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。

1 **save config** コマンドを入力して、設定を保存します。

（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シング

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。 ライセンスがインストールされた後は、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 ポイントで OfficeExtend モードを有効にできます。

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。

（注） LSC の設定は要件ではなく、オプションです。 OfficeExtend アクセス ポイントでは、LSC はサポートされません。

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] をクリックして、変更を確定します。 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、イネーブル 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 [Save Configuration] をクリックします。

ステップ 9 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，（830 ページ）の項で、DCA 間隔、チャネル 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）

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 FlexConnect を有効にします。
config ap mode flexconnect *Cisco_AP*

ステップ 2 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。

ステップ 3 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。

ステップ 4 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 [disabled] 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。

ステップ 5 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。

ステップ 6 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 oeap-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。

ステップ 7 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 oeap-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。

ステップ 8 「**save config**」と入力します。

ステップ 9 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, （830 ページ）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。

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。

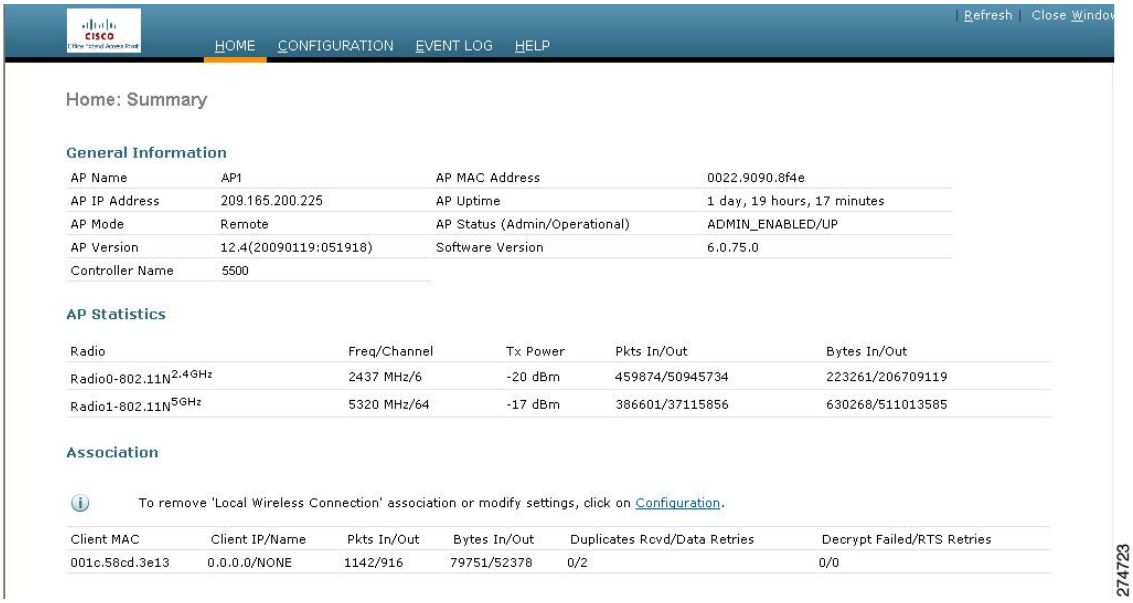
ステップ 2 OfficeExtend アクセス ポイントがホーム ルータに接続された状態で、インターネット ブラウザの [Address] テキスト ボックスに OfficeExtend アクセス ポイントの IP アドレスを入力して [Go] をクリックします。

（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。

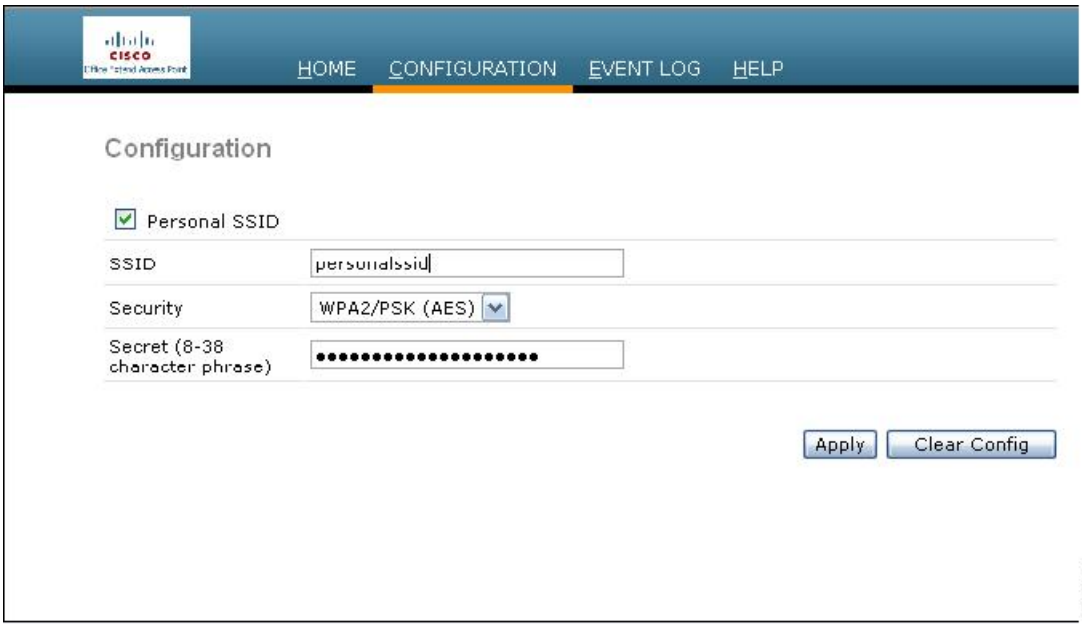
図 *54*：*OfficeExtend* アクセス ポイントの *[Home]* ページ



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 *55* : *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 [disabled] 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*}

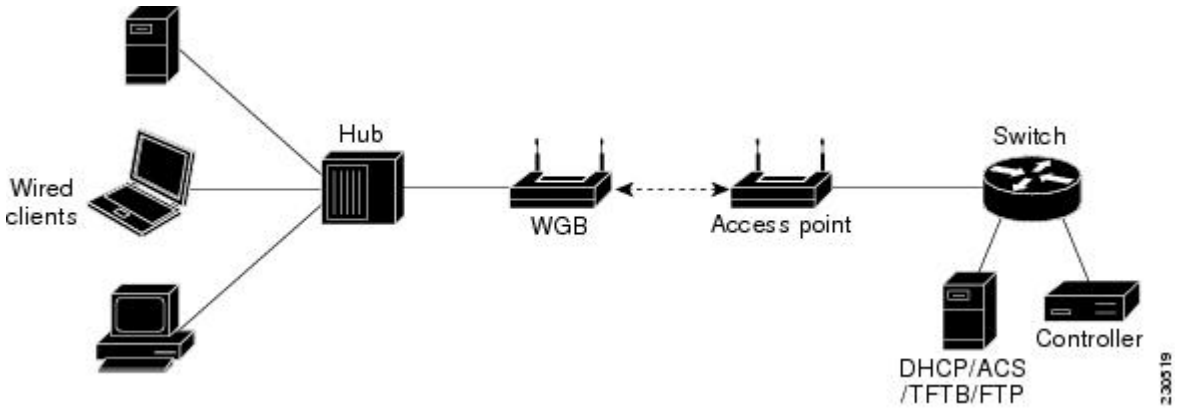
Cisco ワークグループ ブリッジの使用

Cisco ワークグループ ブリッジについて

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、イーサネットで 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。

図 *56* : *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。

注意事項および制約事項

- 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。

- WGB は Lightweight アクセス ポイントにのみ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。

- 次の機能は、WGB との併用がサポートされています。
  - ゲスト N+1 冗長性
  - ローカル EAP
  - Open、WEP 40、WEP 128、CKIP、WPA+TKIP、WPA2+AES、LEAP、EAP-FAST、および EAP-TLS 認証モード
- 次の機能は、WGB との併用が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。

- 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。
- 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 のエージングアウト 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。
- 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。
- 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
- 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。
- 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 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。

a) [Clients > Detail] ページで [Back] をクリックして、[Clients] ページに戻ります。

b) 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。

c) 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

以下に類似した情報が表示されます。

```
Number of WGBs..................................... 1

MAC Address        IP Address  AP Name    Status    WLAN    Auth  Protocol  Clients
-----------------  ----------   --------  ------    ----   ----- --------- --------
00:0d:ed:dd:25:82  10.24.8.73      a1      Assoc     3         Yes   802.11b    1
```

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*

以下に類似した情報が表示されます。

```
Number of wired client(s): 1

MAC Address          IP Address  AP Name   Mobility   WLAN   Auth
-------------------  ----------  -------- ---------  -----  -----
00:0d:60:fc:d5:0b    10.24.8.75     a1           Local      3         Yes
```

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**

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

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

注意事項および制約事項

- リリース 7.0.116.0 より、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。

- Cisco 以外の WGB には、次の制約事項が適用されます。
  - 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 ポイゾ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。

- 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。

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

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。 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、ネットワーク内の特定のアクセス ポイントのプライマリ、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。

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 5.0 以降のリリースでは、コントローラに接続されたすべてのアクセス ポイントおよび、ハートビート タイマーやディスカバリ要求タイマーを含むさまざまなタイマーに、プライマリおよびセカンダリ バックアップ コントローラ（プライマリ、セカンダリ、またはターシャリ コントローラが指定されていない場合、または応答しない場合に使用）を設定することもできます。 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。
- 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。
- 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。

- ソフトウェア リリース 5.2 以降のリリースが実行されているコントローラに別のソフトウェア リリース（4.2、5.0、5.1 など）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。

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 コントローラをは無効です。

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 コントローラを無効にします。

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。

a) [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b) 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。

c) [High Availability] タブを選択して、[All APs > Details for]（[High Availability]）ページを開きます。

d) 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..... 1-4404
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
```

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

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。

注意事項および制約事項

- 5.1 よりも前のコントローラ ソフトウェア リリースでは、バックアップ コントローラはアソシエーション要求を受信した順序ですべてのポートが使用中となるまで許可します。その結果、アクセス ポイントがバックアップ コントローラ上で開いているポートを見つけられる可能性は、コントローラ障害の後のアソシエーション要求キュー内の位置によって決まります。
- コントローラ ソフトウェア リリース 5.1 以降のリリースでは、バックアップ コントローラがプライオリティの高いアクセス ポイントからの join request を認識し、使用可能なポートを提供するための手段として、必要に応じてプライオリティの低いアクセス ポイントをアソシエーション解除するように、ワイヤレス 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。 768 ビットは、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。

アクセスポイントの再送信間隔および再試行回数の設定

アクセス ポイントの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アクセス ポイントは、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、アクセス ポイントは別のコントローラに再びアソシエートされます。

注意事項および制約事項

- 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。

アクセス ポイント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。

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

```
(Cisco Controller) >show ap retransmit all
Global control packet retransmit interval: 5
Global control packet retransmit count: 6
AP Name             Retransmit Interval  Retransmit count
------------------  -------------------  -------------------
```

```
AP_1131                 N/A(Mesh mode)      N/A(Mesh mode)
AP_cisco                        5                   4
abhes_1240                      5                   6
```

（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*

```
(Cisco Controller) >show ap retransmit cisco_AP1
Global control packet retransmit interval: 5
Global control packet retransmit count: 6
AP Name             Retransmit Interval  Retransmit count
------------------  -------------------  -------------------
cisco_AP1                   5                   6
(Cisco Controller) >
```

国番号の設定

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。

注意事項および制約事項

- 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 ソフトウェア リリース 4.1 以降のリリースでは、コントローラごとに 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

または

http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html

- 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コントローラは、同じ国で構成された一連の国々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、Radio Resource Management（RRM）自動 RF 機能が有効になっている場合、許可される共通のチャネルは、各国で許可されているチャネルの組み合わせ（またはスーパーセット）を実行することによって引き出されます。 アクセス ポイントは常にすべての合法的な周波数を使用できますが、共通でないチャネルは手動でのみ割り当てることができます。
- アクセス ポイントは、その国向けに設計されているチャ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。

- 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。

国番号の設定（GUI）

ステップ 1 802.11a および 802.11b/g ネットワークを無効にする手順は、次のとおりです。

a) [Wireless] > [802.11a/n] > [Network] を選択します。
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。
d) [Wireless] > [802.11a/n] > [Network] を選択します。
e) [802.11b/g Network Status] チェックボックスをオフにします。

f) [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 チャネルと電力レベルが共通のチャ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* で複数の国番号を選択した場合、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） 国番号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。

a) 次のいずれかの操作を行います。

- 802.11a および 802.11b/g ネットワークを無効のままにします。
- 802.11a および 802.11b/g ネットワークを再び有効にしてから、国番号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。

b) [Wireless] > [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。
c) 目的のアクセス ポイントのリンクをクリックします。
d) [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国番号は、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* で有効にしなかった場合は、802.11a および 802.11b/g ネットワークを再び有効にします。

ステップ 8 [Save Configuration] をクリックします。

国番号の設定（CLI）

ステップ 1 次のコマンドを入力して、使用可能な国番号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、802.11a および 802.11b/g 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国番号を設定します。
config country *code1*[,*code2*,*code3*,...]

複数の国番号を入力する場合には、各国番号をカンマで区切ります（**config country US,CA,MX** など）。以下に類似した情報が表示されます。

```
Changing country code could reset channel configuration.
If running in RFM One-Time mode, reassign channels after this command.
Check customized APs for valid channel values after this command.
Are you sure you want to continue? (y/n) y
```

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。 以下に類似した情報が表示されます。

```
Configured Country..................... Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
--More-- or (q)uit
            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . . A A A A *
```

```
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . C C C C x
```

ステップ 5 次のコマンドを入力して、国番号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国番号の使用可能なチャネルの一覧を表示します。
show country channels

以下に類似した情報が表示されます。

```
Configured Country............................ Multiple Countries:US,CA,MX
Auto-RF for this country combination is limited to common channels and power.
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-) = Regulatory Domains allowed by this country.
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11BG    :
Channels    :                   1 1 1 1 1
            : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : A * * * * A * * * * A . . .
 CA (-AB)   : A * * * * A * * * * A . . .
 MX (-NA)   : A * * * * A * * * * A . . .
 Auto-RF    : C x x x x C x x x x C . . .
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 802.11A    :                         1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels    : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6

            : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-AB)   : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 CA (-ABN)  : . A . A . A . A A A A A * * * * * . . . * * * A A A A *
 MX (-N)    : . A . A . A . A A A A A . . . . . . . . . . . A A A A *
    Auto-RF : . C . C . C . C C C C C . . . . . . . . . . . C C C C x
------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

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 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

以下に類似した情報が表示されます。

```
Number of APs................................... 2

AP Name    Slots  AP Model              Ethernet MAC          Location          Port    Country
-------- ------ -----------------  -----------------    ----------------    ------- --------
ap1     2  AP1030       00:0b:85:5b:8e:c0   default location        1           US
```

```
ap2      2  AIR-AP1242AG-A-K9   00:14:1c:ed:27:fe   default location              1           US
```

ステップ 9 ステップ *3* で複数の国番号を入力した場合は、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。

- 802.11a/n および 802.11b/g/n ネットワークを無効のままにします。
- 802.11a/n および 802.11b/g/n ネットワークを再び有効にしてから、国番号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**}

選択した国番号が、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、指定した国番号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。

たとえば、**config ap country mx all** と入力した場合、次のような情報が表示されます。

```
To change country code: first disable target AP(s) (or disable all networks).
  Changing the country may reset any customized channel assignments.
  Changing the country will reboot disabled target AP(s).

 Are you sure you want to continue? (y/n) y

AP Name     Country  Status
---------    -------- --------
ap2     US    enabled  (Disable AP before configuring country)
ap1       MX    changed  (New country configured, AP rebooting)
```

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 10 802.11a/n および 802.11b/g/n ネットワークをステップ *9* で再び有効にしなかった場合には、ここで有効にするために次のコマンドを入力します。
config 802.11{a | b} enable network

ステップ 11 「**save config**」と入力します。

アクセス ポイントの -J 規制ドメインから -U 規制ドメインへの移行

アクセス ポイントの -J 規制ドメインから -U 規制ドメインへの移行について

日本政府は、5GHz 無線周波スペクトルの規制を変更しました。 これらの規制によって、802.11a 5GHz 無線のテキスト ボックスがアップグレードできるようになりました。 日本では、次の 3 つの周波数セットが許可されています。

- J52 = 34（5170 MHz）、38（5190 MHz）、42（5210 MHz）、46（5230 MHz）
- W52 = 36（5180 MHz）、40（5200 MHz）、44（5220 MHz）、48（5240 MHz）
- W53 = 52（5260 MHz）、56（5280 MHz）、60（5300 MHz）、64（5320 MHz）

シスコでは、これらの周波数セットを次の規制ドメインにまとめました。

- -J 規制ドメイン = J52
- -P 規制ドメイン = W52 + W53
- -U 規制ドメイン = W52

規制ドメインとは、シスコが世界の周波数の規制を論理的なグループにまとめたものです。 たとえば、ヨーロッパの大半の国は -E 規制ドメインに入ります。 シスコのアクセス ポイントは工場で特定の規制ドメイン向けに設定され、この移行プロセス以外によって変更されることはありません。 規制ドメインは無線ごとに割り当てられるので、アクセス ポイントの 802.11a および 802.11b/g 無線は別々のドメインに割り当てられることがあります。

（注） コントローラとアクセス ポイントは、その国で使用できるように設計されていない場合、正しく動作しない場合があります。 たとえば、部品番号が AIR-AP1030-A-K9（米国の規制ドメインに含まれている）のアクセス ポイントは、オーストラリアでは使用できません。 その国の規制ドメインに適合したコントローラとアクセス ポイントを購入するよう、常に確認してください。

日本の規制では、アクセス ポイントの無線を -J ドメインから -U ドメインへ移行するようにプログラムされた規制ドメインが許可されています。 日本市場向けの新しいアクセスポイントには、-P 規制ドメインに対応した設定の無線が含まれています。 -J 無線は、現在販売されていません。 現在お使いの -J 無線が新しい -P 無線と共に 1 つのネットワーク内で動作することを確認するには、お使いの -J 無線を -U 区域に移行する必要があります。

国番号は、各国で合法的に使用できるチャネルを定義します。 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。

（注） J2 -Q は、1550 および 3600 を除くすべてのアクセス ポイントに対して 7.0.116.0 で動作します。 1550 アクセス ポイントがコントローラに join するには、-J4 区域が必要です。

- J3：-U 周波数を使用しますが、-U 無線および -P 無線の両方をコントローラに join できます。
- J4：2.4G PQU および 5G JPQU がコントローラに join できるようにします。

（注） 移行した後は、J3 国番号を使用する必要があります。 お使いのコントローラでソフトウェア リリース 4.1 以降のリリースが動作している場合には、複数の Country Code 機能を使用して、J2 と J3 の両方を選択できます。 手動で -P 無線を設定して J3 で対応していないチャネルを使用できます。

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。

注意事項および制約事項

アクセスポイントを -U 規制ドメインに移行する場合には、次のガイドラインに従ってください。

- 移行できるのは、-J 規制ドメインおよび Airespace AS1200 アクセス ポイントをサポートする Cisco Aironet 1130、1200、および 1240 Lightweight アクセス ポイントのみです。 その他のアクセス ポイントは移行できません。
- お使いのコントローラとすべてのアクセス ポイントでは、ソフトウェア リリース 4.1 以降のリリースまたはソフトウェア リリース 3.2.193.0 が動作している必要があります。

（注） ソフトウェア リリース 4.0 はサポートされていません。 アクセス ポイントの移行にソフトウェア リリース 3.2.193.0 を使用した場合、ソフトウェア リリース 4.0 にアップグレードできません。アップグレードできるのは、ソフトウェア リリース 4.1 以降のリリースまたは 3.2 ソフトウェアの後続リリースのみです。

- お使いのコントローラを最後にブートしたときに、1 つまたは複数の日本の国番号（JP、J2、または J3）を設定しているはずです。

- -J 規制ドメインをコントローラに join するよう設定したアクセス ポイントが、少なくとも 1 つは必要です。
- アクセス ポイントを -U 規制ドメインから -J 区域へ移行しなおすことはできません。 日本政府は、移行の反転を違法であると規定しています。

（注） アクセス ポイントの移行をやり直すことはできません。アクセス ポイントを移行すると、ソフトウェア リリース 4.0 に戻ることはできません。 移行済みのアクセス ポイントでは、ソフトウェア リリース 4.0 下の 802.11a 無線が機能できなくなります。

- 移行プロセスは、コントローラ GUI を使用して実行できません。

アクセス ポイントの -U 規制ドメインへの移行（CLI）

ステップ 1 次のコマンドを入力して、ネットワーク内のどのアクセス ポイントが移行できるかを決定します。
show ap migrate

以下に類似した情報が表示されます。

```
These 1 APs are eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9 ap1240 "J" Reg. Domain

No APs have already been migrated.
```

ステップ 2 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 ポイントの国番号を変更して、J3 に移行します。
config country J3

ステップ 4 アクセス ポイントがリブートして、コントローラに再 join するのを待機します。

ステップ 5 次のコマンドを入力して、アクセス ポイントを -J 規制ドメインから -U 規制ドメインに移行します。
config ap migrate j52w52 {**all** | *ap_name*}

以下に類似した情報が表示されます。

```
Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
```

```
WARNING: All migrated APs must be promptly reported to the manufacturer.
Send the AP list and your company name to: abc@cisco.com

This AP is eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9 ap1240

Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n)
```

ステップ 6 移行の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 7 すべてのアクセス ポイントがリブートして、コントローラに再 join するまで待機します。 このプロセスは、アクセス ポイントによっては最長 15 分かかる場合があります。 AP1130、AP1200、および AP1240 は 2 回リブートします。それ以外のアクセス ポイントは 1 回リブートします。

ステップ 8 次のコマンドを入力して、すべてのアクセス ポイントの移行を確認します。
show ap migrate

以下に類似した情報が表示されます。

```
No APs are eligible for migration.

These 1 APs have already been migrated:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9 ap1240  "U" Reg. Domain
```

ステップ 9 次のコマンドを入力して、802.11a および 802.11b/g ネットワークを再び有効にします。
config 802.11a enable network

config 802.11b enable network

ステップ 10 会社名を記載した電子メールと移行済みのアクセス ポイントの一覧を、メール アドレス migrateapj52w52@cisco.com に送信します。 ステップ *8* の **show ap migrate** コマンドの出力を切り取り、電子メールに貼り付けることをお勧めします。

日本での W56 帯域の使用

日本政府は、802.11a 無線での W56 帯域周波数の無線 LAN 使用を正式に許可しています。 W56 帯域には、次のチャネル、周波数、および電力レベル（dBm）が含まれます。

チャネル	周波数（MHz）	AIR-LAP1132AG-Q-K9 の最大電力	AIR-LAP1242AG-Q-K9 の最大電力
100	5500	17	15
104	5520	17	15
108	5540	17	15
112	5560	17	15

チャネル	周波数（MHz）	AIR-LAP1132AG-Q-K9 の最大電力	AIR-LAP1242AG-Q-K9 の最大電力
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15
136	5680	17	15
140	5700	17	15

W56 帯域のチャネルはすべて、動的周波数選択（DFS）を必要とします。 日本国内では、W56 帯域は日本の DFS 規制の対象です。 現在、新しい 1130 および 1240 シリーズ アクセス ポイント SKU（プロダクト コードに -Q が付いているもの）のみが、AIR-LAP1132AG-Q-K9 および AIR-LAP1242AG-Q-K9 の要件をサポートします。

-P および -Q アクセス ポイントのみで構成されるネットワークを設定するには、国番号を J2 に設定します。 -P、-Q、および -U のアクセス ポイントで構成されるネットワークを設定するには、国番号を J3 に設定します。

動的周波数選択

Cisco UWN ソリューションは、無線デバイスがレーダー信号を検出して干渉しないようにする動的周波数選択（DFS）の使用を必須とする規制に準拠しています。

5GHz の無線を使用する Lightweight アクセス ポイントが次の表に示す 15 チャネルのいずれかで動作している場合、アクセスポイントがアソシエートするコントローラは、自動的にDFSを使用して動作周波数を設定します。

DFS 対応の 5GHz 無線用のチャネルを手動で選択した場合、コントローラはそのチャネルでのレーダー アクティビティを 60 秒間チェックします。 レーダー アクティビティが検出されない場合、アクセス ポイントは選択されたチャネル上で動作します。 選択されたチャネルでレーダー アクティビティが検出された場合、コントローラは自動的に別のチャネルを選択し、30 分後にアクセス ポイントはチャネルを再試行します。

（注） レーダーが DFS 有効チャネルで検出された後、30 分間は使用できません。

（注） 不正ロケーション検出プロトコル（RLDP）および不正の包含は、次の表に示すチャネルではサポートされていません。

（注） 適法な最大送信電力については、他のチャネルよりも5GHzチャネルの方が大きくなるものがあります。 電力が制限されている5GHzチャネルをランダムに選択した場合、コントローラはそのチャネルの電力制限に合うように送信電力を下げます。

表 *21*：*DFS* の有効な *5GHz* チャネル

52（5260MHz）	104（5520MHz）	124（5620MHz）
56（5280MHz）	108（5540MHz）	128（5640MHz）
60（5300MHz）	112（5560MHz）	132（5660MHz）
64（5320MHz）	116（5580MHz）	136（5680MHz）
100（5500MHz）	120（5600MHz）	140（5700MHz）

DFS の使用時、コントローラはレーダー信号の動作周波数を監視します。 チャネルでレーダー信号が検出された場合、コントローラは次の手順を実行します。

- アクセス ポイント チャネルを、それ以前の 30 分間にレーダー アクティビティが見られなかったチャネルに変更します （レーダー イベントは、30 分後にクリアされます）。コントローラは、ランダムにチャネルを選択します。
- 選択されたチャネルが上記の表に示したチャネルのいずれかである場合、新しいチャネルでレーダー信号を 60 秒間スキャンします。 新しいチャネルでレーダー信号が検出されない場合、コントローラはクライアントのアソシエーションを承認します。
- レーダーアクティビティが検出されたチャネルをレーダーチャネルとして記録し、そのチャネルでのアクティビティを 30 秒間回避します。
- トラップを生成し、ネットワーク マネージャに警告します。

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

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ネル（チャネル 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 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] をクリックして、変更を確定します。

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ネルを選択します。

（注） タグの監視対象となるチャネルは少なくとも 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。

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] をクリックして、変更を保存します。

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 「**save config**」と入力します。

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ネルがサポートされています。 少なくともチャネルを 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 **save config** コマンドを入力して、変更を保存します。

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

以下に類似した情報が表示されます。

```
AP Name           Ethernet MAC            Status           Scanning Channel List
-----------------  -------------------- ----------  ------------------------
AP1131:46f2.98ac       00:16:46:f2:98:ac        Tracking                1, 6, NA, NA
```

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

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、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
```

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

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 Wireless Controller"
PID: WS-C3750G-24PS-W24,  VID: V01,  SN: FLS0952H00F
```

- **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。

リンク テストの実行

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 テスト要求を発行し、クライアントは、応答パケットで受信した要求パケットの RF パラメータを記録します（受信信号強度インジケータ [RSSI]、信号対雑音比 [SNR] など）。 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） CCX は、AP1030 ではサポートされません。

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*

リンク遅延の設定

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の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 接続の可能性がある FlexConnect および OfficeExtend アクセス ポイントで役立ちます。

注意事項および制約事項

- 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 join 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 [disabled] 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*

TCP MSS の設定

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 クライアントへの TCP パケットと、データ パスのワイヤレス クライアントからの TCP パケットをチェックします。 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 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-adjust-mss {**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 **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、変更内容を反映するようコントローラをリブートします。
reset system

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      -
```

Power over Ethernet の設定

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。

注意事項および制約事項

- 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-W PoE 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。 15.4 W 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/epoe.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 *22*：*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）[5]		
				802.3af モード（15.4 W）	ePoE 電力最適化モード（16.8 W）	ePoE モード（20 W）

2.4 GHz	802.11b	1	—	20	20	20
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1 2	無効 有効（デフォルト）	17 無効	17 14（トランスミッタあたり 11）	17 20（トランスミッタあたり 17）
	802.11n MCS 8-15	2	—	無効	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 2	無効 有効（デフォルト）	17 無効	17 20（トランスミッタあたり 17）	17 20（トランスミッタあたり 17）
	802.11n MCS 8-15	2	—	無効	20（トランスミッタあたり 17）	20（トランスミッタあたり 17）

[5] 最大送信電力は、チャ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（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。 768 ビットは、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] をクリックして、変更を確定します。

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] または [802.11b/g/n] の順に選択して、[802.11a/n（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（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] をクリックして、変更を確定します。
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] をクリックして設定を保存します。

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 のイネーブル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て、[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） 手動でアクセス 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.
```

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 リリース 4.0 以降のリリースでは、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 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。

（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。

- 次のコマンドを入力して、コントローラを有効にして、コマンドを CLI からアクセス ポイントに送信します。

  debug ap enable *Cisco_AP*

- 次のコマンドを入力して、特定のアクセス ポイントの LED を指定した秒数間点滅させます。

  debug ap command "led flash *seconds*" *Cisco_AP*

  seconds パラメータには、1 ～ 3600 秒の値を入力できます。

- 次のコマンドを入力して、特定のアクセス ポイントの LED の点滅を無効にします。

  debug ap command "led flash disable" *Cisco_AP*

  このコマンドは、LED の点滅をただちに無効化します。 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。

クライアントの表示

コントローラの GUI または CLI を使用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ているクライアントに関する情報を表示できます。

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、802.11b、802.11g、または 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 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
- クライアントの認可ステータス
- 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 つまたは複数をオンにして、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オンにします。
- [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] をクリックして、変更を確定します。 [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*

  以下に類似した情報が表示されます。

```
MAC Address        AP Id      Status         WLAN Id  Authenticated
-----------------  ------  -------------  ---------  -------------
00:13:ce:cc:8e:b8     1         Associated           1          No
```

- 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

  以下に類似した情報が表示されます。

```
Number of Clients.............................. 1

MAC Address       AP Name           Status       WLAN/Guest-Lan Auth Protocol Port
Wired
----------------- ------------- ---------- --------------- ---- -------- ---- -----
00:13:02:2d:96:24  AP_1130            Associated           1      Yes  802.11a  1
   No
```

- 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*

  以下に類似した情報が表示されます。

```
Client MAC Address.............................. 00:40:96:b2:a3:44
Client Username ................................ N/A
AP MAC Address.................................. 00:18:74:c7:c0:90
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:18:74:c7:c0:9f
Channel......................................... 56
IP Address...................................... 192.168.10.28
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 0
```

```
Client CCX version.............................. 5
Client E2E version.............................. No E2E support
Diagnostics Capability.......................... Supported
S69 Capability.................................. Supported
Mirroring....................................... Disabled
QoS Level....................................... Silver
...
```

アクセス ポイントの LED 状態の設定

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。

注意事項および制約事項

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 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）

- コントローラにアソシエートされたすべてのアクセス ポイントの LED 状態を設定するには、次のコマンドを使用します。
  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*

第 9 章

メッシュ アクセス ポイントの制御

この章で説明する内容は、次のとおりです。

- Cisco Aironet メッシュ アクセス ポイントについて，602 ページ
- 注意事項および制約事項，603 ページ
- その他の関連資料，603 ページ
- アクセス ポイントのロール，603 ページ
- ネットワーク アクセス，604 ページ
- ネットワークのセグメント化，604 ページ
- Cisco 屋内メッシュ アクセス ポイント，604 ページ
- Cisco 屋外メッシュ アクセス ポイント，605 ページ
- メッシュ導入モード，606 ページ
- アーキテクチャの概要，611 ページ
- 設計上の考慮事項，612 ページ
- メッシュ アクセス ポイントのメッシュ ネットワークへの追加，621 ページ
- 拡張機能の設定，666 ページ
- 屋内アクセス ポイントのメッシュ アクセス ポイントへの変換，736 ページ
- 屋内メッシュ アクセス ポイントの非メッシュ Lightweight アクセス ポイントへの変換（1130AG、1240AG），739 ページ
- Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定，740 ページ

Cisco Aironet メッシュ アクセス ポイントについて

メッシュ ネットワーキングでは、スケーラブルで一元化された管理、および屋内展開と屋外展開間のモビリティを提供するために、Cisco Aironet 1500 シリーズ屋外メッシュ アクセス ポイントおよび屋内メッシュ アクセス ポイント（Cisco Aironet 1040、1130、1140、1240、1250、1260、3500e、および 3500i シリーズ アクセス ポイント）と Cisco ワイヤレス LAN コントローラおよび Cisco Prime Network Control System（NCS）が使用されます。 Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、ネットワークへのメッシュ アクセス ポイントの接続を管理します。

メッシュ ネットワーク内のエンドツーエンドのセキュリティは、ワイヤレス メッシュ アクセス ポイントと Wi-Fi Protected Access 2（WPA2）クライアントの間で Advanced Encryption Standard（AES; 高度な暗号化標準）の暗号化を採用することでサポートされています。 本書では、屋外ネットワークの設計時に考慮しなければならない無線周波数（RF）コンポーネントの概略についても説明しています。

コントローラ ソフトウェア リリース 7.0.116.0 以降のリリースでは、次の Cisco Aironet メッシュ アクセス ポイントがサポートされます。

- Cisco Aironet 1520 シリーズ屋外メッシュ アクセス ポイント：1522 デュアル無線メッシュ アクセス ポイントと 1524PS/シリアル バックホール マルチ無線メッシュ アクセス ポイントから構成されます。

（注） AP1130 および AP1240 は、屋内メッシュ アクセス ポイントとして動作するよう変換する必要があります。 屋内アクセス ポイントのメッシュ アクセス ポイントへの変換を参照してください。

- Cisco Aironet 1550 シリーズ屋外メッシュ アクセス ポイントは、次のモデルから構成されます。
  - 1552E
  - 1552C
  - 1552I
  - 1552H
  - 1552EU
  - 1552CU

7.0.98.0 リリースでは、屋内メッシュはデュアルバンド対応の Cisco Aironet 1130 および 1240 シリーズ アクセス ポイントで利用可能です。 7.0.116.0 リリースでは、屋内メッシュはデュアルバンド対応の 11n アクセス ポイント（Cisco Aironet 1040、1140、1250、1260、3500e、および 3500i シリーズ アクセス ポイント）で利用可能です。 メッシュ バックホール アクセスには 5 GHz が必要なため、屋内メッシュでは 802.11b/g のみのアクセス ポイントはサポートされません。

注意事項および制約事項

- この章で説明されているすべての機能は、特に記載のない限り、屋内メッシュ アクセス ポイント（1040、1140、1250、1260、3500）および屋外メッシュ アクセス ポイント（1500 シリーズ）に適用されます。 以降で、メッシュ アクセス ポイントまたは *MAP* は、屋内メッシュ アクセス ポイントと屋外メッシュ アクセス ポイントの両方について言及する場合に使用されます。
- Cisco Aironet 1505 および 1510 アクセス ポイントはこのリリースではサポートされていません。

その他の関連資料

関連項目	参照先
メッシュ アクセス ポイントの物理的な取り付けと初期設定	『*Cisco Aironet 1520 Series Outdoor Mesh Access Point Hardware Installation Guide*』 http://www.cisco.com/en/US/products/ps8368/tsd_products_support_series_home.html
稼働する屋内アクセスポイントをメッシュ アクセス ポイントとして変換	屋内アクセス ポイントのメッシュ アクセス ポイントへの変換
Cisco Aironet 1550 シリーズ屋外メッシュ アクセス ポイントの詳細	http://www.cisco.com/en/US/docs/wireless/technology/mesh/7.0MR1/design/guide/MeshAP_70MR1.html
メッシュ機能の概要、重要事項、および 4.1.19x.xx メッシュ リリースからコントローラ リリース 7.0.116.0 へのソフトウェア アップグレード手順	『*Release Notes for Cisco Wireless LAN controllers and Lightweight Access Points for Release 7.0.116.0*』 http://www.cisco.com/en/US/products/ps6366/prod_release_notes_list.html

アクセス ポイントのロール

メッシュ ネットワーク内のアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）のいずれかとして動作します。

RAP はコントローラへ有線で接続され、MAP はコントローラへ無線で接続されます。

MAP は MAP 間および RAP への通信に 802.11a 無線バックホールを使用して無線接続を行います。 MAP では Cisco Adaptive Wireless Path Protocol（AWPP）を使用して、他のメッシュ アクセス ポイントを介したコントローラへの最適なパスを決定します。

MAP と RAP との間にある考えられるすべてのパスが無線メッシュ ネットワークを形成します。

ネットワーク アクセス

無線メッシュ ネットワークでは同時に 2 つの異なるトラフィック タイプ（無線 LAN クライアント トラフィックおよび MAP イーサネット ポート トラフィック）が伝送されます。

無線LANクライアントトラフィックはコントローラで終端し、イーサネット トラフィックはメッシュ アクセス ポイントのイーサネット ポートで終端します。

メッシュ アクセス ポイントでのワイヤレス LAN メッシュへのアクセスは次の認証方法で管理されます。

- MAC 認証：メッシュ アクセス ポイントがデータベースに追加され、特定のコントローラおよびメッシュ ネットワークに確実にアクセスできるようにします。 屋内アクセス ポイントのメッシュ アクセス ポイントへの変換の項を参照してください。
- 外部 RADIUS 認証：メッシュ アクセス ポイントが、証明書を使用する EAP-FAST のクライアント認証タイプをサポートする Cisco ACS 4.1 以降のリリースなどの RADIUS サーバを使用することを外部的に許可できます。 RADIUS サーバの設定の項を参照してください。

ネットワークのセグメント化

メッシュ アクセス ポイント用のワイヤレス LAN メッシュ ネットワークへのメンバーシップは、ブリッジ グループ名（BGN）によって制御されます。 メッシュ アクセス ポイントは、類似のブリッジグループに配置して、メンバーシップを管理したり、ネットワーク セグメンテーションを提供したりすることができます。 「アンテナ ゲインの設定」の項を参照してください。

Cisco 屋内メッシュ アクセス ポイント

7.3 リリースでは、屋内メッシュは、2600 シリーズのアクセス ポイントで使用可能です。

7.2 リリースでは、屋内メッシュは、3600 シリーズのアクセス ポイントで使用可能です。

7.0.116.0 リリースでは、屋内メッシュは 802.11n アクセス ポイント（Cisco Aironet 1040、1140、1250、1260、3500e、および 3500i シリーズ アクセス ポイント）でも利用可能です。

7.0 リリースでは、屋内メッシュは Cisco Aironet 1130 および 1240 シリーズ アクセス ポイントで利用可能です。

エンタープライズ 11n メッシュは、802.11n アクセス ポイントで動作するために CUWN 機能に追加される拡張機能です。 エンタープライズ 11n メッシュ機能は 802.11n 以外のメッシュと互換性がありますが、バックホールとクライアントのアクセス速度が向上します。 802.11n 屋内アクセス ポイントは、特定の屋内展開用のデュアル無線 Wi-Fi インフラストラクチャ デバイスです。 一方の無線をアクセス ポイントのローカル（クライアント）アクセスに使用でき、もう一方の無線をワイヤレス バックホールに対して設定できます。 バックホールは、5 GHz 無線でのみサポート

されます。エンタープライズ 11n メッシュは、P2P、P2MP、およびアーキテクチャのメッシュ タイプをサポートします。

屋内アクセス ポイントをブリッジモードに直接設定して、これらのアクセス ポイントをメッシュ アクセス ポイントとして直接使用できます。 これらのアクセス ポイントがローカル モード（非メッシュ）である場合は、これらのアクセス ポイントをコントローラに接続し、AP モードをブリッジモード（メッシュ）に変更する必要があります。 このシナリオは、特に、展開されるアクセス ポイントの量が大きく、アクセス ポイントが従来の非メッシュ ワイヤレス カバレッジに対してローカル モードですでに展開されている場合に、煩雑になります。

Cisco 屋内メッシュ アクセス ポイントでは、次の 2 つの無線が同時に動作します。

- クライアント アクセスに使用される 2.4 GHz の無線
- データ バックホールに使用される 5 GHz の無線

5 GHz の無線は、5.15 GHz、5.25 GHz、5.47 GHz、および 5.8 GHz の帯域をサポートします。

Cisco 屋外メッシュ アクセス ポイント

Cisco 屋外メッシュ アクセス ポイントは、Cisco Aironet 1500 シリーズ アクセス ポイントから構成されます。 1500 シリーズには、1552 11n 屋外メッシュ アクセス ポイント、1522 デュアル無線メッシュ アクセス ポイント、および 1524 マルチ無線メッシュ アクセス ポイントが含まれます。1524 には次のような 2 つのモデルがあります。

- Public Safety モデルの 1524PS
- シリアル バックホール モデルの 1524SB

（注） 6.0 リリースでは、AP1524SB アクセス ポイントは、A、C、および N のドメインで使用されていました。 7.0 リリースでは、AP1524SB アクセス ポイントは、-E、-M、-K、-S、および -T のドメインでも使用されます。

Cisco 1500 シリーズ メッシュ アクセス ポイントは、ワイヤレス メッシュ展開の中核的なコンポーネントです。 AP1500 は、コントローラ（GUI および CLI）と Cisco WCS の両方により設定されます。 屋外メッシュ アクセス ポイント（MAP および RAP）間の通信は、802.11a/n 無線バックホールを介します。 一般的に、クライアント トラフィックは、802.11b/g/n 無線（802.11a/n がクライアント トラフィックを受け入れるよう設定することもできます）を介して伝送され、Public Safety トラフィック（AP1524PS のみ）は 4.9 GHz 無線を介して伝送されます。

メッシュ アクセス ポイントは、有線ネットワークに直接接続されていない他のアクセス ポイントの中継ノードとしても動作します。 インテリジェントな無線ルーティングは Adaptive Wireless Path Protocol（AWPP）によって提供されます。 このシスコのプロトコルを使用することで、各メッシュ アクセス ポイントはネイバー アクセス ポイントを識別し、パスごとに信号の強度とコントローラへのアクセスに必要なホップ カウントについてコストを計算して、有線ネットワークまでの最適なパスをインテリジェントに選択できるようになります。

AP1500 には、ケーブルありとケーブルなしの 2 つの異なる構成があります。

- ケーブル構成は、ケーブルより線に取り付け可能であり、Power-Over-Cable（POC）をサポートします。
- ケーブルなし構成は、複数のアンテナをサポートします。 この構成は、柱や建物壁面に取り付け可能で、電源関連のオプションをいくつか用意しています。

アップリンク サポートには、ギガビット イーサネット（1000BASE-T）と、ファイバまたはケーブル モデム インターフェイスに接続できる小型フォーム ファクタ（SFP）スロットが含まれます。 1000BASE-BX までのシングルモード SFP とマルチモード SFP の両方がサポートされます。 メッシュ アクセス ポイントのタイプに基づき、ケーブル モデムは DOCSIS 2.0 または DOCSIS/EuroDOCSIS 3.0 になります。

AP1500 は、危険な場所用ハードウェア格納ラックに設置します。 危険場所対応の AP1500 は、Class I、Division 2、Zone 2 の危険場所での安全基準を満たしています。

（注） モデル別の電源、取り付け、アンテナ、および規制対応については、『*Cisco Aironet 1520 Series Lightweight Outdoor Access Point Ordering Guide*』（http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/product_data_sheet0900aecd8066a157.html）を参照してください。

メッシュ導入モード

メッシュ アクセス ポイントは次のような複数の導入モードをサポートしています。

- 無線メッシュ
- ワイヤレス バックホール
- ポイントツーマルチポイント無線ブリッジング
- ポイントツーポイント無線ブリッジング

ワイヤレス メッシュ ネットワーク

Cisco のワイヤレス屋外メッシュ ネットワークでは、複数のメッシュ アクセス ポイントによって、安全でスケーラブルな屋外ワイヤレス LAN を提供するネットワークが構成されます。

それぞれの場所で、3 つの RAP が有線ネットワークに接続され、建物の屋根に配置されています。 すべてのダウンストリーム アクセス ポイントは、MAP として動作し、ワイヤレス リンク（表示されていません）を使用して通信します。

MAP と RAP の両方共、WLAN クライアント アクセスを提供できますが、RAP の場所がクライアント アクセスの提供には向いていないことがよくあります。

メッシュ アクセス ポイントから CAPWAP セッションを終端させるオンサイト コントローラがある建物もありますが、CAPWAP セッションはワイドエリア ネットワーク（WAN）を介してコントローラにバックホールできるため、それは必須要件ではありません

ワイヤレス バックホール

Cisco ワイヤレス バックホール ネットワークでは、トラフィックを MAP と RAP の間でブリッジできます。このトラフィックは、ワイヤレスメッシュによってブリッジされている有線デバイスからのトラフィックか、メッシュ アクセス ポイントからの CAPWAP トラフィックになります。このトラフィックは、ワイヤレス バックホールなどのワイヤレス メッシュ リンクを通るときに必ず AES 暗号化されます。

AES 暗号化は、他のメッシュ アクセス ポイントと共に、メッシュ アクセス ポイントにおけるネイバー同士の関係として確立されます。メッシュ アクセス ポイント間で使用される暗号キーは、EAP 認証プロセス中に生成されます。

2.4 または 5 GHz 無線をバックホール無線として設定できる 1522 を除くすべてのメッシュ アクセス 5 GHz バックホールだけが可能です（拡張機能の設定を参照）。

ユニバーサル アクセス

802.11a 無線を介してクライアント トラフィックを受け入れるようメッシュ アクセス ポイントでバックホールを設定できます。この機能は、コントローラの GUI の Backhaul Client Access（[Monitor] > [Wireless]）で識別できます。この機能が無効な場合、バックホール トラフィックは 802.11a または 802.11a/n 無線を介してのみ伝送され、クライアント アソシエーションは 802.11b/g または 802.11b/g/n 無線を介してのみ許可されます。設定の詳細については拡張機能の設定の項を参照してください。

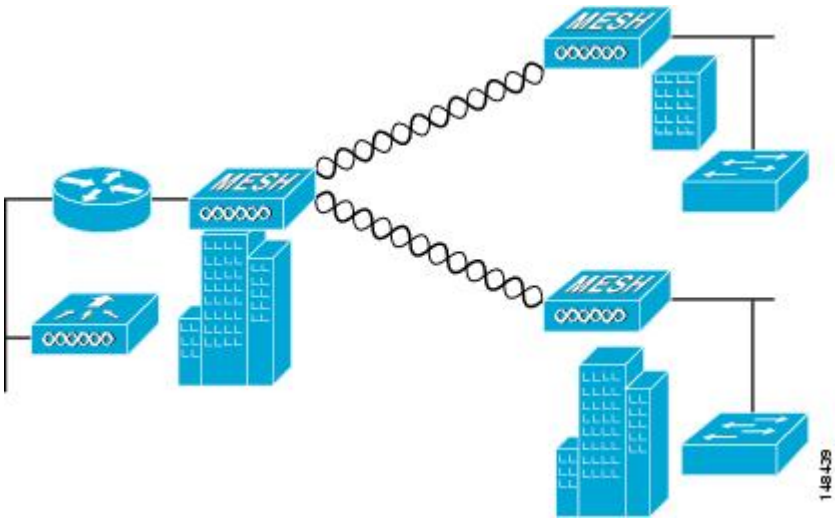
ポイントツーマルチポイント無線ブリッジング

ポイントツーマルチポイント ブリッジング シナリオでは、ルート ブリッジとして機能する RAP が、アソシエートされた有線 LAN を使用して複数の MAP を非ルート ブリッジとして接続します。デフォルトでは、この機能はすべての MAP に対して無効になっています。イーサネット ブリッジングを使用する場合、各 MAP および RAP のコントローラでイーサネット ブリッジングをイネーブルにする必要があります。

次の図は、1 つの RAP と 2 つの MAP がある単純な導入を示していますが、この構成は基本的に WLAN クライアントがないワイヤレス メッシュです。イーサネット ブリッジングを有効にする

ことでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアント アクセスに適していないことがあります。

図 *57*：ポイントツーマルチポイント ブリッジングの例

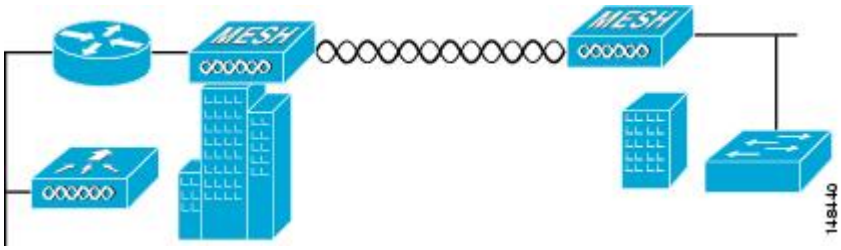


ポイントツーポイント無線ブリッジング

ポイントツーポイントブリッジング シナリオでは、バックホール無線を使用してスイッチド ネットワークの 2 つのセグメントをブリッジ接続することにより、1500 シリーズ メッシュ AP を使用してリモート ネットワークを拡張できます。 これは基本的には、1 つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。 ポイントツーマルチポイント ネットワークと同様に、イーサネットブリッジングを有効にすることでクライアントアクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。

イーサネットブリッジドアプリケーションを使用する場合は、RAP およびそのセグメント内のすべての MAP でブリッジング機能を有効にすることをお勧めします。 MAP のイーサネット ポートに接続されたすべてのスイッチで VLAN Trunking Protocol（VTP）を使用していないことを確認する必要があります。 VTP によってメッシュ全体のトランキングされた VLAN が再設定される場合があるので、プライマリ WLC と RAP 間の接続が失われることがあります。 設定が正しくないと、メッシュ導入がダウンすることがあります。

図 *58*：ポイントツーポイント無線ブリッジングの例



セキュリティ上の理由により、デフォルトでは MAP のイーサネット ポートは無効になっています。 有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定する必要があります。

イーサネット ブリッジングは、次の 2 つの場合に有効にする必要があります。

1 メッシュ ノードをブリッジとして使用する場合。

2 MAP でイーサネット ポートを使用してイーサネットデバイス（ビデオ カメラなど）を接続する場合。

該当するメッシュ AP からコントローラへのパスを取る各親メッシュ AP に対してイーサネット ブリッジングを有効にします。 たとえば、Hop 2 の MAP2 でイーサネット ブリッジングを有効にする場合は、MAP1（親 MAP）と、コントローラに接続している RAP でもイーサネット ブリッジングを有効にする必要があります。

[Wireless]>[Mesh] タブで長いリンクに対してレンジパラメータを設定する必要があります。 ルートアクセスポイント（RAP）と最遠のメッシュアクセスポイント（MAP）間に最適な距離（フィート単位）が存在します。 RAP ブリッジから MAP ブリッジまでのレンジは、フィート単位で記述する必要があります。

ネットワーク内のコントローラと既存のすべてのメッシュ アクセス ポイントに join する場合は、次のグローバル パラメータがすべてのメッシュ アクセス ポイントに適用されます。

レンジ：150 ～ 132,000 フィート

デフォルト：12,000 フィート

メッシュ レンジの設定（CLI）

- ブリッジングを行うノード間の距離を設定するには、次のコマンドを入力します。

  config mesh range *range-in-feet*

- メッシュ レンジを取得するには、次のコマンドを入力します。

  show mesh config

  次のような情報が表示されます。

```
Mesh Range....................................... 12000
Mesh Statistics update period.................... 3 minutes
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
Backhaul Amsdu State............................. disabled

Mesh Security
Security Mode.................................... EAP
External-Auth.................................... disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled

Mesh Alarm Criteria
Max Hop Count.................................... 4
Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20
Low Link SNR..................................... 12
High Link SNR.................................... 60
Max Association Number........................... 10
```

```
Association Interval.......................... 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval........................ 60 minutes

Mesh Multicast Mode............................... In-Out
Mesh Full Sector DFS.............................. enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

（注） レンジの指定後に、AP はリブートされます。

レンジを推測するために、次の URL で利用可能なレンジ計算ツールを使用できます。

- Cisco 1520 シリーズ屋外メッシュ レンジ計算ユーティリティ：http://www.cisco.com/en/US/products/ps8368/products_implementation_design_guides_list.html
- 1550 シリーズ屋外メッシュ アクセス ポイント用範囲カルキュレータ：http://www.cisco.com/en/US/products/ps11451/products_implementation_design_guides_list.html

AP1522 レンジ計算ツールの前提条件

- 一覧表示された規制ドメインの送信電力およびEIRPの制限内に収まるようAP1522 レンジ計算ツールが編集されています。 この制限を超える場合があります。 取り付けは、取り付ける地域の法律に従って行う必要があります。
- AP1522 レンジ計算ツールを使用する場合に、規制ドメイン、選択されたアンテナ（またはアンテナ ゲイン）、および選択されたデータ レートに基づく変調モード（一部の区域ではOFDM で低い電力レベルが必要です）に基づいて、利用可能な電力レベルが変わります。 パラメータの変更後にすべてのパラメータを確認する必要があります。
- 2.4 GHz の受信感度は、3 つのすべての受信パスの複合感度です。 つまり、MRC が 2.4 GHz に含まれます。 5 GHz には 1 つの受信しか存在しません。
- アクセス ポイントで認定されたチャネルのみを選択できます。
- 有効な電力レベルのみを選択できます。

AP1552 レンジ計算ツールの前提条件

- 一覧表示された規制ドメインの送信電力およびEIRPの制限内に収まるようAP1552 レンジ計算ツールが編集されています。 この制限を超える場合があります。 取り付けは、取り付ける地域の法律に従って行う必要があります。
- 効果的なパフォーマンスを実現するために、1552 の外部アンテナ モデルに対して 3 つのすべてのアンテナ ポートを使用する必要があります。 使用しない場合は、レンジが大幅に減少します。 1552 無線には、2 つの送信パスと 3 つの受信パスがあります。
- 送信電力は、両方の送信パスの総複合電力です。
- 受信感度は、3 つのすべての受信パスの複合感度です。 つまり、MRC が含まれます。

- AP1552 レンジ計算ツールでは、ClientLink（ビームフォーミング）がオンになっていることを前提とします。
- AP1552 レンジ計算ツールを使用する場合に、規制ドメイン、選択されたアンテナ（またはアンテナ ゲイン）、および選択されたデータ レートに基づいて、利用可能な電力レベルが変わります。 パラメータの変更後にすべてのパラメータを確認する必要があります。
- デフォルトで利用可能な 2 つとは異なるアンテナを選択できます。 高ゲイン アンテナを入力し、EIRP 制限を超える電力を選択した場合は、警告が表示され、範囲が 0 になります。
- アクセス ポイントで認定されたチャネルのみを選択できます。
- 有効な電力レベルのみを選択できます。

アーキテクチャの概要

ワイヤレス アクセス ポイントの制御およびプロビジョニング（CAPWAP）

CAPWAP は、ネットワーク内のアクセス ポイント（メッシュおよび非メッシュ）を管理するためにコントローラで使用されるプロビジョニングおよび制御プロトコルです。 コントローラのソフトウェア リリース 5.2 以降では、LWAPP の代わりにこのプロトコルを使用します。

Cisco Adaptive Wireless Path Protocol ワイヤレス メッシュ ルーティング

Cisco Adaptive Wireless Path Protocol（AWPP）は、無線メッシュ ネットワーキング専用に設計されています。 AWPP では、リンクの品質とホップ数に基づいてパスが決定されます。

また、AWPP の重要な要素として、展開の容易さ、高速コンバージェンス、最低限のリソース消費があります。

AWPP の目的は、RAP のブリッジ グループの一部である各 MAP から RAP への最適なパスを検出することです。 これを実行するため、MAP はネイバー MAP をアクティブに要請メッセージを送信します。 要請メッセージのやり取りの際に、MAP は RAP への接続に使用可能なネイバーをすべて学習し、最適なパスを提供するネイバーを決定して、そのネイバーと同期します。

メッシュ ネイバー、親、および子

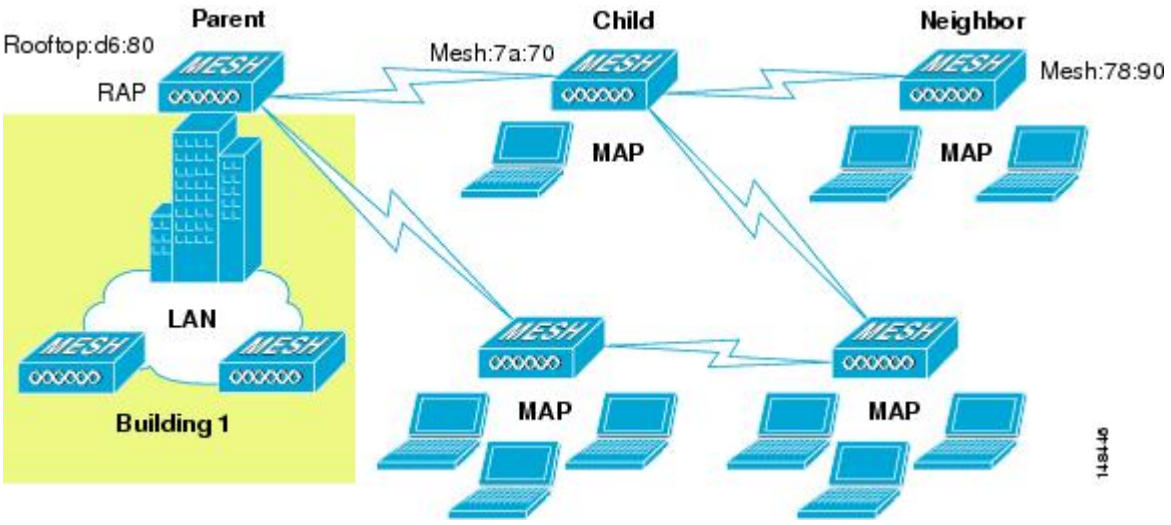
メッシュ ネットワークにおけるアクセス ポイント間の関係は、次のように親、子、またはネイバーとして分類されます。

- 親アクセス ポイントは、容易度の値（ease value）に基づいて RAP への最適なルートを提供します。 親は RAP 自身または別の MAP のいずれかです。 容易度の値（ease value）は各ネ

イバーの SNR およびリンク ホップ値を用いて計算されます。 複数の選択肢がある場合は、容易度の値（ease value）の高いアクセス ポイントが選択されます。

- 子アクセス ポイントは、RAP に戻る最適なルートとして親アクセス ポイントを選択します。
- ネイバー アクセス ポイントは、別のアクセス ポイントの無線周波数（RF）の範囲内にありますが、容易度の値（ease value）が親よりも低いため、親または子として選択されません。

図 *59*：親、子、およびネイバー アクセス ポイント



設計上の考慮事項

屋外のワイヤレス メッシュの導入はそれぞれが独自のため、利用できる場所や障害物、利用可能なネットワーク インフラストラクチャに伴い、環境ごとに課題が異なります。 主要な設計要件には、想定されるユーザ、トラフィック、および可用性のニーズによって決まる設計基準もあります。 この項では、設計上の重要な考慮事項について説明し、ワイヤレス メッシュの設計例を示します。

無線メッシュの制約

ワイヤレス メッシュ ネットワークを設計および構築する場合に考慮すべきシステムの特徴は次のとおりです。 これらの一部の特徴はバックホール ネットワークの設計に適用され、残りの特徴は CAPWAP コントローラの設計に適用されます。

ワイヤレス バックホール データ レート

バックホールは、アクセス ポイント間でワイヤレス接続のみを作成するために使用されます。 バックホール インターフェイスは、アクセス ポイントに基づいてデフォルトで 802.11a または

802.11a/n になります。 利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。また、レートはクライアントデバイスのスループットにも影響を与えることがあり、スループットはベンダー デバイスを評価するために業界出版物で使用される重要なメトリックです。

Dynamic Rate Adaptation（DRA）には、パケット伝送のために最適な伝送レートを推測するプロセスが含まれます。 レートを正しく選択することが重要です。 レートが高すぎると、パケット伝送が失敗し、通信障害が発生します。 レートが低すぎると、利用可能なチャネル帯域幅が使用されず、品質が低下し、深刻なネットワーク輻輳および障害が発生する可能性があります。

データ レートは、RF カバレッジとネットワーク パフォーマンスにも影響を与えます。 低データ レート（6 Mbps など）が、高データ レート（300 Mbps など）よりもアクセス ポイントからの距離を延長できます。 結果として、データ レートはセル カバレッジと必要なアクセス ポイントの数に影響を与えます。 異なるデータ レートは、ワイヤレス リンクで冗長度の高い信号を送信することにより（これにより、データをノイズから簡単に復元できます）、実現されます。 1 Mbps のデータ レートで 1 つのパケットに対して送信される記号の数は、11 Mbps で同じパケットに対して使用される記号の数よりも多くなります。 したがって、低ビット レートでのデータの送信には、高ビット レートでの同じデータの送信よりも時間がかり、スループットが低下します。

低ビット レートでは、MAP 間の距離を長くすることが可能になりますが、WLAN クライアント カバレッジにギャップが生じる可能性が高く、バックホール ネットワークのキャパシティが低下します。 バックホール ネットワークのビット レートを増加させる場合は、より多くの MAP が必要となるか、MAP 間の SNR が低下し、メッシュの信頼性と相互接続性が制限されます。 無線バックホール データ レートの設定の詳細については、次の表を参照してください。

（注） データ レートは、AP ごとにバックホールで設定できます。 これはグローバル コマンドではありません。

表 *23*：バックホールのデータ レートと *LinkSNR* の最小要件

802.11a データ レート（Mbps）	必要な最小 LinkSNR（dB）
54	31
48	29
36	26
24	22
18	18
12	16
9	15
6	14

- LinkSNR の必要最小値は、データ レートと次の公式で決まります：最小 *SNR* + フェードマージン。
  - 最小 SNR は、干渉とノイズがなく、システムのパケット エラー レート（PER）が 10 % 未満の理想的な状態における値です。
  - 一般的なフェード マージンは約 9 ～ 10 dB です。

表 *24*：データ レート別の必要最小 *LinkSNR* の計算

802.11n データ レート（Mbps）	最小 SNR（dB）+	フェード マージン =	必要な最小 LinkSNR（dB）
6	5	9	14
9	6	9	15
12	7	9	16
18	9	9	18
24	13	9	22
36	17	9	26

- 必要最小リンク SNR を計算するために MRC の効果を考慮する場合。

  LinkSNR = 最小 *SNR - MRC* + フェード マージン（*9 dB*）

次の表に、3 Rx アンテナ（MRC ゲイン）と AP1552 および 1522 の 802.11a/g（2.4 GHz および 5 GHz）用必要リンク SNR を示します。

表 *25*：*802.11a/g* 用必要リンク *SNR* の計算

802.11a/g MCS（Mbps）	変調	最小 SNR（dB）	3 RX からの MRC ゲイン（dB）	フェード マージン（dB）	必要リンク SNR（dB）
6	BPSK 1/2	5	4.7	9	9.3
9	BPSK 3/4	6	4.7	9	10.3
12	QPSK 1/2	7	4.7	9	11.3
18	QPSK 3/4	9	4.7	9	13.3
24	16QAM 1/2	13	4.7	9	17.3
36	16QAM 3/4	17	4.7	9	21.3

802.11a/g MCS（Mbps）	変調	最小 SNR（dB）	3 RX からの MRC ゲイン（dB）	フェード マージン（dB）	必要リンク SNR（dB）
48	64QAM 2/3	20	4.7	9	24.3
54	64QAM 3/4	22	4.7	9	26.3

次の表に、2.4 および 5 GHz の AP1552 とリンク SNR 要件を示します。

表 *26*：*AP1552* の *2.4* および *5 GHz* 用リンク *SNR* の要件

空間ストリーム数	11n MCS	変調	最小 SNR（dB）	3 RX からの MRC ゲイン（dB）	フェードマージン（dB）	リンク SNR (dB)
1	MCS 0	BPSK 1/2	5	4.7	9	9.3
1	MCS 1	QPSK 1/2	7	4.7	9	11.3
1	MCS 2	QPSK 3/4	9	4.7	9	13.3
1	MCS 3	16QAM 1/2	13	4.7	9	17.3
1	MCS 4	16QAM 3/4	17	4.7	9	21.3
1	MCS 5	64QAM 2/3	20	4.7	9	24.3
1	MCS 6	64QAM 3/4	22	4.7	9	26.3
1	MCS 7	64QAM 5/6	23	4.7	9	27.3
2	MCS 8	BPSK 1/2	5	1.7	9	12.3
2	MCS 9	QPSK 1/2	7	1.7	9	14.3
2	MCS 10	QPSK 3/4	9	1.7	9	16.3
2	MCS 11	16QAM 1/2	13	1.7	9	20.3
2	MCS 12	16QAM 3/4	17	1.7	9	24.3
2	MCS 13	64QAM 2/3	20	1.7	9	27.3
2	MCS 14	64QAM 3/4	22	1.7	9	29.3
2	MCS 15	64QAM 5/6	23	1.7	9	30.3

（注） 2 つの空間ストリームの場合、MRC ゲインは半分になります。つまり、MRC ゲインは 3 dB 少なくなります。 これは、システムに 10 ログ（3/1 SS）ではなく 10 ログ（3/2 SS）があるためです。 3 つの受信器で 3 SS がある場合は、MRC ゲインがゼロになります。

- バックホールのホップ数は最大 8 ですが、3 ～ 4 にすることをお勧めします。

  ホップ数は 3 か 4 に制限して、主に、十分なバックホール スループットを維持することをお勧めします。これは、各メッシュ アクセス ポイントはバックホール トラフィックの伝送と受信に同じ無線を使用するためです（つまり、スループットはホップごとに約半分になります）。 たとえば、24 Mbps の最大スループットは、最初のホップで約 14 Mbps、2 番目のホップで 9 Mbps、3 番目のホップで 4 Mbps になります。

- RAP ごとの MAP 数

  RAP ごとに設定できる MAP 数について、現在ソフトウェアによる制限はありません。 ただし、1 台の RAP につき 20 台の MAP に数を制限することをお勧めします。

- コントローラ数

  - モビリティ グループごとのコントローラ数は 72 に制限されます。

- コントローラごとにサポートされるメッシュ アクセス ポイントの数。

ClientLink テクノロジー

多くのネットワークは、依然として 802.11a/g クライアントと 802.11n クライアントの混在をサポートします。 802.11a/g クライアント（レガシー クライアント）は低データ レートで動作するため、古いクライアントにより、ネットワーク全体のキャパシティが減少することがあります。シスコの ClientLink テクノロジーは、802.11a/g クライアントが、特にセル境界に近い場合に、最適なレートで動作できるようにすることで、クライアントが混在するネットワークにおける 802.11n の採用に関連する問題を解決します。

高度な信号処理が Wi-Fi チップセットに追加されました。 複数の送信アンテナが 802.11a/g クライアントの方向に伝送を収束するために使用され、ダウンリンクの信号対ノイズ比と一定のレンジにおけるデータ レートが増加するため、カバレッジ ホールが減少し、システム全体のパフォーマンスが向上します。 このテクノロジーは、クライアントから受信された信号を合成する最適な方法を学習し、この情報を使用してパケットを最適な方法でクライアントに送り返します。 このテクニックは、MIMO（複数入力複数出力）ビームフォーミング、送信ビームフォーミング、またはコフェージングとも呼ばれ、高価なアンテナ アレイを必要としない、市場で唯一のエンタープライズクラスかつサービス プロバイダークラスのソリューションです。

802.11n システムは、複数の無線信号を同時に送信することによりマルチパスを利用します。 空間ストリームと呼ばれるこれらの各信号は、独自のトランスミッタを使用して独自のアンテナから送信されます。 これらのアンテナ間には空間があるため、各信号は受信装置への若干異なるパスに従います（空間ダイバーシティと呼ばれる状況）。 レシーバにも、独自の無線を使用する複数のアンテナがあります。各アンテナは受信した信号を独自にデコードし、各信号は他のレシー

バの無線からの信号と結合されます。 その結果、複数のデータ ストリームが同時に受信されます。 これにより、以前の 802.11a/g システムよりも高いスループットが実現されますが、信号を解読する 802.11n 対応クライアントが必要になります。 したがって、AP とクライアントの両方がこの機能をサポートする必要があります。 問題が複雑であるため、第 1 世代のメインストリーム 802.11n チップセットでは、AP およびクライアント チップセットで 802.11n 送信ビームフォーミングが実装されていません。 したがって、802.11n 標準伝送ビームフォーミングは将来利用可能になりますが、次世代のチップセットが市場に出るまで待つ必要があります。 シスコは、この分野の発展をリードしていく所存です。

現在の世代の 802.11n AP の場合、2 番目の送信パスは 802.11n クライアントに対して（空間ダイバーシティを実装するために）使用されますが、802.11a/g クライアントに対して完全には使用されません。 802.11 a/g クライアントの場合は、追加の送信パスの一部の機能がアイドル状態になります。 また、多くのネットワークで、取り付けられた 802.11 a/g クライアント ベースのパフォーマンスが、ネットワークの制限要因となります。

ClientLink は高度な信号処理手法と複数の送信パスを使用して、ダウンリンク方向で 802.11a/g クライアントが受信した信号を、フィードバックを必要とせずに、最適化します。 特別なフィードバックが必要ないため、Cisco ClientLink は、既存のすべての 802.11a/g クライアントで動作します。

Cisco ClientLink テクノロジーにより、クライアントが配置された場所でアクセス ポイントが SNR を効果的に最適化できるようになります。 ClientLink は、ダウンリンク方向にほぼ 4 dB のゲインを提供します。 SNR が改善され、再試行回数の減少やデータ レートの向上などの多くの利点が提供されます。 たとえば、以前に 12 Mbps でパケットを受信できたセルの端にあるクライアントが 36 Mbps でパケットを受信できるようになります。 ClientLink を使用した場合のダウンリンク パフォーマンスの一般的な測定値は、802.11a/g クライアントではスループットが 65 % 向上します。 Wi-Fi システムがより高いデータ レート、少ない再試行回数で動作できるようにすることで、ClientLink はシステムのキャパシティ全体を拡張します。つまり、スペクトル リソースを効率的に利用できます。

1552 アクセス ポイントの ClientLink は、AP3500 で使用可能な ClientLink 機能をベースにしています。 したがって、アクセス ポイントは近接するクライアントに対してビームフォーミングを行い、802.11ACK でビームフォーミング情報を更新できます。 したがって、専用アップリンク トラフィックがない場合でも、ClientLink は適切に動作します。これは、TCP および UDP 両方のトラフィック ストリームに有用です。 Cisco 802.11n アクセス ポイントでこのビーム形成を使用するためにクライアントが通過する必要がある RSSI ウォーターマークはありません。

ClientLink は、同時に 15 のクライアントにビーム形成を行うことができます。 したがって、レガシー クライアントの数が無線ごとに 15 を超える場合に、ホストは最良の 15 クライアントを選択する必要があります。 AP1552 には 2 つの無線があるため、タイム ドメインで最大 30 個のクライアントに対してビームフォーミングを行えます。

ClientLink は、屋内および屋外 802.11n アクセス ポイント用の 11a/g レート（11b ではない）を示す、パケットのレガシー OFDM 部分に適用されますが、屋内 11n 用の ClientLink と屋外 11n 用の ClientLink には 1 つの違いがあります。 屋内 11n アクセス ポイントの場合、SW は影響を受けるレートを 24、36、48、54 Mbps に制限します。 これは、屋内環境の遠くの AP にクライアントが接続し続けることを避けるためです。 また、スループット ゲインが非常に小さいため、SW によって ClientLink が 11n クライアント用のレートで動作できなくなります。 ただし、純粋なレガシー クライアントに対しては明らかなゲインがあります。 屋外 11n アクセス ポイントでは、24

Mbps 未満の 3 つの追加レガシー データ レートが追加されました。 屋外用 ClientLink は、9、12、18、24、36、48、および 54 Mbps のレガシー データ レートに適用できます。

ClientLink の設定（CLI）

7.2 リリース以降から、コントローラ GUI を使用して ClientLink（ビーム形成）を設定することはできません。

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、802.11a または 802.11g ネットワーク上でビーム形成をグローバルにイネーブルまたはディセーブルにします。
config {802.11a | 802.11b} beamforming global {enable | disable}

デフォルト値は [disabled] です。

（注） ネットワーク上でビーム形成をイネーブルにすると、そのネットワーク タイプに該当するすべての無線で自動的に有効になります。

ステップ 3 次のコマンドを入力して、グローバル設定をオーバーライドして、特定のアクセス ポイントのビーム形成をイネーブルまたはディセーブルにします。
config {802.11a | 802.11b} beamforming ap *Cisco_AP* **{enable | disable}**

デフォルトの値は、ネットワーク上でビームフォーミングが無効である場合はディセーブル、ネットワーク上でビーム形成が有効である場合はイネーブルになります。

ステップ 4 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

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、ネットワークのビームフォーミング 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。

```
802.11a Network.............................. Enabled
11nSupport................................... Enabled
802.11a Low Band..................... Enabled
802.11a Mid Band..................... Enabled
802.11a High Band.................... Enabled
...
Pico-Cell-V2 Status.......................... Disabled
TI Threshold................................. -50
Legacy Tx Beamforming setting................ Enabled
```

ステップ 7 次のコマンドを入力して、特定のアクセス ポイントのビーム形成ステータスを表示します。
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.............................. 14
Cisco AP Name.................................... 1250-1
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-A     802.11a:-A
...
Phy OFDM parameters
Configuration ............................... AUTOMATIC
Current Channel ............................. 149
Extension Channel ........................... NONE
Channel Width................................ 20 Mhz
Allowed Channel List........................ 36,40,44,48,52,56,60,64,100,
.......................................... 104,108,112,116,132,136,140,
.......................................... 149,153,157,161,165
TI Threshold ................................ -50
Legacy Tx Beamforming Configuration ....... CUSTOMIZED
Legacy Tx Beamforming ..................... ENABLED
```

ClientLink に関連するコマンド

- 次のコマンドを AP コンソールで入力します。
  - AP のビーム形成のステータスを確認するには、**show controller d0/d1** コマンドを入力します。
  - AP rbf テーブルでクライアントを見つけるには、**show interface dot110** コマンドを入力します。
  - AP に割り当てられたビーム形成レートを確認するには、**debug d0 trace print rates** コマンドを入力します。
- トラブルシューティングを行うには、AP コンソールで次のコマンドを使用します。
  - 無線で ClientLink が有効であることを示すには、**show controllers | inc Beam** コマンドを入力します。

    次のような出力が表示されます。

    ```
    Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -50 dBm
    Legacy Beamforming: Configured Yes, Active Yes, RSSI Threshold -60 dBm
    ```

  - ClientLink が特定のクライアントにビーム形成を行っていることを表示するには、**show interface dot11radio 1 lbf rbf** コマンドを入力します。

    次のような出力が表示されます。

    ```
    RBF Table:
    Index      Client MAC      Reserved      Valid    Tx BF     Aging
     1       0040.96BA.45A0      Yes          Yes      Yes       No
    ```

コントローラの計画

次の項目は、メッシュ ネットワークに必要なコントローラの数に影響します。

- ネットワーク内のメッシュ アクセス ポイント（RAP および MAP）。

  RAP とコントローラを接続する有線ネットワークは、そのネットワーク内でサポートされるアクセス ポイントの総数に影響を与えることがあります。 このネットワークによって、コントローラが、WLAN のパフォーマンスに影響なく、すべてのアクセス ポイントから利用できるようになっている場合、アクセスポイントはすべてのコントローラにわたって最大の効率で等しく分散できます。 これに当てはまらない場合で、コントローラがさまざまなクラスタまたはPoPにグループ化されるとき、アクセスポイントの総数とカバレッジは減少します。

- コントローラごとにサポートされるメッシュ アクセス ポイント（RAP および MAP）の数。

  本書では、わかりやすくするために非メッシュ アクセス ポイントを、ローカル アクセス ポイントと呼びます。

表 *27*：コントローラ モデル別にサポートされるメッシュ アクセス ポイント

コントローラ モデル	ローカル **AP** サポート（非メッシュ）[6]	最大 メッシュ **AP** サポート
5508[7]	500	500
2504[8]	50	50
WiSM2	500	500

6 ローカル AP サポートは、コントローラ モデルでサポートされている非メッシュ AP の総数です。
7 5508、2112、および 2125 コントローラの場合、MAP の数は（ローカル AP サポート - RAP 数）になります。
8 2504 の場合。

（注） ワイヤレス LAN コントローラ モジュール NM および NME は、ワイヤレス LAN コントローラ（WLC）ソフトウェア リリース 5.2 以降でメッシュ 1520 シリーズ アクセス ポイントをサポートするようになりました。

（注） メッシュは、Cisco 5508 コントローラで完全にサポートされています。 屋内および屋外 AP（AP152X）には基本ライセンス（LIC-CT508-Base）で十分です。 WPlus ライセンス（LIC-WPLUS-SW）は、基本ライセンスに含まれます。 屋内メッシュ AP には WPlus ライセンスは必要ありません。 Cisco 5508 コントローラでは、メッシュ AP（MAP/RAP）は完全な AP と見なされます。 他のコントローラ プラットフォームでは、MAP は不完全な AP と見なされます。 メッシュ アクセス ポイントでは、Data Plane Transport Layer Security（DTLS）がサポートされません。

メッシュ アクセス ポイントのメッシュ ネットワークへの追加

この項では、コントローラがネットワーク内でアクティブで、レイヤ 3 モードで動作していることを前提としています。 メッシュ アクセス ポイントが接続するコントローラ ポートは、タグなしでなければなりません。

次の手順を実行してください。

ステップ 1 メッシュ アクセス ポイントの MAC アドレスを、コントローラの MAC フィルタに追加します。 MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加, （622 ページ）を参照してください。

ステップ 2 メッシュ アクセス ポイントのロール（RAP または MAP）を定義します。 メッシュ アクセス ポイントのロール定義, （624 ページ）を参照してください。

ステップ 3 各メッシュ アクセス ポイントに、プライマリ、セカンダリ、およびターシャリのコントローラを設定します。 DHCP 43 および DHCP 60 を使用した複数のコントローラの設定, （626 ページ）を参照してください。

ステップ 4 バックアップ コントローラを設定します。 バックアップ コントローラの設定, （627 ページ）を参照してください。

ステップ 5 外部 RADIUS サーバを使用して、MAC アドレスの外部認証を設定します。 RADIUS サーバを使用した外部認証および認可の設定, （633 ページ）を参照してください。

ステップ 6 グローバル メッシュ パラメータを設定します。 グローバル メッシュ パラメータの設定, （637 ページ）を参照してください。

ステップ 7 ユニバーサル クライアント アクセスを設定します。 ユニバーサル クライアント アクセスの設定は、項「Configuring Advanced Features」に含まれます。 ユニバーサル クライアント アクセス, （669 ページ）を参照してください。

ステップ 8 ローカル メッシュ パラメータを設定します。 ローカル メッシュ パラメータの設定, （644 ページ）を参照してください。

ステップ 9 （必要に応じて）モビリティ グループを設定し、コントローラを割り当てます。 第 15 章「モビリティ グループの設定」を参照してください。

MAC フィルタへのメッシュ アクセス ポイントの MAC アドレスの追加

メッシュ ネットワーク内で使用するすべてのメッシュ アクセス ポイントの MAC アドレスを適切なコントローラに入力する必要があります。 コントローラは、許可リストに含まれる屋外無線からの discovery request にだけ応答します。 コントローラでは、MAC フィルタリングがデフォルトで有効になっているため、MAC アドレスだけを設定する必要があります。 アクセス ポイントが SSC を持ち、AP 認可リストに追加された場合は、AP の MAC アドレスを MAC フィルタリング リストに追加する必要がありません。

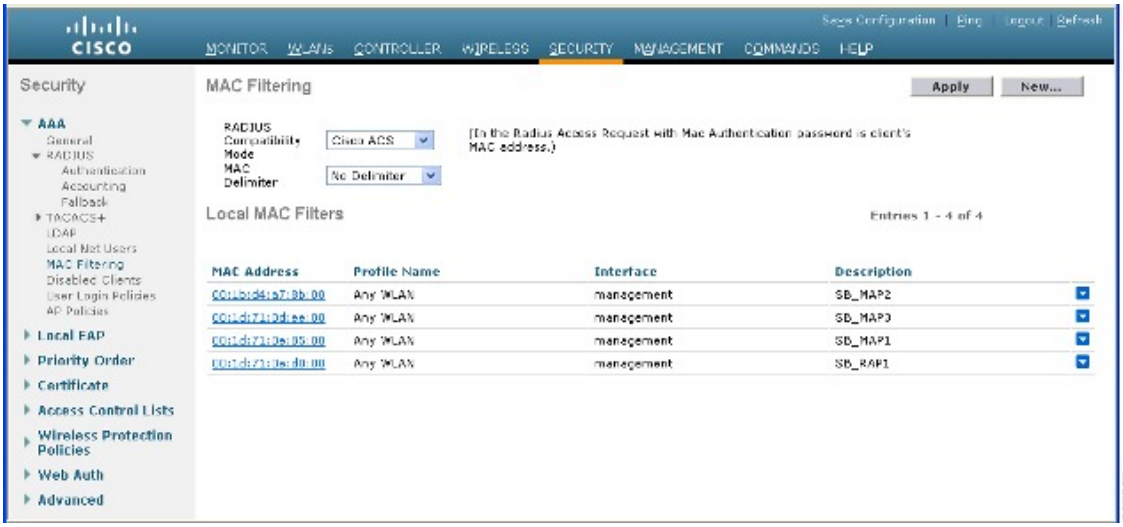
GUI と CLI のどちらを使用しても、メッシュ アクセス ポイントを追加できます。

（注） メッシュ アクセス ポイントの MAC アドレスのリストは、ダウンロードして、Cisco Prime インフラストラクチャを使用してコントローラにプッシュすることもできます。 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。

コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（GUI）

ステップ 1 [Security] > [AAA] > [MAC Filtering] を選択します。 [MAC Filtering] ページが表示されます。

図 *60*：*[MAC Filtering]* ページ



ステップ 2 [New] をクリックします。 [MAC Filters > New] ページが表示されます。

ステップ 3 メッシュ アクセス ポイントの MAC アドレスを入力します。

（注） 1500 シリーズ屋外メッシュ アクセス ポイントの場合は、コントローラへのメッシュ アクセス ポイントの BVI MAC アドレスを MAC フィルタとして指定します。 屋内メッシュ アクセス ポイントの場合は、イーサネット MAC を入力します。 必要な MAC アドレスがメッシュ アクセス ポイントの外部に記載されていない場合は、アクセス ポイントのコンソールで *sh int | i Hardware* コマンドを入力して、BVI およびイーサネット MAC アドレスを表示します。

ステップ 4 [Profile Name] ドロップダウン リストから、[Any WLAN] を選択します。

ステップ 5 [Description] フィールドで、メッシュ アクセス ポイントの説明を指定します。 入力するテキストによって、コントローラでメッシュ アクセス ポイントが識別されます。

（注） ap1522:62:39:10 などのように、省略名と最後の数桁の MAC アドレスを含めることができます。 ロケーションの詳細（屋上、ポール トップ、交差道路など）を記述することもできます。

ステップ 6 [Interface Name] ドロップダウン リストから、メッシュ アクセス ポイントを接続するコントローラ インターフェイスを選択します。

ステップ 7 [Apply] をクリックして、変更を確定します。 この時点で、メッシュ アクセス ポイントが [MAC Filtering] ページの MAC フィルタのリストに表示されます。

ステップ 8 [Save Configuration] をクリックして、変更を保存します。

ステップ 9 この手順を繰り返して、追加のメッシュ アクセス ポイントの MAC アドレスを、リストに追加します。

コントローラ フィルタ リストへのメッシュ アクセス ポイントの MAC アドレスの追加（CLI）

ステップ 1 メッシュ アクセス ポイントの MAC アドレスをコントローラ フィルタ リストに追加するには、次のコマンドを入力します。

config macfilter add *ap_mac wlan_id interface* [*description*]

wlan_id パラメータの値をゼロ（0）にすると任意の WLAN を指定し、*interface* パラメータの値をゼロ（0）にするとなしを指定します。 オプションの *description* パラメータには、最大 32 文字の英数字を入力できます。

ステップ 2 変更を保存するには、次のコマンドを入力します。

save config

メッシュ アクセス ポイントのロール定義

デフォルトでは、AP1500 はMAP に設定された無線のロールで出荷されます。 RAP として動作させるには、メッシュ アクセス ポイントを再設定する必要があります。

MAP および RAP とコントローラとのアソシエーションについて

- MAP は常に、イーサネット ポートを、プライマリ バックホールとして設定し（イーサネット ポートが UP である場合）、802.11a/n 無線をセカンダリとして設定します。 これによって、最初に、ネットワーク管理者がメッシュ アクセス ポイントを RAP として再設定する時間を取ることができます。 ネットワークでのコンバージェンスを高速にするため、メッシュ ネットワークに join するまではイーサネット デバイスを MAP に接続しないことをお勧めします。
- UP イーサネット ポートでコントローラへの接続に失敗した MAP は、802.11a/n 無線をプライマリ バックホールとして設定します。 MAP がネイバーを見つけられなかった場合、またはネイバーを介してコントローラに接続できなかった場合、イーサネット ポートは再びプライマリ バックホールとして設定されます。
- イーサネット ポートを介してコントローラに接続されている MAP は、（RAP とは違って）メッシュ トポロジをビルドしません。
- RAP は、常にイーサネット ポートをプライマリ バックホールとして設定します。
- イーサネット ポートが RAP で DOWN の場合、または RAP が UP イーサネット ポートでコントローラに接続できない場合は、802.11a/n 無線が 15 分間プライマリ バックホールとして設定されます。 ネイバーを見つけられなかった場合、または 802.11a/n 無線上でネイバーを介してコントローラに接続できない場合は、プライマリ バックホールがスキャン状態になります。 プライマリ バックホールは、イーサネット ポートでスキャンを開始します。

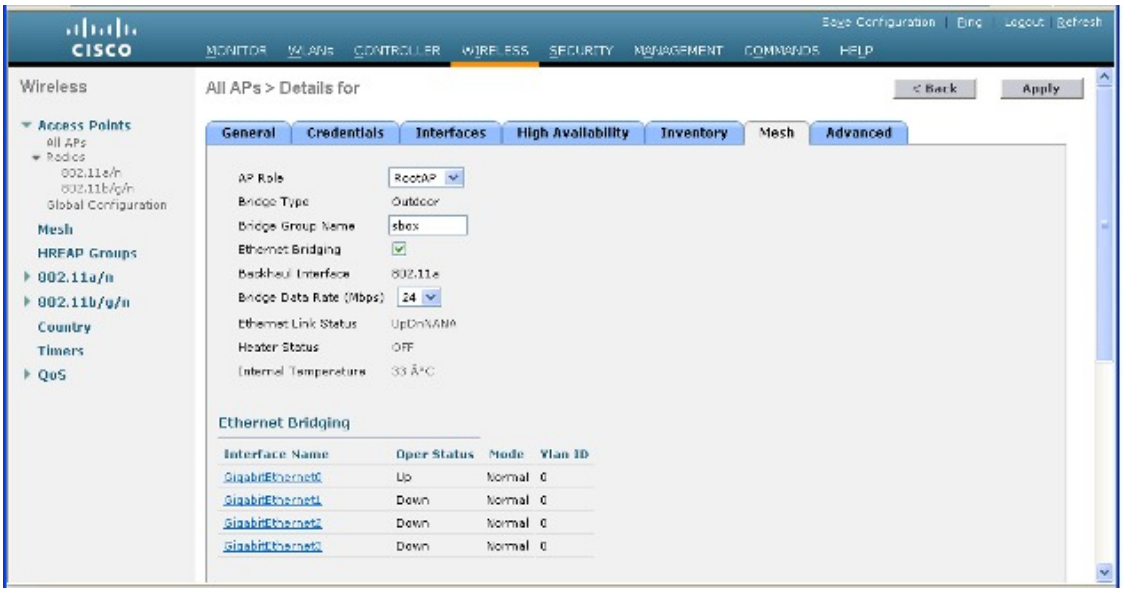
AP ロールの設定（GUI）

ステップ 1 [Wireless] をクリックして、[All APs] ページを開きます。

ステップ 2 アクセス ポイントの名前をクリックします。 [All APs > Details]（[General]）ページが表示されます。

ステップ 3 [Mesh] タブをクリックします。

図 *61*：*[All APs > Details for]*（*[Mesh]*）ページ



ステップ 4 [AP Role] ドロップダウン リストから [RootAP] または [MeshAP] を選択します。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

AP ロールの設定（CLI）

CLI を使用してメッシュ アクセス ポイントのロールを設定するには、次のコマンドを入力します。

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

DHCP 43 および DHCP 60 を使用した複数のコントローラの設定

組み込みの Cisco IOS DHCP サーバを使用して、メッシュ アクセス ポイント用に DHCP オプション 43 および 60 を設定する手順は、次のとおりです。

ステップ 1 Cisco IOS の CLI でコンフィギュレーション モードに切り替えます。

ステップ 2 DHCPプール（デフォルトのルータやネームサーバなどの必要なパラメータを含む）を作成します。 DHCP プールの作成に使用するコマンドは次のとおりです。

ip dhcp pool *pool name*
network *IP Network Netmask*
default-router *Default router*
dns-server *DNS Server*

値は次のとおりです。

```
pool name is the name of the DHCP pool, such as AP1520
IP Network is the network IP address where the controller resides, such as 10.0.15.1
Netmask is the subnet mask, such as 255.255.255.0
Default router is the IP address of the default router, such as 10.0.0.1
DNS Server is the IP address of the DNS server, such as 10.0.10.2
```

ステップ 3 次の構文に従って、オプション 60 の行を追加します。

option 60 ascii *VCI string*

VCI 文字列の場合は、次のいずれかの値を使用します。 引用符は必ず含める必要があります。

```
For Cisco 1550 series access points, enter Cisco AP c1550
For Cisco 1520 series access points, enter Cisco AP c1520
For Cisco 1240 series access points, enter Cisco AP c1240
For Cisco 1130 series access points, enter Cisco AP c1130
```

ステップ 4 次の構文に従って、オプション 43 の行を追加します。

option 43 hex *hex string*

hex string には、次の TLV 値を組み合わせて指定します。

型 + 長さ + 値

型は常に f1（16 進数）であり、長さはコントローラの管理 IP アドレスの数に 4 を掛けた値（16 進数）であり、値は一覧表示されるコントローラの IP アドレスを順番に 16 進数で表したものです。

たとえば、管理インターフェイスの IP アドレス 10.126.126.2 および 10.127.127.2 を持ったコントローラが 2 つあるとします。 型は、*f1*（*16* 進数）です。 長さは、*2 * 4 = 8 = 08*（*16* 進数）です。 IP アドレスは、*0a7e7e02* および *0a7f7f02* に変換されます。 文字列を組み合わせて、*f1080a7e7e020a7f7f02* と指定します。

DHCP スコープに追加された結果の Cisco IOS コマンドは、次のとおりです。

option 43 hex *f1080a7e7e020a7f7f02*

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

中央の場所にあるコントローラは、ローカル地方にあるプライマリ コントローラとメッシュ アクセス ポイントとの接続が失われたときに、バックアップ コントローラ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。コントローラの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るため、メッシュ アクセス ポイントはMobility Groupの外部にあるコントローラに対してフェール オーバーすることができます。

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 タイマーやディスカバリ要求タイマーなどの各種タイマーを設定することもできます。

注意事項および制約事項

- メッシュ アクセス ポイントでは、ファスト ハートビート タイマーはサポートされていません。 ファスト ハートビート タイマーは、ローカルおよびFlexConnectモードのアクセス ポイントでのみ設定されます。
- メッシュ 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保守し、定期的にPrimary discovery requestをリストの各エントリに対して送信します。 メッシュ アクセス ポイントがコントローラから新規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。 メッシュ アクセス ポイントのローカル コントローラが失敗した場合は、バックアップ コントローラのリストから使用可能なコントローラが選択されます。選択される順序は、プライマリ コントローラ、セカンダリ コントローラ、ターシャリ コントローラ、プライマリ バックアップ、およびセカンダリ バックアップです。メッシュ アクセス ポイントは、バックアップのリストで最初に使用可能な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に設定された時間内に応答を受信した場合はそのコントローラにjoinします。 時間の制限に達すると、メッシュ アクセス ポイントは、コントローラにjoinできなかったと見なし、リストで次に使用可能なコントローラからの discovery response を待機します。

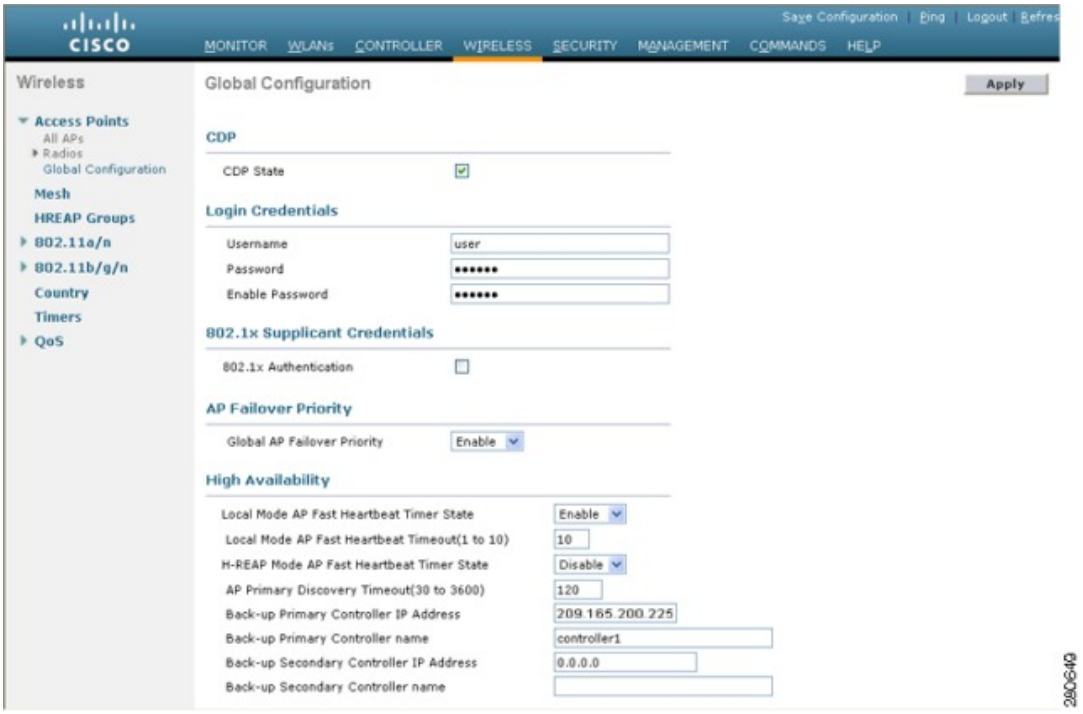
- メッシュ アクセス ポイントのプライマリ コントローラがオンラインに復帰すると、メッシュ アクセス ポイントはバックアップ コントローラとのアソシエーションを解除し、プライマリ コントローラに再接続します。 メッシュ アクセス ポイントは、設定されているセカンダリ コントローラではなく、プライマリ コントローラにフォール バックします。 たとえばプライマリ、セカンダリ、およびターシャリのコントローラを持つメッシュ アクセス ポイントが設定されている場合、プライマリとセカンダリのコントローラが応答なしになると、ターシャリ コントローラにフェール オーバーします。その後、プライマリ コントローラがオンラインに復帰するまで待って、プライマリ コントローラにフォール バックします。 セカンダリ コントローラがオンラインに復帰しても、メッシュ アクセス ポイントはターシャリ コントローラからセカンダリ コントローラにフォール バックせず、プライマリ コントローラが復帰するまでターシャリ コントローラに接続したままになります。
- ソフトウェア リリース 6.0 を実行するコントローラと、別のソフトウェア リリース（4.2、5.0、5.1、5.2 など）を実行するフェールオーバー コントローラを意図せず設定した場合、メッシュ 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 するのに時間がかかることがあります。これは、メッシュ アクセス ポイントがディスカバリ処理を LWAPP で開始し、その後 CAPWAP ディスカバリに切り替わるためです。

バックアップ コントローラの設定（GUI）

プライマリ コントローラ、セカンダリ コントローラ、特定のメッシュ アクセス ポイントのターシャリ コントローラを設定し、すべてのメッシュ アクセス ポイントのプライマリおよびセカンダリ バックアップ コントローラを設定するには、次の手順を実行します。

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。

図 *62*：*[Global Configuration]* ページ



（注） メッシュ アクセス ポイントでは、ファスト ハートビート タイマーはサポートされていません。

ステップ 2 [AP Primary Discovery Timeout] フィールドで、30 ～ 3600 秒の範囲（両端を含む）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 3 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] フィールドに指定し、コントローラの名前を [Back-up Primary Controller Name] フィールドに指定します。

（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 コントローラをは無効です。

ステップ 4 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] フィールドに指定し、コントローラの名前を [Back-up Secondary Controller Name] フィールドに指定します。

（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 コントローラを無効にします。

ステップ 5 [Apply] をクリックして、変更を確定します。

ステップ 6 特定のアクセス ポイントのプライマリ、セカンダリ、およびターシャリのバックアップ コントローラを設定する手順は、次のとおりです。

a) [Access Points] > [All APs] の順に選択して、[All APs] ページを開きます。

b) 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。

c) [High Availability] タブをクリックします

図 *63*：*[All APs > Details for]*（*[High Availability]*）ページ

d) 必要に応じて、このアクセス ポイントのプライマリ バックアップ コントローラの名前と IP アドレスを [Primary Controller] フィールドに指定します。

（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 アドレスの指定はオプションです。 バックアップ コントローラが、メッシュ アクセス ポイントが接続されている Mobility Group（プライマリ コントローラ）の外部にある場合、プライマリ、セカンダリ、ターシャリのコントローラそれぞれの 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必要があります。 そうしなければ、メッシュ アクセス ポイントがバックアップ コントローラに join できません。

e) 必要に応じて、[Secondary Controller] フィールドに、このメッシュ アクセス ポイントのセカンダリ バックアップ コントローラの名前と IP アドレスを指定します。

f) 必要に応じて、[Tertiary Controller] フィールドに、このメッシュ アクセス ポイントのターシャリ バックアップ コントローラの名前と IP アドレスを指定します。

g) [AP Failover Priority] の値を変更する必要はありません。 メッシュ アクセス ポイントのデフォルト値は *critical* で、変更することができません。

h) [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。

バックアップ コントローラの設定（CLI）

ステップ 1 特定メッシュ アクセス ポイントのプライマリ 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 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、メッシュ アクセス ポイントが接続されている Mobility Group（プライマリ コントローラ）の外部にある場合、プライマリ、セカンダリ、ターシャリのコントローラそれぞれの 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必要があります。 そうしなければ、メッシュ アクセス ポイントがバックアップ コントローラに join できません。

ステップ 2 特定メッシュ アクセス ポイントのセカンダリ 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 ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 3 特定メッシュ アクセス ポイントのターシャリ 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 ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

ステップ 4 すべてのメッシュ 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するには、次のコマンドを入力します。
config advanced backup-controller primary *backup_controller_name backup_controller_ip_address*

ステップ 5 すべてのメッシュ 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するには、次のコマンドを入力します。
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 メッシュ 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するには、次のコマンドを入力します。
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 7 メッシュ アクセス ポイントのディスカバリ タイマーを設定するには、次のコマンドを入力します。
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 8 802.11 認証応答タイマーを設定するには、次のコマンドを入力します。
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 9 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 10 メッシュ アクセス ポイントの設定を表示するには、次のコマンドを入力します。

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**
- **show mesh config**

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........................ 1-4404
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 Primary Discovery Timeout (seconds)........... 120
```

show mesh config コマンドに対しては、次のような情報が表示されます。

```
Mesh Range....................................... 12000
Backhaul with client access status............... disabled
Background Scanning State........................ enabled
Mesh Security
```

```
Security Mode..................................... EAP
External-Auth..................................... disabled
Use MAC Filter in External AAA server......... disabled
Force External Authentication.................. disabled
Mesh Alarm Criteria
Max Hop Count..................................... 4
Recommended Max Children for MAP.............. 10
Recommended Max Children for RAP.............. 20
Low Link SNR...................................... 12
High Link SNR..................................... 60
Max Association Number........................ 10
Association Interval........................... 60 minutes
Parent Change Numbers......................... 3
Parent Change Interval........................ 60 minutes
Mesh Multicast Mode............................... In-Out
Mesh Full Sector DFS.............................. enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

RADIUS サーバを使用した外部認証および認可の設定

リリース 5.2 以降では、Cisco ACS（4.1 以降）などの RADIUS サーバを使用した、メッシュ アクセス ポイントの外部認証および認可がサポートされています。 RADIUS サーバは、クライアント認証タイプとして、証明書を使用する EAP-FAST をサポートする必要があります。

メッシュ ネットワーク内で外部認証を使用する前に、次の変更を行う必要があります。

- AAA サーバとして使用する RADIUS サーバをコントローラに設定する必要があります。
- コントローラも、RADIUS サーバで設定する必要があります。
- 外部認証および認可用に設定されたメッシュ アクセス ポイントを RADIUS サーバのユーザ リストに追加します。
  - 詳細については、RADIUS サーバへのユーザ名の追加を参照してください。
- RADIUS サーバで EAP-FAST を設定し、証明書をインストールします。 802.11a インターフェイスを使用してメッシュ アクセス ポイントをコントローラに接続する場合には、EAP-FAST 認証が必要です。外部 RADIUS サーバは、Cisco Root CA 2048 を信頼する必要があります。CA 証明書のインストールと信頼については、RADIUS サーバの設定を参照してください。

（注） ファストイーサネットまたはギガビットイーサネットインターフェイスを使用してメッシュ アクセス ポイントをコントローラ接続する場合は、MAC 認可だけが必要です。

（注） また、この機能は、コントローラ上のローカル EAP および PSK 認証をサポートしています。

RADIUS サーバの設定

ステップ 1 次の場所から Cisco Root CA 2048 の CA 証明書をダウンロードします。

- http://www.cisco.com/security/pki/certs/crca2048.cer
- http://www.cisco.com/security/pki/certs/cmca.cer

ステップ 2 次のように証明書をインストールします。

a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [ACS Certification Authority Setup] の順にクリックします。
b) [CA certificate file] ボックスに、CA 証明書の場所（パスと名前）を入力します （たとえば、*c:\Certs\crca2048.cer*）。
c) [Submit] をクリックします。`

ステップ 3 次のように外部 RADIUS サーバを設定して、CA 証明書を信頼するようにします。

a) Cisco Secure ACS のメイン メニューから、[System Configuration] > [ACS Certificate Setup] > [Edit Certificate Trust List] の順に選択します。 [Edit Certificate Trust List] が表示されます。
b) 証明書の名前（[Cisco Root CA 2048 (Cisco Systems)]）の横にあるチェックボックスをオンにします。
c) [Submit] をクリックします。`
d) ACS を再起動するには、[System Configuration] > [Service Control] の順に選択してから、[Restart] をクリックします。

Cisco ACS サーバに関する追加の設定詳細については、次のドキュメントを参照してください。

- http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html（Windows）
- http://www.cisco.com/en/US/products/sw/secursw/ps4911/<?Line-Break?><?HardReturn?>(UNIX)

RADIUS サーバへのユーザ名の追加

メッシュ アクセス ポイントの RADIUS 認証を有効にする前に、外部 RADIUS サーバによって認可および認証されるメッシュ アクセス ポイントの MAC アドレスをサーバのユーザ リストに追加します。

リモート認可および認証の場合、EAP-FASTは製造元の証明書（CERT）を使用して、子メッシュ アクセス ポイントを認証します。 また、この製造元証明書に基づく ID は、ユーザの確認においてメッシュ アクセス ポイントのユーザ名として機能します。

Cisco IOS ベースのメッシュ アクセス ポイントの場合は、MAC アドレスをユーザ リストに追加するだけでなく、*platform_name_string–Ethernet_MAC_address* 文字列をユーザ リストに入力する必要があります（たとえば、c1240-001122334455）。 コントローラは最初に MAC アドレスをユーザ名として送信します。この初回の試行が失敗すると、コントローラは *platform_name_string–Ethernet_MAC_address* 文字列をユーザ名として送信します。

（注） *platform_name_string–Ethernet_MAC_address* 文字列だけをユーザ リストに入力する場合は、AAA サーバに初回試行時失敗のログが表示されます。ただし、Cisco IOS ベースのメッシュ アクセス ポイントは、*platform_name_string–Ethernet_MAC_address* 文字列をユーザ名として使用して 2 回目の試行で認証されます。

（注） パスワードは、ユーザ名と同じでなければなりません（たとえば *c1520-001122334455*）。

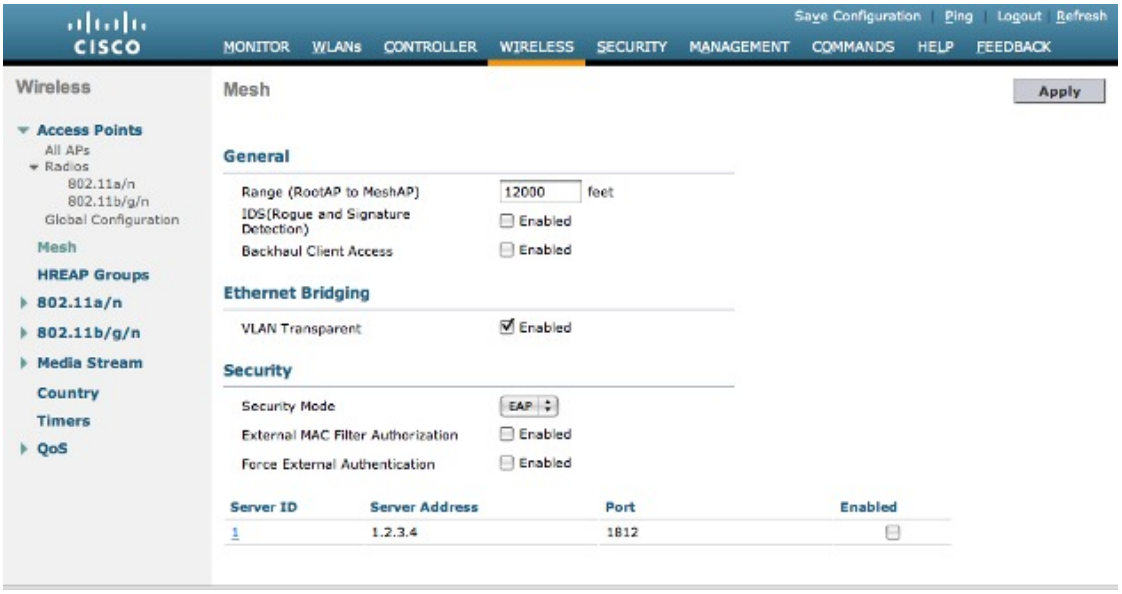
メッシュ アクセス ポイントの外部認証の有効化

この項では、メッシュ アクセス ポイントの外部認証を有効にする方法について説明します。

メッシュ アクセス ポイントの外部認証の有効化（GUI）

ステップ 1 [Wireless] > [Mesh] を選択します。 [Mesh] ページが表示されます。

図 *64* : *[Mesh]* ページ



ステップ 2 セキュリティ セクションで、[Security Mode] ドロップダウン リストから [EAP] オプションを選択します。

ステップ 3 [External MAC Filter Authorization] オプションと [Force External Authentication] オプションの [Enabled] チェックボックスをオンにします。

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。

メッシュ アクセス ポイントの外部認証のイネーブル化（CLI）

1. **config mesh security eap**
2. **config macfilter mac-delimiter colon**
3. **config mesh security rad-mac-filter enable**
4. **config mesh radius-server index enable**
5. **config mesh security force-ext-auth enable**（任意）

セキュリティ統計の表示

CLI を使用してメッシュ アクセス ポイントのセキュリティ統計を表示するには、次のコマンドを入力します。

show mesh security-stats *Cisco_AP*

このコマンドを使用すると、指定のアクセス ポイントとその子アクセス ポイントのパケット エラー統計、エラー数、タイムアウト数、アソシエーションと認証の成功数、再アソシエーション数、および再認証数が表示されます。

グローバル メッシュ パラメータの設定

グローバル メッシュ パラメータについて

この項では、メッシュアクセスポイントがコントローラとの接続を確立するよう設定する手順について説明します。内容は次のとおりです。

- RAP と MAP 間の最大レンジの設定（屋内 MAP には非適用）
- クライアント トラフィックを伝送するバックホールの有効化
- VLAN タグが転送されるかどうかの指定
- セキュリティ設定（ローカルおよび外部認証）を含むメッシュアクセスポイントの認証モード（EAP または PSK）および認証方式（ローカルまたは外部）の定義

必要なメッシュ パラメータを設定するには、GUI と CLI のいずれかを使用できます。 パラメータはすべてグローバルに適用されます。

グローバル メッシュ パラメータの設定（GUI）

ステップ 1 [Wireless] > [Mesh] を選択します。

ステップ 2 必要に応じて、メッシュ パラメータを修正します。
次の表に、各パラメータについての説明を示します。

表 *28*：グローバル メッシュ パラメータ

パラメータ	説明
Range (RootAP to MeshAP)	ルート アクセス ポイント（RAP）とメッシュ アクセス ポイント（MAP）間に必要な最良の距離（フィート単位）です。 ネットワーク内のコントローラと既存のすべてのアクセス ポイントに join する場合、このグローバル パラメータは、すべてのメッシュ アクセス ポイントに適用されます。 **範囲**：150 ～ 132,000 フィート **デフォルト**：12,000 フィート （注） この機能をイネーブルにすると、すべてのメッシュ アクセス ポイントがリブートします。
IDS（Rogue and Signature Detection）	この機能を有効にすると、クライアント アクセスだけ（バックホールではなく）のすべてのトラフィックに対する IDS レポートが生成されます。 この機能をディセーブルにすると、IDS レポートは生成されませんが、バックホール上の帯域幅が節約されます。 次のコマンドを使用して、メッシュ AP でこの機能を有効または無効にする必要があります。 **config mesh ids-state {enable | disable}** （注） 2.4-GHz IDS は、コントローラのグローバル IDS 設定を使用してアクティブになっています。

パラメータ	説明
Backhaul Client Access	（注） このパラメータは、2つ以上の無線があるメッシュ アクセス ポイント（1552、1524SB、1522、1240、1130、および11n屋内メッシュ AP（ただし、1524PSを除く））に適用されます。 ユニバーサル クライアント アクセスが有効な場合は、バックホール無線を介したワイヤレス クライアント アソシエーションが許可されます。 一般的に、バックホール無線は、バックホールが2.4 GHzである可能性がある1522を除くほとんどのメッシュ アクセス ポイントで5 GHz無線です。 つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。 ユニバーサル クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは2番目の無線のみを介して送信されます。 **デフォルト**：無効 （注） この機能をイネーブルにすると、すべてのメッシュ アクセス ポイントがリブートします。

パラメータ	説明
VLAN Transparent	この機能によって、メッシュ アクセス ポイントでイーサネット ブリッジド トラフィックの VLAN タグを処理する方法が決定されます。 VLAN 透過が有効な場合は、VLAN タグが処理されず、パケットがタグなしパケットとしてブリッジされます。 （注） VLAN 透過が有効な場合、イーサネット ポートの設定は必要ありません。イーサネット ポートは、タグありフレームとタグなしフレームの両方を解釈せずに渡します。 VLAN 透過が無効な場合は、すべてのパケットがポートの VLAN 設定（トランク モード、アクセス モード、またはノーマル モード）に従って処理されます。 （注） イーサネット ポートがトランク モードに設定されている場合は、イーサネット VLAN タギングを設定する必要があります。「イーサネットブリッジングの有効化」の項を参照してください。 （注） 通常、アクセス、およびトランク モードのイーサネット ポートの使用の概要については、「イーサネット ポートに関する注意」の項を参照してください。 （注） VLAN タギングを使用するには、[VLAN Transparent] チェックボックスをオフにする必要があります。 **デフォルト**：有効
Security Mode	メッシュ アクセス ポイントのセキュリティ モード（Pre-Shared Key（PSK; 事前共有キー）または Extensible Authentication Protocol（EAP））を定義します。 （注） RADIUS サーバを使用する外部 MAC フィルタ認可を設定する場合、EAP を選択する必要があります。 （注） [External MAC Filter Authorization] パラメータを無効にする（チェックボックスをオフにする）と、ローカル EAP または PSK 認証はコントローラ内で実行されます。 **オプション**：PSK または EAP **デフォルト**：EAP

パラメータ	説明
External MAC Filter Authorization	デフォルトでは、MACフィルタリングは、コントローラ上のローカル MAC フィルタを使用します。 外部 MAC フィルタ認証が有効であり、MAC アドレスがローカル MAC フィルタで検出されない場合には、外部 RADIUS サーバの MAC アドレスが使用されます。 これにより、外部サーバで定義されていないメッシュ アクセス ポイントの join を防ぎ、不正なメッシュ アクセス ポイントからネットワークを保護します。 メッシュ ネットワーク内で外部認証を利用するには、次の設定が必要です。 • AAA サーバとして使用する RADIUS サーバをコントローラに設定する必要があります。 • コントローラも、RADIUS サーバで設定する必要があります。 • 外部認証および認証用に設定されたメッシュ アクセス ポイントは、RADIUS サーバのユーザ リストに追加する必要があります。 ◦ リモート認可および認証の場合、EAP-FAST は製造元の証明書（CERT）を使用して、子メッシュ アクセス ポイントを認証します。 また、この製造元証明書に基づく ID は、ユーザの確認においてメッシュ アクセス ポイントのユーザ名として機能します。 ◦ IOS ベースのメッシュ アクセス ポイント（1130、1240、1522、1524）の場合、メッシュ アクセス ポイントのプラットフォーム名は、証明書内のイーサネット アドレスの前に位置します。つまり、外部 RADIUS サーバのユーザ名は、*platform_name_string*–イーサネット *MAC* アドレスであり、たとえば *c1520-001122334455* のようになります。 • RADIUS サーバに証明書をインストールして、EAP-FAST を設定する必要があります。 （注） この機能はデフォルトで有効ではなく、コントローラは MAC アドレス フィルタを使用してメッシュ アクセス ポイントを許可および認証します。 **デフォルト**：無効

パラメータ	説明
Force External Authorization	このパラメータが有効で、[EAP] および [External MAC Filter Authorization] パラメータも有効の場合、メッシュ アクセス ポイントの外部の許可および認証はデフォルトで外部 RADIUS サーバ（Cisco 4.1 以降など）が行います。 RADIUS サーバによって、コントローラによる MAC アドレスのローカル認証（デフォルト）が無効になります。 **デフォルト**：無効

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。

グローバル メッシュ パラメータの設定（CLI）

（注） CLI コマンドで使用されるパラメータの説明、有効範囲およびデフォルト値については、グローバル メッシュ パラメータの設定（GUI）を参照してください。

ステップ 1 ネットワークの全メッシュ アクセス ポイントの最大レンジをフィート単位で指定するには、次のコマンドを入力します。
config mesh range *feet*

現在のレンジを確認するには、**show mesh range** と入力します。

ステップ 2 バックホールのすべてのトラフィックに関して IDS レポートをイネーブルまたはディセーブルにするには、次のコマンドを入力します。
config mesh ids-state {**enable** | **disable**}

ステップ 3 バックホール インターフェイスでのアクセス ポイント間のデータ共有レート（Mbps 単位）を指定するには、次のコマンドを入力します。
config ap bhrate {*rate* | **auto**} *Cisco_AP*

ステップ 4 メッシュ アクセス ポイントのプライマリ バックホール（802.11a）でクライアント アソシエーション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 mesh client-access {**enable** | **disable**}

config ap wlan {**enable** | **disable**} **802.11a** *Cisco_AP*

config ap wlan {**add** | **delete**} **802.11a** *wlan_id Cisco_AP*

ステップ 5 VLAN トランスペアレントをイネーブルまたはディセーブルにするには、次のコマンドを入力します。
config mesh ethernet-bridging VLAN-transparent {**enable** | **disable**}

ステップ 6 メッシュ アクセス ポイントのセキュリティ モードを定義するには、次のいずれかのコマンドを入力します。

a) コントローラによるメッシュ アクセス ポイントのローカル認証を提供するには、次のコマンドを入力します。
config mesh security {**eap** | **psk**}

b) 認証用にコントローラ（ローカル）の代わりに外部 RADIUS サーバに MAC アドレス フィルタを格納するには、次のコマンドを入力します。
config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server index enable

c) RADIUS サーバで外部認証を提供し、コントローラでローカル MAC フィルタを定義するには、次のコマンドを入力します。
config mesh security eap

config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server index enable

config mesh security force-ext-auth enable

d) RADIUS サーバで MAC ユーザ名（*c1520-123456* など）を使用し、RADIUS サーバで外部認証を提供するには、次のコマンドを入力します。
config macfilter mac-delimiter colon

config mesh security rad-mac-filter enable

config mesh radius-server index enable

config mesh security force-ext-auth enable

ステップ 7 変更を保存するには、次のコマンドを入力します。
save config

グローバル メッシュ パラメータ設定の表示（CLI）

- **show mesh client-access**：ユニバーサル クライアント アクセスが有効な場合は、バックホール無線を介したワイヤレス クライアント アソシエーションが許可されます。 一般的に、バックホール無線は、バックホールが 2.4 GHz である可能性がある 1522 を除くほとんどのメッシュ アクセス ポイントで 5 GHz 無線です。 つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

ユニバーサル クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは2番目の無線のみを介して送信されます。

例：

show mesh client-access

```
Backhaul with client access status: enabled
```

- **show mesh ids-state**：バックホールの IDS レポートのステータスが有効か無効かを示します。

例：

show mesh ids-state

```
Outdoor Mesh IDS(Rogue/Signature Detect): .... Disabled
```

- **show mesh config**：グローバル構成の設定を表示します。

例：

show mesh config

```
Mesh Range...................................... 12000
Mesh Statistics update period................... 3 minutes
Backhaul with client access status.............. disabled
Background Scanning State....................... enabled
Backhaul Amsdu State............................ disabled

Mesh Security
Security Mode................................... EAP
External-Auth................................... disabled
Use MAC Filter in External AAA server........... disabled
Force External Authentication.................. disabled

Mesh Alarm Criteria
Max Hop Count................................... 4
Recommended Max Children for MAP............... 10
Recommended Max Children for RAP............... 20
Low Link SNR.................................... 12
High Link SNR................................... 60
Max Association Number.......................... 10
Association Interval............................ 60 minutes
Parent Change Numbers........................... 3
Parent Change Interval.......................... 60 minutes

Mesh Multicast Mode............................. In-Out
Mesh Full Sector DFS............................ enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
```

ローカル メッシュ パラメータの設定

グローバル メッシュ パラメータを設定したら、ネットワークで使用中の機能について次のローカル メッシュ パラメータを設定する必要があります。

- バックホール データ レート。ワイヤレス バックホール データ レートの設定，（645 ページ）を参照してください。

- イーサネット ブリッジング。 イーサネット ブリッジングの設定, （647 ページ）を参照してください。
- ブリッジ グループ名。 イーサネット ブリッジングの設定, （647 ページ）を参照してください。
- ワークグループ ブリッジ。 ワークグループ ブリッジの設定, （685 ページ）を参照してください。
- Public Safety 帯域設定。 Public Safety 帯域設定の構成, （649 ページ）を参照してください。
- Cisco 3200 シリーズのアソシエーションおよび相互運用性。 Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定（GUI）, （742 ページ）を参照してください。
- 電源およびチャネル設定。 電力およびチャネルの設定, （654 ページ）を参照してください。
- アンテナ ゲイン設定。 アンテナ ゲインの設定, （656 ページ）を参照してください。
- シリアル バックホール アクセス ポイントでのバックホール チャネル選択解除。 シリアル バックホール アクセス ポイントでのバックホール チャネル選択解除, （657 ページ）を参照してください。
- 動的チャネル割り当て。 動的チャネル割り当ての設定（GUI）, （836 ページ）を参照してください。

ワイヤレス バックホール データ レートの設定

バックホールは、アクセス ポイント間でワイヤレス接続のみを作成するために使用されます。バックホール インターフェイスは、アクセス ポイントに基づいてデフォルトで 802.11a または 802.11a/n になります。 利用可能な RF スペクトラムを効果的に使用するにはレート選択が重要です。また、レートはクライアントデバイスのスループットにも影響を与えることがあり、スループットはベンダー デバイスを評価するために業界出版物で使用される重要なメトリックです。

Dynamic Rate Adaptation（DRA）には、パケット伝送のために最適な伝送レートを推測するプロセスが含まれます。 レートを正しく選択することが重要です。 レートが高すぎると、パケット伝送が失敗し、通信障害が発生します。 レートが低すぎると、利用可能なチャネル帯域幅が使用されず、品質が低下し、深刻なネットワーク輻輳および障害が発生する可能性があります。

データ レートは、RF カバレッジとネットワーク パフォーマンスにも影響を与えます。 低データ レート（6 Mbps など）が、高データ レート（300 Mbps など）よりもアクセス ポイントからの距離を延長できます。 結果として、データ レートはセル カバレッジと必要なアクセス ポイントの数に影響を与えます。 異なるデータ レートは、ワイヤレス リンクで冗長度の高い信号を送信することにより（これにより、データをノイズから簡単に復元できます）、実現されます。 1 Mbps のデータ レートで 1 つのパケットに対して送信される記号の数は、11 Mbps で同じパケットに対して使用される記号の数よりも多くなります。 したがって、低ビット レートでのデータの送信には、高ビット レートでの同じデータの送信よりも時間がかり、スループットが低下します。

コントローラ リリース 5.2 では、メッシュ 5 GHz バックホールのデフォルト データ レートは 24 Mbps です。 これは、6.0 および 7.0 コントローラ リリースでも同じです。

6.0 コントローラ リリースでは、メッシュ バックホールに「Auto」データ レートを設定できます。設定後に、アクセスポイントは、最も高いレートを選択します（より高いレートは、すべてのレートに影響を与える状況のためではなくそのレートに適切でない状況のため、使用できません）。 つまり、設定後は、各リンクが、そのリンク品質に最適なレートに自動的に設定されます。

メッシュ バックホールを「Auto」に設定することをお勧めします。

たとえば、メッシュ バックホールが 48 Mbps を選択した場合、この決定は、誰かが電子レンジを使用したためではなく（これによりすべてのレートが影響を受けます）、54 に対して十分な SNR がないため、54 Mbps を使用できないことが確認された後に行われます。

低ビット レートでは、MAP 間の距離を長くすることが可能になりますが、WLAN クライアント カバレッジにギャップが生じる可能性が高く、バックホール ネットワークのキャパシティが低下します。 バックホール ネットワークのビット レートを増加させる場合は、より多くの MAP が必要となるか、MAP 間の SNR が低下し、メッシュの信頼性と相互接続性が制限されます。

（注） データ レートは、AP ごとにバックホールで設定できます。 これはグローバル コマンドではありません。

以下のコマンドを使用してバックホールに関する情報を取得します。

- **config ap bhrate**：Cisco ブリッジ バックホール送信レートを設定します。

  config ap bhrate *backhaul-rate ap-name*

（注） 各 AP に対して設定済みのデータ レート（RAP=18 Mbps、MAP1=36 Mbps）は、6.0 以降のソフトウェア リリースへのアップグレード後も保持されます。6.0 リリースにアップグレードする前に、データ レートに設定されるバックホール データ レートがある場合は、その設定が保持されます。

次の例は、RAP でバックホール レートを 36000 Kbps に設定する方法を示しています。

(Cisco Controller) > **config ap bhrate** *36000 HPRAP1*

- **show ap bhrate**：Cisco ブリッジ バックホール レートを表示します。

  (Cisco Controller) > **show ap bhrate** *ap-name*

- **show mesh neigh summary**：バックホールで現在使用されているレートを含むリンク レート概要を表示します。

  (Cisco Controller) > **show mesh neigh summary** *HPRAP1*

```
AP Name/Radio    Channel     Rate     Link-Snr     Flags      State
-------------- --------   --------   -------     -----      -----
00:0B:85:5C:B9:20 0          auto        4       0x10e8fcb8   BEACON
00:0B:85:5F:FF:60 0          auto        4       0x10e8fcb8   BEACON DEFAULT
00:0B:85:62:1E:00 165        auto        4       0x10e8fcb8   BEACON
OO:0B:85:70:8C:A0 0          auto        1       0x10e8fcb8   BEACON
HPMAP1           165         54          40      0x36         CHILD BEACON
```

```
HJMAP2          0          auto         4       0x10e8fcb8   BEACON
```

バックホールのキャパシティとスループットは AP のタイプ（つまり、802.11a/n であるかや、802.11a のみであるかや、バックホール無線の数など）によって異なります。

AP1524 SB では、ダウンリンク方向にバックホールを延長するために RAP の 5 GHz 無線のスロット 2 が使用され、アップリンクのバックホールには MAP の 5 GHz 無線のスロット 2 が使用されます。 スロット 2 無線では指向性アンテナを使用することをお勧めします。 MAP はダウンリンク方向にスロット 1 無線を拡張し、Omni または指向性アンテナもクライアント アクセスを提供します。 7.0 リリース以降は、クライアント アクセスをスロット 2 無線で提供できます。

AP1524SB は優れたスループットを提供し、スループットは最初のホップ後もほとんど低下しません。 AP1524SB のパフォーマンスは、AP1522 および AP1524PS よりも優れています。これは、これらの AP にはバックホール アップリンクとダウンリンクに対して単一無線しか使用されないためです。

表 *29*：*AP1552* バックホール キャパシティ

ホップ	RAP	1	2	3	4
最大スループット（20 MHz BH）	112 Mbps	83 Mbps	41 Mbps	25 Mbps	15 Mbps
最大スループット（40 MHz BH）	206 Mbps	111 Mbps	94 Mbps	49 Mbps	35 Mbps

イーサネット ブリッジングの設定

セキュリティ上の理由により、デフォルトではすべての MAP でイーサネット ポートが無効になっています。 有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定します。

（注） イーサネット ブリッジングが無効な場合であっても、いくつかのプロトコルで例外が許可されます。 たとえば、次のプロトコルが許可されます。

- スパニングツリー プロトコル（STP）
- アドレス解決プロトコル（ARP）
- ワイヤレス アクセス ポイントの制御およびプロビジョニング（CAPWAP）
- ブートストラップ プロトコル（BOOTP）パケット

レイヤ 2 のループの発生を防止するために、接続されているすべてのスイッチ ポート上でスパニングツリー プロトコルを有効にします。

イーサネット ブリッジングは、次の 2 つの場合に有効にする必要があります。

1 メッシュ ノードをブリッジとして使用する場合。

（注） ポイントツーポイントおよびポイントツーマルチポイント ブリッジング導入でイーサネット ブリッジングを使用するのに、VLAN タギングを設定する必要はありません。

2 MAP でイーサネット ポートを使用して任意のイーサネット デバイス（ビデオ カメラなど）を接続する場合。 VLAN タギングを有効にするときの最初の手順です。

イーサネット ブリッジングの有効化（GUI）

ステップ 1 [Wireless] > [All APs] を選択します。

ステップ 2 イーサネットブリッジングを有効にするメッシュアクセスポイントのAP名のリンクをクリックします。

ステップ 3 詳細ページで、[Mesh] タブをクリックします。

ステップ 4 [AP Role] ドロップダウン リストから [RootAP] または [MeshAP] を選択します（すでに選択されていない場合）。

ステップ 5 イーサネット ブリッジングを有効にする場合は、[Ethernet Bridging] 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、このチェックボックスをオフにします。

ステップ 6 [Apply] をクリックして、変更を確定します。 ページの最下部の [Ethernet Bridging] セクションに、メッシュ アクセス ポイントの各イーサネット ポートが一覧表示されます。

ステップ 7 該当するメッシュ AP からコントローラへのパスを取る各親メッシュ AP に対してイーサネット ブリッジングを有効にします。たとえば、Hop 2 の MAP2 でイーサネットブリッジングを有効にする場合は、MAP1（親 MAP）と、コントローラに接続している RAP でもイーサネットブリッジングを有効にする必要があります。

ブリッジ グループ名の設定

ブリッジグループ名（BGN）は、メッシュアクセスポイントのアソシエーションを制御します。BGN を使用して無線を論理的にグループ分けしておくと、同じチャネルにある 2 つのネットワークが相互に通信することを防止できます。 この設定はまた、同一セクター（領域）のネットワーク内に複数の RAP がある場合にも便利です。 BGN は最大 10 文字までの文字列です。

NULL VALUE という BGN は、工場で設定されているデフォルトです。 装置自体にブリッジ グループ名は表示されていませんが、このグループ名を使用することで、ネットワーク固有の BGN を割り当てる前に、メッシュ アクセス ポイントをネットワークに join させることができます。

同一セクターのネットワーク内に（より大きなキャパシティを得るために）RAP が 2 つある場合は、別々のチャネルで 2 つの RAP に同じ BGN を設定することをお勧めします。

ブリッジ グループ名の設定（CLI）

- CLI を使用して、次のコマンドを入力します。

  config ap bridgegroupname set *bridge-group-name*

  次のような情報が表示されます。

```
Setting bridgegroupname on an AP permanently restricts the APs to which it may connect,
 use with caution.
Are you sure you want to continue? (y/n) n

AP bridgegroupname not changed!
```

BGN の設定後に、メッシュ アクセス ポイントがリブートします。

注意 稼働中のネットワークで BGN を設定する場合は、注意してください。 BGN の割り当ては、必ず RAP から最も遠い距離にあるノード（メッシュ ツリーの一番下にある終端ノード）から開始し、RAP に向かって設定して、同じネットワーク内に混在する BGN（古い BGN と新しい BGN）のため、メッシュ アクセス ポイントがドロップしないようにします。

ブリッジ グループ名の確認（GUI）

ステップ 1 [Wireless] > [Access Points] > [AP Name] をクリックします。 選択したメッシュ アクセス ポイントの詳細ページが表示されます。

ステップ 2 [Mesh] タブをクリックします。 BGN を含むメッシュ アクセス ポイントの詳細が表示されます

ブリッジ グループ名の確認（CLI）

- BGN を確認するには、次のコマンドを入力します。

  (Cisco controller) > **show ap config general** *AP_Name*

  次のような情報が表示されます。

Public Safety 帯域設定の構成

AP1522 と AP1524PS では、Public Safety 帯域（4.9 GHz）がサポートされています

- AP1524PS の場合、4.9 GHz 無線は 5 GHz 無線と独立しており、バックホールに使用されません。 5.8 GHz はバックホールにのみ使用され、クライアント アクセスが不可能です。 AP1524PS では、4.9 GHz 帯域がデフォルトで有効になっています。

- 日本の場合、4.9GHzはアンライセンスであるため、デフォルトで有効になっています。

- AP1522 の場合、バックホールで 4.9 GHz の Public Safety 帯域を有効にすることができます。これはグローバル レベルでのみ可能であり、メッシュ アクセス ポイントごとに行うことはできません。
  - AP1522 の 4.9 GHz 帯域のクライアント アクセスでは、ユニバーサル クライアント アクセス機能を有効にする必要があります。

- Public Safety のみの導入では、AP1522 および AP1524PS をそれぞれ独自の個別 RAP ベース ツリーに接続する必要があります。 このような導入の場合、1522 は 4.9 GHz バックホールを使用する必要があり、1524PS は独自の RAP ツリーに所属し、5.8 GHz バックホールを使用する必要があります。
- 米国を含む一部の地域では、4.9 GHz バックホールでのみ Public Safety トラフィックを使用できます。 設置前に、対象国における適合性を確認してください。

AP1524PS の 4.9 GHz サブバンド無線は、5 MHz（チャネル 1 ～ 10）、10 MHz（チャネル 11 ～ 19）、および 20 MHz（チャネル 20 ～ 26）の帯域幅内の Public Safety チャネルをサポートします。

- 5 MHz の帯域幅では、データ レート 1.5、2.25、3、4.5、6、9、12、および 13.5 Mbps がサポートされます。 デフォルトのレートは 6 Mbps です。
- 10 MHz の帯域幅では、3、4.5、6、9、12、18、24、および 27 Mbps のデータ レートがサポートされます。 デフォルトのレートは 12 Mbps です。

（注）
- シリアル番号が FTX1150XXXX よりも小さい API1522 は、4.9 GHz 無線で 5 および 10 MHz のチャネルを**サポートしません**。ただし、20 MHz のチャネルはサポートされます。
- シリアル番号が FTX1150XXXX よりも大きい AP1522 は、5 MHz、10 MHz、および 20 MHz のチャネルをサポートします。

4.9 GHz 帯域の有効化

4.9 GHz帯域を有効にしようとすると、この帯域が世界中の大半の地域で認可されていることを示す警告が表示されます

図 *65*：設定中の *Public Safety* 警告

```
(Cisco Controller) >config mesh public-safety ?

enable          Enable/Disable 4.9GHz Public Safety Bands for Mesh AP.

disable         Enable/Disable 4.9GHz Public Safety Bands for Mesh AP.

(Cisco Controller) >config mesh public-safety enable ?

all             For All Cisco AP

(Cisco Controller) >config mesh public-safety enable all

4.9GHz is a licensed frequency band in -A domain for public-safety usage
 Are you sure you want to continue? (y/N)y

        Global Public Safety State: Already configured, Configuring Local States
...


(Cisco Controller) >config mesh public-safety enable HJRap1

Public Safety can't be configured on individual Cisco APs.
```

273943

- CLI を使用して Public Safety 帯域がメッシュ アクセス ポイント上にあることを確認するには、次のコマンドを入力します。

  show mesh public-safety

  次の出力が表示されます。

  ```
  Global Public Safety status: enabled
  ```

- GUI を使用して Public Safety 帯域がメッシュ アクセス ポイント上にあることを確認するには、次のように操作します。

  [Wireless] > [Access Points] > [802.11a radio] > [Configure]（[Antenna] ドロップダウン リストから）

Cisco 3200 との相互運用性の設定

Cisco AP1522 および AP1524PS は、Public Safety チャネル（4.9 GHz）と、2.4 GHz アクセスおよび 5.8 GHz バックホールで、Cisco 3200 と相互運用できます。

Cisco 3200 は車載ネットワークを作成します。車載ネットワークでは、PC、監視カメラ、デジタルビデオカメラ、プリンタ、PDA、スキャナなどの装置が、メインのインフラストラクチャへと接続されている携帯電話ベースまたは WLAN ベースのサービスなどのワイヤレス ネットワークを共有できます。 この機能により、警察車両などの車載展開から収集されたデータをワイヤレス インフラストラクチャ全体に統合できます。

この項では、Cisco 3200、AP1522、および AP1524PS 間の相互運用性を設定する際のガイドラインと詳細な手順について説明します。

1130、1240、および 1520（1522、1524PS）シリーズのメッシュ アクセス ポイントと Cisco 3200 との間の具体的な相互運用性の詳細については、次の表を参照してください。

表 *30*：メッシュ アクセス ポイントと *Cisco 3200* の相互運用性

メッシュ アクセス ポイントのモデル	Cisco 3200 のモデル
1552、1522[9]	c3201、c3202[10][11][12]
1524PS	c3201、c3202
1524SB、1130、1240、屋内 802.11n メッシュ アクセス ポイント	c3201、c3205

9 Cisco 3200 に 802.11a 無線または 4.9 GHz 帯域で接続する場合は、AP1522 でユニバーサル アクセスが有効である必要があります。
10 モデル c3201 は、802.11b/g 無線（2.4 GHz）が搭載された Cisco 3200 です。
11 モデル c3202 は、4.9 GHz サブバンド無線が搭載された Cisco 3200 です。
12 モデル c3205 は、802.11a 無線（5.8 GHz サブバンド）が搭載された Cisco 3200 です。

AP1522 で Cisco 3200 とアソシエートできるようにする手順は、次のとおりです。

Public Safety 4.9 GHz 帯域の設定ガイドライン

AP1522 または AP1524PS と Cisco 3200 を Public Safety ネットワークで相互運用するには、次の設定時のガイドラインを満たす必要があります。

- バックホールでクライアント アクセスを有効にする必要があります（メッシュ グローバル パラメータ）。 この機能は AP1524PS ではサポートされません。
- メッシュ ネットワーク内のすべてのメッシュ アクセス ポイント（MAP）でグローバルに Public Safety への対応を有効にする必要があります。
- AP1522 または AP1524PS でのチャネル番号の割り当てが Cisco 3200 無線インターフェイスでの割り当てと一致する必要があります。
  - Cisco 3200 との相互運用性を実現するために、チャネル 20（4950 GHz）～ 26（4980 GHz）、およびサブバンド チャネル 1 ～ 19（5 および 10 MHz）が使用されます。 この設定の変更はコントローラで行います。 メッシュ アクセス ポイントの設定は変更されません。
  - チャネル割り当ては、RAP に対してのみ行われます。 MAP へのアップデートは、RAP によって伝搬されます。

Cisco 3200 のデフォルトのチャネル幅は 5 MHz です。 チャネル幅を 10 または 20 MHz に変更して WGB が AP1522 および AP1524PS とアソシエートできるようにするか、AP1522 または AP1524PS

のチャネルを 5 MHz 帯域（チャネル 1 ～ 10）または 10 MHz 帯域（チャネル 11 ～ 19）のチャネルに変更する必要があります。

- 無線（802.11a）は、チャネルの設定時に無効にし、CLI の使用時に再び有効にする必要があります。 GUI を使用する場合、チャネルの設定時に 802.11a 無線をイネーブルおよびディセーブルにする必要はありません。
- Cisco 3200 は、5、10、または 20 MHz 帯域内のチャネルをスキャンできます。ただし、これらの帯域をまたがるようにはスキャンできません。

AP1522 が Cisco 3200 とアソシエートできるように設定（GUI）

ステップ 1 クライアント アクセスのバックホールを有効にするには、[Wireless] > [Mesh] の順に選択して、[Mesh] ページにアクセスします。

ステップ 2 バックホール クライアント アクセスの [Enabled] チェックボックスをオンにして、802.11a 無線を介したワイヤレス クライアントのアソシエーションを許可します。 [Apply] をクリックします。

（注） ネットワークでバックホールクライアントアクセスを有効にするためにすべてのメッシュ アクセス ポイントをリブートするように許可するかどうかを確認するメッセージが表示されます。 [OK] をクリックします。

ステップ 3 バックホールに使用するチャネル（チャネル 20 ～ 26）を割り当てるには、[Wireless] > [Access Points] > [Radio] をクリックし、[Radio] サブヘッダーから [802.11a/n] を選択します。 すべての 802.11a 無線に関する概要ページが表示されます。

ステップ 4 適切な RAP の [Antenna] ドロップダウン リストで、[Configure] を選択します。 [Configure] ページが表示されます。

ステップ 5 [RF Channel Assignment] セクションで、[Assignment Method] オプションとして [WLC Controlled] オプションを選択し、1 ～ 26 の間の任意のチャネルを選択します。

ステップ 6 [Apply] をクリックして、変更を確定します。

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

Cisco 3200 と 1522 および 1524PS とのアソシエーションの有効化（CLI）

ステップ 1 AP1522 でクライアント アクセス モードを有効にするには、次のコマンドを入力します。
config mesh client-access enable

ステップ 2 グローバルに Public Safety を有効にするには、次のコマンドを入力します。
config mesh public-safety enable *all*

ステップ 3 Public Safety チャネルを有効にするには、次のコマンドを入力します。

1 AP1522 では、次のコマンドを入力します。

config 802.11a disable *Cisco_MAP*

config 802.11a channel ap *Cisco_MAP channel number*

config 802.11a enable *Cisco_MAP*

2 AP1524PS では、次のコマンドを入力します。

config 802.11–a49 disable *Cisco_MAP*

config 802.11–a49 channel ap *Cisco_MAP channel number*

config 802.11–a49 enable *Cisco_MAP*

（注） 5.8-GHz 無線を有効にするには、**config 802.11–a58 enable** *Cisco_MAP* コマンドを入力します。

（注） AP1522 と AP1524PS の両方では、*channel number* は 1 ～ 26 の任意の値です。

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 設定を確認するには、次のコマンドを入力します。
show mesh public-safety

show mesh client-access

show ap config 802.11a summary（1522 のみ）

show ap config 802.11–a49 summary（1524PS のみ）

（注） **show config 802.11-a58 summary** コマンドを入力して 5.8 GHz 無線の設定詳細を表示します。

電力およびチャネルの設定

バックホール チャネル（802.11a/n）は、RAP 上で設定できます。 MAP は、RAP チャネルに合わされます。 ローカル アクセスは、MAP とは無関係に設定できます。

電力およびチャネルの設定（GUI）

ステップ 1 [Wireless] > [Access Points] > [802.11a/n] の順に選択します。
無線スロットは各無線に対して表示されます。 AP1524SB の場合は、802.11a/n 無線は 5 GHz 帯域で動作するスロット 1 および 2 に対して表示されます。 AP1524PS の場合は、それぞれ 5 GHz 帯域と 4.9 GHz 帯域で動作するスロット 1 および 2 に対して 802.11a/n 無線が表示されます。

ステップ 2 802.11 a/n 無線の [Antenna] ドロップダウン リストで、[Configure] を選択します。 [Configure] ページが表示されます。

（注） 1524SB の場合は、[Antenna] ドロップダウン リストで、Radio Role が DOWNLINK の RAP を選択します。

ステップ 3 無線のチャネル（[AP Controlled] および [WLC Controlled] の割り当て方法）を割り当てます。

（注） チャネルを AP1524SB に割り当てる場合は、[WLC Controlled] 割り当て方法を選択し、5 GHz 帯域のサポートされたいずれかのチャネルを選択します。

ステップ 4 無線の送信電力レベル（[AP Controlled] および [WLC Controlled]）を割り当てます。
AP1500 の 802.11a バックホールでは、選択可能な 5 つの電力レベルがあります。

（注） バックホールのデフォルトの送信電力レベルは最大電力レベル（レベル 1）です。

（注） Radio Resource Management（RRM）はデフォルトでオフ（無効）になります。 バックホールでは RRM をオン（有効）にすることができません。

ステップ 5 電力およびチャネルの割り当てが完了したら、[Apply] をクリックします。

ステップ 6 [802.11a/n Radios] ページで、チャネルの割り当てが正しく行われたことを確認します。

シリアル バックホールでのチャネルの設定（CLI）

ステップ 1 RAP のスロット 2 にある無線のバックホール チャネルを設定するには、次のコマンドを入力します。
config slot 2 channel ap *Cisco_RAPSB channel*

5.8 GHz 帯域で使用可能なチャネルは、149、153、157、161、および 165 です。

ステップ 2 RAP のスロット 2 にある無線の送信電力レベルを設定するには、次のコマンドを入力します。
config slot 2 txPower ap *Cisco_RAPSB power*

有効な値は 1 ～ 5 で、デフォルト値は 1 です。

ステップ 3 メッシュ アクセス ポイントの設定を表示するには、次のコマンドを入力します。

- **show mesh path** *MAP*

以下に類似した情報が表示されます。

AP Name/Radio	Channel	Rate	Link-Snr	Flags	State
MAP1SB	161	auto	60	0x10ea9d54	UPDATED NEIGH PARENT BEACON
RAPSB	153	auto	51	0x10ea9d54	UPDATED NEIGH PARENT BEACON

```
RAPSB is a Root AP.
```

- **show mesh backhaul** *RAPSB*

以下に類似した情報が表示されます。

```
Current Backhaul Slot(s)..................... 1, 2,

Basic Attributes for Slot 1
    Radio Type.............................. RADIO_TYPE_80211a
    Radio Role.............................. ACCESS
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
    Current Tx Power Level ................. 1
    Current Channel ........................ 165
    Antenna Type............................ EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBm units)...... 0

Basic Attributes for Slot 2
    Radio Type.............................. RADIO_TYPE_80211a
    Radio Role.............................. RADIO_DOWNLINK
    Administrative State ................... ADMIN_ENABLED
    Operation State ........................ UP
    Current Tx Power Level ................. 3
    Current Channel ........................ 153
    Antenna Type............................ EXTERNAL_ANTENNA
    External Antenna Gain (in .5 dBm units)...... 0
```

- **show ap channel** *MAP1SB*

以下に類似した情報が表示されます。

```
802.11b/g Current Channel ................. 11
Slot Id ................................... 0
Allowed Channel List....................... 1,2,3,4,5,6,7,8,9,10,11
802.11a(5.8Ghz) Current Channel ........... 161
Slot Id ................................... 1
Allowed Channel List....................... 149,153,157,161,165
802.11a(5.8Ghz) Current Channel ........... 153
Slot Id ................................... 2
Allowed Channel List....................... 149,153,157,161,165
```

アンテナ ゲインの設定

コントローラの GUI または CLI を使用して、取り付けられているアンテナのアンテナ ゲインと一致するように、メッシュ アクセス ポイントのアンテナ ゲインを設定する必要があります。

アンテナ ゲインの設定（GUI）

ステップ 1 [Wireless] > [Access Points] > [Radio] > [802.11a/n] の順に選択して、[802.11a/n Radios] ページを開きます。

ステップ 2 設定するメッシュ アクセス ポイントのアンテナについて、一番右の青色の矢印にマウスを移動してアンテナのオプションを表示します。 [Configure] を選択します。

（注） 外部アンテナだけに設定可能なゲイン設定があります。

ステップ 3 [Antenna Parameters] エリアで、アンテナ ゲインを入力します。
ゲインは 0.5 dBm 単位で入力します。 たとえば、2.5 dBm = 5 です。

（注） 入力するゲイン値は、アンテナのベンダーが指定した値と同じにする必要があります。

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

アンテナ ゲインの設定（CLI）

コントローラの CLI を使用して 802.11a バックホール無線のアンテナ ゲインを設定するには、次のコマンドを入力します。

config 802.11a antenna extAntGain *antenna_gain AP_name*

ここで、ゲインは 0.5 dBm 単位で入力します（たとえば、2.5 dBm の場合は 5 になります）。

シリアル バックホール アクセス ポイントでのバックホール チャネル選択解除

この機能は、1524SB（シリアル バックホール）などの、2 つの 5 GHz 無線があるメッシュ AP に適用できます。

バックホール チャネル選択解除機能を使用すると、シリアル バックホール MAP および RAP に割り当てることができるチャネルのセットを制限できます。 1524SB MAP チャネルは自動的に割り当てられるため、この機能を使用すると、メッシュアクセスポイントに割り当てられるチャネルのセットを制限できます。 たとえば、チャネル 165 をどの 1524SB メッシュ アクセス ポイントにも割り当てない場合は、DCA リストからチャネル 165 を削除し、この機能を有効にする必要があります。

DCA リストから特定のチャネルを削除し、**mesh backhaul dca-channel** コマンドを有効にする場合、これらのチャネルはどのシナリオのどのシリアル バックホール アクセス ポイントにも割り当てられません。 DCA リスト チャネル内のすべてのチャネルでレーダーが検出された場合であっても、無線は DCA リスト チャネル外のチャネルに移動するのではなくシャットダウンされます。 トラップ メッセージが WCS に送信され、DFS のため、無線がシャット ダウンされたことを示すメッセージが表示されます。 **config mesh backhaul dca-channels enable** コマンドが有効な場合は、DCA リストの外部のシリアル バックホール RAP にチャネルを割り当てることはできません。 ただし、これは、1552、1522、1524PS AP などの、1 つの 5 GHz 無線がある AP には該当しません。

これらの AP の場合は、RAP に対する DCA リスト外部の任意のチャネルを割り当てることができ、DCA リストからレーダーフリーのチャネルを利用できない場合に、コントローラまたは AP が DCA リストの外部のチャネルも選択できます。

この機能は、屋外アクセス ポイントとは異なるチャネル セットをサポートする屋内メッシュ アクセス ポイントまたはワークグループ ブリッジを使用する相互運用性シナリオに最適です。 たとえば、チャネル 165 は外部アクセス ポイントによりサポートされますが、-A ドメインの屋内アクセス ポイントによりサポートされません。 バックホール チャネル選択解除機能を有効にすると、屋内アクセスポイントと屋外アクセスポイントに共通なチャネルにのみチャネルの割り当てを制限できます。

（注） チャネル選択解除は、7.0 以降のリリースに適用できます。

一部のシナリオでは、モビリティのために2つの直線的な線路や道路が共存する場合があります。 MAP のチャネル選択は自動的に行われるため、1 つのチャネルに 1 つのホップが存在することがあります（これは自律側では利用できません）。あるいは、同じチャネルまたは隣接するチャネルが、異なる並びに属する領域アクセス ポイントで選択された場合に、チャネルをスキップする必要があります。

バックホール チャネル選択解除の設定（GUI）

ステップ 1 [Controller] > [Wireless] > [802.11a/n] > [DCA] の順に選択します。
[Dynamic Channel Assignment Algorithm] ページが表示されます。

ステップ 2 DCA リストに含めるチャネルを 1 つまたは複数選択します。
DCA リストに含まれるチャネルは、自動チャネル割り当て中にこのコントローラにアソシエートされたアクセス ポイントに割り当てられません。

ステップ 3 [Wireless] > [Mesh] の順に選択します。
[Mesh] ページが表示されます。

ステップ 4 [Mesh DCA Channels] チェックボックスをオンにして、DCA リストを使用したバックホール チャネル選択解除を有効にします。 このオプションは、シリアル バックホール アクセス ポイントに適用できます。

ステップ 5 バックホール選択解除オプションを有効にした後に、[Wireless] > [Access Points] > [Radios] > [802.11a/n] の順に選択して RAP ダウンリンク無線のチャネルを設定します。

ステップ 6 アクセス ポイントのリストから、RAP の [Antenna] ドロップダウン リストをクリックし、[Configure] を選択します。
[Configure] ページが表示されます。

ステップ 7 [RF Backhaul Channel] 割り当てセクションで、[Custom] を選択します。

ステップ 8 [Custom] を選択したときに表示されるドロップダウン リストから RAP ダウンリンク無線のチャネルを選択します。

ステップ 9 [Apply] をクリックして、バックホール チャネル選択解除設定の変更を適用し、保存します。

バックホール チャネル選択解除の設定（CLI）

ステップ 1 DCA リストですでに設定されたチャネル リストを確認するには、次のコマンドを入力します。
show advanced 802.11a 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
  Anchor time (Hour of the day)............... 0
  Channel Update Contribution................. SNI..
  CleanAir Event-driven RRM option............ Enabled
  CleanAir Event-driven RRM sensitivity....... Medium
  Channel Assignment Leader................... 09:2b:16:28:00:03
  Last Run.................................... 286 seconds ago
  DCA Sensitivity Level....................... MEDIUM (15 dB)
  DCA 802.11n Channel Width................... 20 MHz
  DCA Minimum Energy Limit.................... -95 dBm
  Channel Energy Levels
    Minimum................................... unknown
    Average................................... unknown
    Maximum................................... unknown
  Channel Dwell Times
    Minimum................................... 0 days, 17 h 02 m 05 s
    Average................................... 0 days, 17 h 46 m 07 s
    Maximum................................... 0 days, 18 h 28 m 58 s
  802.11a 5 GHz Auto-RF Channel List

--More-- or (q)uit
    Allowed Channel List...................... 36,40,44,48,52,56,60,64,116,
                                               140
    Unused Channel List....................... 100,104,108,112,120,124,128,
                                               132,136
  DCA Outdoor AP option....................... Disabled
```

ステップ 2 DCA リストにチャネルを追加するには、**config advanced 802.11a channel add** *channel number* コマンドを入力します。*channel number* は、DCA リストに追加するチャネル番号です。
また、**config advanced 802.11a channel delete** *channel number* コマンドを入力して、DCA リストからチャネルを削除することもできます。*channel number* は、DCA リストから削除するチャネル番号です。

DCA リストに対してチャネルを追加または削除する前に、802.11a ネットワークが無効であることを確認します。

- 802.11a ネットワークをディセーブルにするには、次のコマンドを入力します。

  config 802.11a disable network

- 802.11a ネットワークをイネーブルにするには、次のコマンドを入力します。

  config 802.11a enable network

  チャネルが 1524 RAP に割り当てられている場合は、DCA リストからそのチャネルを直接削除できません。 RAP に割り当てられたチャネルを削除するには、最初に、RAP に割り当てられたチャネルを変更し、次にコントローラから **config advanced 802.11a channel delete** *channel number* コマンドを入力する必要があります。

  次に、**add channel** コマンドと **delete channel** コマンドの出力例を示します。

```
(Controller) > config 802.11a disable network

Disabling the 802.11a network may strand mesh APs. Are you sure you want to continue? (y/n)y


(Controller) > config advanced 802.11a channel add 132


(Controller) > config advanced 802.11a channel delete 116

802.11a 5 GHz Auto-RF:
Allowed Channel List..................... 36,40,44,48,52,56,60,64,116,
                                          132,140
DCA channels for cSerial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul Mesh
APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y


Failed to delete channel.
Reason: Channel 116 is configured for one of the Serial Backhaul RAPs.
Disable mesh backhaul dca-channels or configure a different channel for Serial Backhaul RAPs.

(Controller) > config advanced 802.11a channel delete 132

  802.11a 5 GHz Auto-RF:
Allowed Channel List..................... 36,40,44,48,52,56,60,64,116,132,140
DCA channels for Serial Backhaul Mesh APs is enabled.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul Mesh
APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y

(Controller) > config 802.11a enable network
```

ステップ 3 適切な DCA リストが作成された後に、**config mesh backhaul dca-channels enable** コマンドを入力して、メッシュ アクセス ポイントのバックホール チャネル選択解除機能を有効にします。
メッシュ アクセス ポイントのバックホール チャネル選択解除機能を無効にする場合は、**config mesh backhaul dca-channels disable** コマンドを入力します。

この機能を有効または無効にするために 802.11a ネットワークを無効にする必要はありません。

次に、出力例を示します。

```
(Controller) > config mesh backhaul dca-channels enable
  802.11a 5 GHz Auto-RF:
    Allowed Channel List..................... 36,40,44,48,52,56,60,64,116,
                                              140
Enabling DCA channels for c1524 mesh APs will limit the channel set to the DCA channel list.
DCA list should have at least 3 non public safety channels supported by Serial Backhaul Mesh APs.
Otherwise, the Serial Backhaul Mesh APs can get stranded.
Are you sure you want to continue? (y/N)y

(Controller) > config mesh backhaul dca-channels disable
```

ステップ 4 バックホール チャネル選択解除機能の現在のステータスを確認するには、**show mesh config** コマンドを入力します。
次に、出力例を示します。

```
(Controller) > show mesh config

Mesh Range..................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. enabled
Background Scanning State...................... enabled
Backhaul Amsdu State........................... disabled

Mesh Security
   Security Mode............................... PSK
   External-Auth............................... enabled
      Radius Server 1.......................... 209.165.200.240
   Use MAC Filter in External AAA server..... disabled
   Force External Authentication.............. disabled

Mesh Alarm Criteria
   Max Hop Count............................... 4
   Recommended Max Children for MAP............ 10
   Recommended Max Children for RAP............ 20
   Low Link SNR................................ 12
   High Link SNR............................... 60
   Max Association Number...................... 10
   Association Interval........................ 60 minutes
   Parent Change Numbers....................... 3

--More-- or (q)uit
   Parent Change Interval...................... 60 minutes
```

```
Mesh Multicast Mode............................. In-Out
Mesh Full Sector DFS............................ enabled


Mesh Ethernet Bridging VLAN Transparent Mode..... enabled

Mesh DCA channels for Serial Backhaul APs..... disabled
```

ステップ 5 **config slot** *slot number* **channel ap** *ap-name channel number* コマンドを入力して、特定のチャネルを 1524 RAP ダウンリンク無線に割り当てます。

- *slot number* は、チャネルが割り当てられたダウンリンク無線のスロットを示します。
- *ap-name* は、チャネルが設定されたアクセス ポイントの名前を示します。
- *channel number* は、アクセス ポイントのスロットに割り当てられたチャネルを示します。

1524 RAP のスロット 2 はダウンリンク無線として動作します。 バックホール チャネル選択解除が有効な場合は、DCA リストで利用可能なチャネルのみをアクセス ポイントに割り当てることができます。

次に、出力例を示します。

```
(Controller) > config slot 2 channel ap Controller-RAP2-1524 136
Mesh backhaul dca-channels is enabled. Choose a channel from the DCA list.
(Controller) > config slot 2 channel ap Controller-RAP2-1524 140
```

バックホール チャネル選択解除のガイドライン

バックホール チャネルの選択解除を設定する場合は、次のガイドラインに従います。

- シリアル バックホール RAP 11a アクセス無線とシリアル バックホール MAP の両方の 11a 無線のチャネルは自動的に割り当てられます。 これらのチャネルは設定できません。
- コントローラでトラップ ログを探します。 レーダー検出および後続のチャネル変更が起こった場合、次のようなメッセージが表示されます。

```
Channel changed for Base Radio MAC: 00:1e:bd:19:7b:00 on 802.11a
radio. Old channel: 132. New Channel: 116. Why: Radar. Energy
before/after change: 0/0. Noise before/after change: 0/0.
Interference before/after change: 0/0.

Radar signals have been detected on channel 132 by 802.11a radio
with MAC: 00:1e:bd:19:7b:00 and slot 2
```

- 各シリアル バックホール AP に対して、ダウンリンク無線とアップリンク無線のチャネルは常に干渉しない必要があります（たとえば、アップリンクがチャネル 104 である場合、100、104、および 108 のチャネルをその AP のダウンリンク無線に割り当てることはできません）。 また、RAP の 11a アクセス無線には別の隣接チャネルが選択されます。

- レーダー信号がアップリンク無線チャネルを除くすべてのチャネルで検出された場合、ダウンリンク無線はシャットダウンされ、アップリンク無線はアップリンクおよびダウンリンクの両方として動作します（つまり、この場合、動作は 1522 AP に類似します）。
- レーダーの検出は 30 分後にクリアされます。 レーダー検出のためシャット ダウンされたすべての無線は、この時間の経過後に再び稼働します。
- DFS 対応チャネルへの移動直後に 60 秒間のサイレント期間が発生します（チャネルの変更がレーダー検出によるか、RAP の場合のユーザ設定によるかに関係ありません）。この期間の間、AP は何も伝送せずにレーダー信号をスキャンします。 新しいチャネルも DFS 対応である場合は、レーダー検出のため、短い期間（60 秒）のダウンタイムが発生することがあります。 サイレント期間中に新しいチャネルでレーダーが再び検出された場合は、サイレント期間中の伝送が許可されてないため、親 AP が子 AP に通知せずにチャネルを変更します。この場合、子 AP はアソシエート解除され、スキャンモードに戻り、新しいチャネルで親 AP を再検出し、再び join します。この場合は、若干長い（約 3 分）ダウンタイムが発生します。
- RAP の場合、ダウンリンク無線のチャネルは、バックホール チャネル選択解除機能が有効になっているかどうかに関係なく、常に DCA リスト内から選択されます。 MAP の場合は、動作が異なります。これは、バックホール チャネル選択解除機能が有効でない限り、MAP はそのドメインに許可された任意のチャネルを選択できるためです。 バックホール チャネル選択解除機能が使用されていない場合であっても、チャネルが足りないため無線がシャットダウンされることを防ぐために、802.11a DCA チャネル リストに多数のチャネルを追加することをお勧めします。
- RRM 機能に使用された DCA リストはバックホール チャネル選択解除機能を介してメッシュ AP にも使用されるため、DCA リストに対してチャネルを追加または削除すると、非メッシュ アクセス ポイントの RRM 機能に入力されたチャネル リストも影響を受けることに注意してください。 RRM ではメッシュがオフになっています。
- -M ドメイン AP の場合は、メッシュ ネットワークが稼働するまで若干長い時間（通常よりも 25 ～ 50 % 長い時間）が必要になることがあります。これは、各 AP が親 AP に join する前にスキャンする、-M ドメインの DFS 対応チャネルのリストが長いためです。

動的チャネル割り当ての設定（GUI）

RRM スキャンに使用されるチャネルを選択する際に動的チャネル割り当て（DCA）アルゴリズムで考慮されるチャネルを、コントローラの GUI を使用して指定する手順は、次のとおりです。 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。

（注） ここで説明する手順は、メッシュ ネットワークのみに関係します。

ステップ 1 802.11a/n または 802.11b/g/n ネットワークを無効にする手順は、次のとおりです。

a) [Wireless] > [802.11a/n] 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）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックして、変更を確定します。

ステップ 2 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [DCA] の順に選択して、[802.11a（または 802.11b/g）> RRM > 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、コントローラの DCA モードを指定します。

- [Automatic]：コントローラは join しているすべてのメッシュ アクセス ポイントのチャネル割り当てを定期的に評価し、必要に応じて更新するようにします。 768 ビットは、デフォルト値です。
- [Freeze]：[Invoke Channel Update Once] をクリックしたときに限り、コントローラは必要に応じて join しているすべてのメッシュ アクセス ポイントのチャネル割り当てを評価して更新します。

  （注） [Invoke Channel Update Once] をクリックしても、すぐにチャネル割り当ての評価と更新が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 をオフにし、すべてのメッシュアクセスポイント無線をデフォルトで帯域の最初のチャネルに設定します。 このオプションを選択する場合は、すべての無線のチャネルを手動で割り当てる必要があります。

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。

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、コントローラの RRM アルゴリズムによって、Lightweight アクセス ポイントにチャネルを割り当てるときに、外部アクセス ポイント（ワイヤレス ネットワークに含まれないアクセス 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、このチェックボックスをオフにします。 たとえばRRM では、外部アクセス ポイントに近いチャネルをアクセス ポイントが回避するようにチャ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、コントローラの RRM アルゴリズムによって、チャネルを割り当てるときに、ワイヤレス 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、このチェックボックスをオフにしま

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、コントローラの RRM アルゴリズムによって、Lightweight アクセス ポイントにチャネルを割り当てるときに、チャネルのノイズ（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、このチェックボックスをオフにします。 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 [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、無線帯域によって異なります。

表 *31*：*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 10 802.11a/n ネットワークの場合のみ、次のいずれかの[Channel Width] 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ネル帯域幅を指定します。

- [20 MHz]：20 MHz のチャネル帯域幅（デフォルト）

（注） [802.11a/n Cisco APs] > [Configure] ページで 20 MHz モードのアクセス ポイントの無線を静的に設定することで、グローバルに設定されたDCAチャネル幅設定を上書きすることができます。 アクセス ポイント無線で静的 RF チャ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以前に使用していたチャネル幅設定が上書きされます。

このページには、次のような変更できないチャネル パラメータの設定も表示されます。

- [Channel Assignment Leader]：チャネル割り当てを行う RF グループ リーダーの MAC アドレス。
- [Last Auto Channel Assignment]：RRM が現在のチャネル割り当てを最後に評価した時間。

ステップ 11 [DCA Channel List] の [DCA Channels] フィールドには、現在選択されているチャネルが表示されます。チャネルを選択するには、[Select] カラムでそのチャネルのチェックボックスをオンにします。 チャネルを除外するには、チャネルのチェックボックスをオフにします。
範囲：?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：?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 チャネル（100、104、108、112、116、132、136、および 140）は、チャネル リストには表示されません。 -E 規制ドメインに Cisco Aironet 1500 シリーズ メッシュ アクセス ポイントがある場合は、運用を開始する前に、DCA チャネル リストにこれらのチャ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、これらのチャネルが DCA チャネル リストに含まれていることを確認します。 チャネル リストにこれらのチャネルを含めるには、[Extended UNII-2 Channels] チェックボックスをオンにします。

ステップ 12 ネットワークで AP1500 を使用している場合は、4.9 GHz チャネルが動作する 802.11a 帯域で 4.9 GHz チャ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。 チャネルを除外するには、チャネルのチェックボックスをオフにします。
範囲：?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：?802.11a：20、26

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 14 802.11a または 802.11b/g ネットワークを再び有効にする手順は、次のとおりです。

1. [Wireless] > [802.11a/n] または [802.11b/g/n] > [Network] の順にクリックして、[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] をクリックして、変更を確定します。

ステップ 15 [Save Configuration] をクリックして、変更を保存します。
DCA アルゴリズムによってチャネルが変更された理由を確認するには、[Monitor] をクリックし、次に [Most Recent Traps] の下にある [View All] をクリックします。 トラップにより、チャネルが変更された無線の MAC アドレス、前のチャネルと新規のチャネル、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。

拡張機能の設定

この項では、次のトピックについて取り上げます。

• バックホール用 2.4 GHz 無線の使用

- ユニバーサル クライアント アクセス
- シリアル バックホール アクセス ポイントのユニバーサル クライアント アクセス
- イーサネット VLAN タギングの設定
- ワークグループ ブリッジとメッシュ インフラストラクチャとの相互運用性
- クライアント ローミング
- 屋内メッシュ ネットワークの音声パラメータの設定
- ビデオのメッシュ マルチキャストの抑制の有効化
- IGMP スヌーピング
- メッシュ AP のローカルで有効な証明書

バックホール用 2.4 GHz 無線の使用

7.0 リリースまで、メッシュではバックホール用に 5 GHz 無線が使用され、2.4 GHz 無線はクライアント アクセスにのみ使用されていました。 バックホール用に 5 GHz 無線のみを使用する理由は次のとおりです。

- より多くのチャネルが利用可能である
- より多くの EIRP が利用可能である
- 干渉が少ない
- ほとんどのクライアント アクセスが 2.4 GHz 帯域を介して行われる

ただし、葉が生い茂った地域などの特定の状況では、2.4 GHz の方がペネトレーションが優れているため、バックホール用に 2.4 GHz を使用する必要がある場合がありました。

7.0.116.0 リリースでは、メッシュ ネットワーク全体が 5 GHz または 2.4 GHz の単一バックホールを使用するよう設定できます。

注意 この機能は、AP1522（2 つの無線）だけで使用できます この機能は、5 GHz バックホール オプションを理解した後に使用する必要があります。

注意 最初のオプションとして 5 GHz を使用し、5 GHz オプションが動作しない場合にのみ、2.4 GHz を使用することをお勧めします。

5 GHz から 2.4 GHz へのバックホールの変更

コマンドへの引数として RAP 名のみを指定する場合は、メッシュ セクター全体が 2.4 GHz または 5 GHz バックホールに変更されます。 バックホールの変更（2.4 GHz から 5 GHz、または 5 GHz から 2.4 GHz）を示す警告メッセージが表示されます。

（注） 2.4 GHz バックホールは、コントローラのユーザ インターフェイスを使用して設定できず、CLI を使用することによってのみ設定できます。

1. バックホールを変更するには、次のコマンドを入力します。

   `(Cisco Controller) >` **config mesh backhaul slot 0 enable** *RAP*

   次のメッセージが表示されます。

   ```
   Warning! Changing backhaul slot will bring down the mesh for renegotiation!!!
   After backhaul is changed, 5 GHz client access channels need to be changed manually

   Are you sure you want to continue? (y/N)
   ```

2. **y** を押します。

（注） 5 GHz バックホールをローカル クライアント アクセスに変更する場合は、クライアント アクセス用のバックホール周波数がこれらの 5 GHz 無線でポートされるため、すべての AP の 5 GHz クライアント アクセス周波数は同じになります。 優れた周波数プランニングを行うには、これらのチャネルを設定する必要があります。

2.4 GHz から 5 GHz へのバックホールの変更

ステップ 1 バックホールを変更するには、次のコマンドを入力します。

`(Cisco Controller) >` **config mesh backhaul slot 1 enable** `RAP`

次のメッセージが表示されます。

```
Warning! Changing backhaul slot will bring down the mesh for renegotiation!!!
Are you sure you want to continue? (y/N)
```

ステップ 2 **y** を押します。

（注） 2.4 GHz バックホールは、コントローラの GUI を使用して設定できませんが、CLI を使用して設定できます。

現在使用中のバックホールの確認

使用中の現在のバックホールを確認するには、次のコマンドを入力します。

```
(Cisco Controller) > show mesh backhaul AP_name
```

（注） 5 GHz バックホールの場合、動的周波数選択（DFS）は 2.4 GHz ではなく 5 GHz のみで行われます。 このメカニズム（RAP と MAP では異なります）は、調整変更メカニズムと呼ばれます。 5 GHz がバックホールからクライアント アクセスに変換された場合、または 2.4 GHz がバックホールとして使用される場合は、DFS がローカル モード AP の場合と同様に動作します。 DFS は 5 GHz クライアント アクセスで検出され、新しいチャネルの要求がコントローラに送信されます。 2.4 GHz バックホールに対するメッシュの隣接は影響を受けません。

（注） 2.4 GHz バックホールではユニバーサル クライアント アクセスを利用できません。

ユニバーサル クライアント アクセス

ユニバーサル クライアント アクセスが有効な場合は、バックホール無線を介したワイヤレス クライアントアソシエーションが許可されます。 一般的に、バックホール無線は、バックホールが 2.4 GHz である可能性がある 1522 を除くほとんどのメッシュ アクセス ポイントで 5 GHz 無線です。 つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

ユニバーサル クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント アソシエーションは 2 番目の無線のみを介して送信されます。

（注） ユニバーサル クライアント アクセスはデフォルトで無効になります。 この機能をイネーブルにすると、すべてのメッシュ アクセス ポイントがリブートします。

この機能は、1524PS を除く、2 つ以上の無線があるメッシュ アクセス ポイント（1552、1524SB、1522、メッシュ モードの屋内 AP）に適用できます。

ユニバーサル クライアント アクセスの設定（GUI）

ステップ 1 [Wireless] > [Mesh] の順に選択して、[Mesh] ページを開きます。

ステップ 2 [Backhaul Client Access] チェックボックスをオンにします。

すべてのメッシュ AP がリブートされるプロンプトが表示されます。

ステップ 3 [OK] をクリックして作業を続行します。

ユニバーサル クライアント アクセスの設定（CLI）

次のコマンドを使用して、ユニバーサル クライアント アクセスを有効にします。

```
(Cisco Controller)> config mesh client-access enable
```

次のメッセージが表示されます。

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

シリアル バックホール アクセス ポイントのユニバーサル クライアント アクセス

ユニバーサル クライアント アクセスを使用すると、バックホール機能に加えてバックホール 802.11a 無線でのクライアント アクセスが提供されます。 この機能は、1524PS を除く、2 つ以上の無線があるメッシュ アクセス ポイント（1552、1524SB、1522、メッシュ モードの屋内 AP）に適用できます。

デュアル 5 GHz ユニバーサル クライアント アクセス機能は、3 つの無線スロットがあるシリアル バックホール アクセス ポイント プラットフォームを対象としています。 スロット 0 の無線は、2.4 GHz 帯域で動作し、クライアント アクセスに使用されます。 スロット 1 とスロット 2 の無線は 5 GHz 帯域で動作し、主にバックホールに使用されます。 ただし、ユニバーサル クライアント アクセス機能により、クライアントはスロット 1 無線を介してアソシエートすることが許可されていました。 また、スロット 2 無線はバックホールにのみ使用されていました。 7.0 リリースでは、このデュアル 5 GHz ユニバーサル アクセス機能を使用して、スロット 2 無線を介したクライアント アクセスが許可されます。

デフォルトでは、両方のバックホール無線を介したクライアントアクセスが無効になります。次のガイドラインに従って、ダウンリンクまたはアップリンクとして使用される無線に関係なく、5 GHz 無線を提供する無線スロットでクライアント アクセスを有効または無効にします。

- スロット 2 でクライアント アクセスが無効であっても、スロット 1 でクライアント アクセスを有効にできます。
- スロット 2 のクライアント アクセスは、スロット 1 でクライアント アクセスが有効な場合にのみ有効にできます。
- スロット 1 でクライアント アクセスを無効にすると、スロット 2 のクライアント アクセスは CLI で自動的に無効になります。

- 拡張されたクライアント アクセス（スロット 2 無線）のみを無効にするには、GUI を使用します。
- クライアント アクセスが有効または無効になると、常にすべてのメッシュ アクセス ポイントがリブートされます。

2 つの 802.11a バックホール無線は、同じ MAC アドレスを使用します。 複数のスロットの同じ BSSID に対して WLAN をマッピングする場合があります。 本書では、スロット 2 無線のクライアント アクセスは、Extended Universal Access（EUA）と呼ばれます。

Extended Universal Access の設定（GUI）

ステップ 1 [Wireless] > [Mesh] の順に選択します。
[Controller GUI when Backhaul Client Access is disabled] ページが表示されます。

ステップ 2 [Backhaul Client Access] チェックボックスをオンにして、[Extended Backhaul Client Access] チェックボックスを表示します。

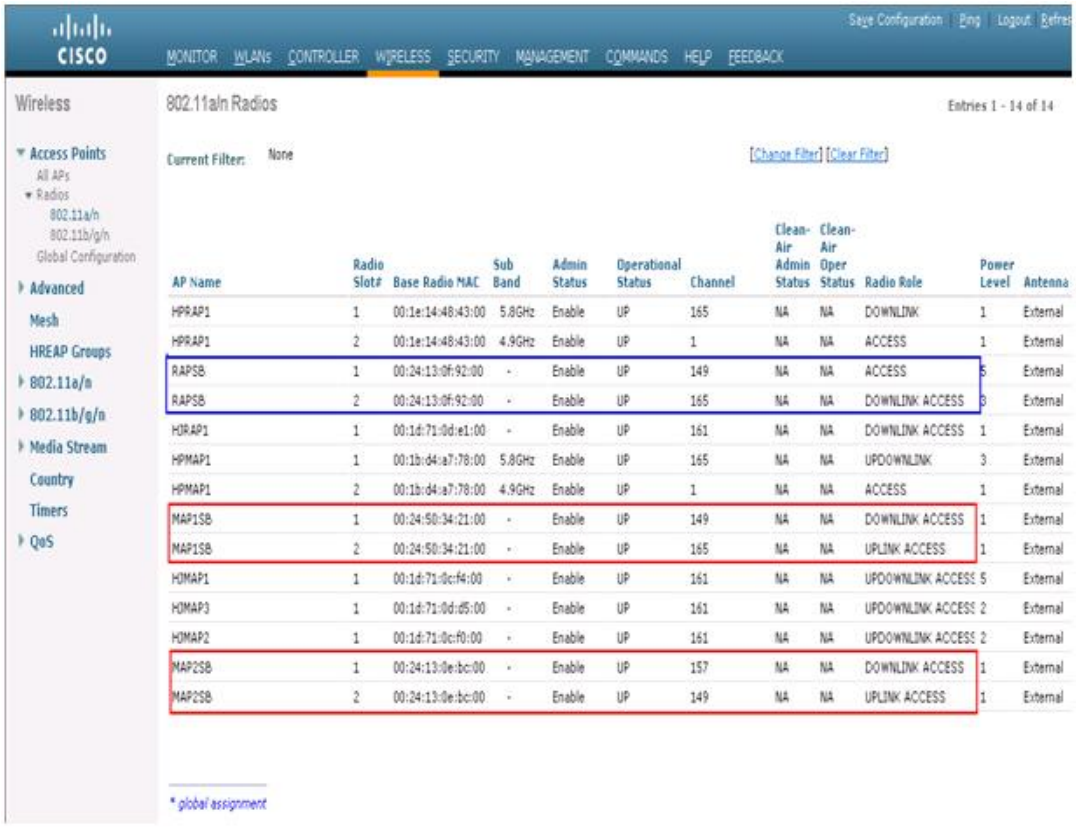
ステップ 3 [Extended Backhaul Client Access] チェックボックスをオンにし、[Apply] をクリックします。
すべてのメッシュ AP がリブートされるプロンプトが表示されます。

ステップ 4 [OK] をクリックして作業を続行します。

次の作業

EUA を有効になった後、802.11a 無線が次の図に示されているように表示されます。

図 *66*：*EUA* の有効後の *802.11a* 無線

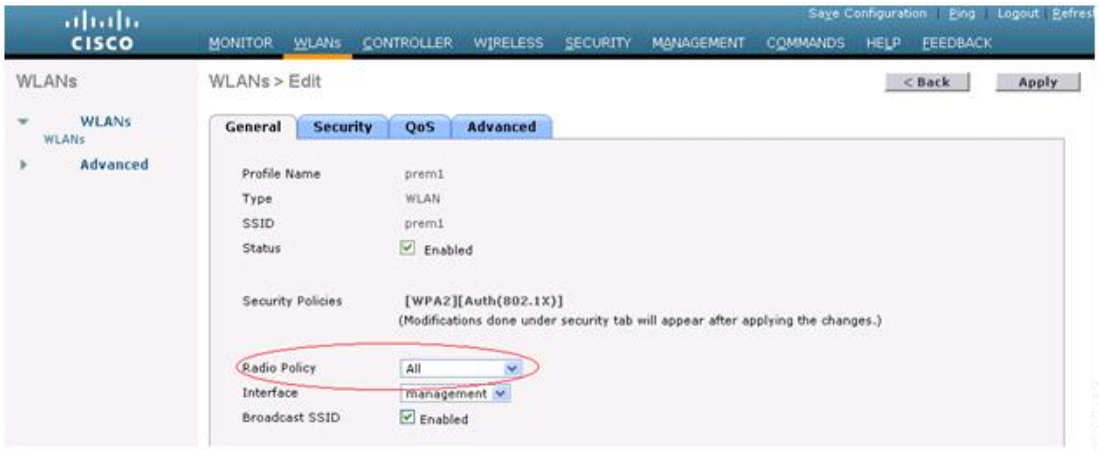


DOWNLINK 方向にバックホールを延長するために使用される RAPSB（シリアル バックホール）の 5 GHz 無線のスロット 2 が DOWNLINK ACCESS として表示されます。この場合、クライアント アクセスに使用される RAPSB の 5 GHz 無線のスロット 1 が ACCESS として表示されます。UPLINK に使用される MAPSB の 5 GHz 無線のスロット 2 が UPLINK ACCESS として表示され、MAPSB のスロット 1 が DOWNLINK ACCESS に使用されます（クライアント アクセスを提供する全方向性アンテナを使用）。

正しいインターフェイス（VLAN）にマッピングされた適切な SSID を使用して WLC 上で WLAN を作成します。 WLAN を作成すると、WLAN はデフォルトですべての無線に適用されます。

802.11a無線でのみクライアントアクセスを有効にする場合は、次の図に表示されているリストから適切な無線ポリシーのみを選択します。

図 *67*：無線ポリシーの選択



Extended Universal Access の設定（CLI）

- コントローラのプロンプトに移動し、**config mesh client-access enable extended** コマンドを入力します。

  次のメッセージが表示されます。

```
Enabling client access on both backhaul slots
Same BSSIDs will be used on both slots
All Mesh Serial Backhaul APs will be rebooted
Are you sure you want to start? (y/N)
```

- **show mesh client-access** コマンドを入力して、クライアント アクセスがあるバックホールと拡張されたクライアント アクセスがあるバックホールのステータスを確認します。

  ステータスは次のとおりです。

```
Backhaul with client access status: enabled
Backhaul with client access extended status(3 radio AP): enabled
```

- スロット 2（EUA）のみでクライアント アクセスを無効にする明示的なコマンドはありません。次のコマンドを入力して、両方のバックホールスロットのクライアントアクセスをディセーブルにする必要があります。

  config mesh client-access disable

  次のメッセージが表示されます。

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

- EUA は、スロット 1 無線のクライアント アクセスに影響を与えずに GUI から無効にできますが、すべての 1524SB アクセス ポイントがリブートされます。

次のコマンドを入力することで、スロット 1 でのみクライアント アクセスをイネーブルにして、スロット 2 ではイネーブルにしないことができます。

config mesh client-access enable

次のメッセージが表示されます。

```
All Mesh APs will be rebooted
Are you sure you want to start? (y/N)
```

拡張ユニバーサル アクセスの設定：Cisco Prime Infrastructure

ステップ 1 [Controllers] > [Controller IP Address] > [Mesh] > [Mesh Settings] の順に選択します。
バックホール クライアント アクセスが無効な場合は、[Mesh] ページが表示されます。

ステップ 2 [Client Access on Backhaul Link] チェックボックスをオンにして、[Extended Backhaul Client Access] チェックボックスを表示します。

ステップ 3 [Extended Backhaul Client Access] チェックボックスをオンにし、[Apply] をクリックします。 Extended Backhaul Client Access の有効化の結果を示すメッセージが表示されます。

ステップ 4 [OK] をクリックして作業を続行します。

イーサネット VLAN タギングの設定

イーサネット VLAN タギングを使用すると、無線メッシュ ネットワーク内で特定のアプリケーション トラフィックをセグメント化して、有線 LAN に転送（ブリッジング）するか（アクセス モード）、別の無線メッシュ ネットワークにブリッジングすることができます（トランク モード）。

イーサネット VLAN タギングを使用した一般的な Public Safety アクセス アプリケーションは、市内のさまざまな屋外の場所へのビデオ監視カメラの設置を前提にしたものです。 これらのビデオ カメラはすべて MAP に有線で接続されています。 また、これらのカメラのビデオはすべてワイ

ヤレス バックホールを介して有線ネットワークにある中央の指令本部にストリーミングされます。

図 *68*：イーサネット *VLAN* タギング

イーサネット ポートに関する注意

イーサネット VLAN タギングを使用すると、屋内と屋外の両方の実装で、イーサネット ポートをノーマル、アクセス、またはトランクとして設定できます。

（注） VLAN 透過が無効な場合、デフォルトのイーサネット ポート モードはノーマルです。 VLAN タギングを使用し、イーサネット ポートの設定を許可するには、VLAN 透過を無効にする必要があります。 グローバル パラメータである VLAN 透過を無効にするには、グローバル メッシュ パラメータの設定を参照してください。

- ノーマル モード：このモードでは、イーサネット ポートが、タグ付きパケットを受信または送信しません。 クライアントからのタグ付きフレームは破棄されます。

  単一 VLAN のみを使用している場合や、複数の VLAN にわたるネットワークでトラフィックをセグメント化する必要がない場合は、アプリケーションでノーマル モードを使用します。

- アクセス モード：このモードでは、タグなしパケットだけを許可します。 すべての着信パケットに、アクセス VLAN と呼ばれるユーザ設定 VLAN のタグが付けられます。

  MAP に接続され、RAP に転送される装置（カメラや PC）から情報を収集するアプリケーションでは、アクセス モードを使用します。 次に、RAP はタグを適用し、トラフィックを有線ネットワーク上のスイッチに転送します。

- トランク モード：このモードでは、ユーザがネイティブ VLAN および許可された VLAN リストを設定する必要があります（デフォルトではありません）。 このモードではタグ付きのパケットとタグなしパケットの両方が許可されます。 タグなしパケットは許可され、ユーザ

指定のネイティブ VLAN のタグが付けられます。 許可された VLAN リスト内の VLAN のタグが付けられたタグ付きパケットは許可されます。

- キャンパス内の別々の建物に存在している 2 つの MAP 間でトラフィックを転送するようなブリッジング アプリケーションでは、トランク モードを使用します。

イーサネット VLAN タギングは、バックホールとして使用されていないイーサネット ポートで動作します。

イーサネット VLAN タギングのガイドライン

イーサネット タギングの以下のガイドラインに従います。

- セキュリティの理由で、メッシュ アクセス ポイント（RAP および MAP）にあるイーサネット ポートはデフォルトでは無効です。 このイーサネット ポートは、メッシュ アクセス ポイント ポートでイーサネット ブリッジングを設定することにより、有効になります。
- イーサネット VLAN タギングが動作するには、メッシュ ネットワーク内の全メッシュ アクセス ポイントでイーサネット ブリッジングが有効である必要があります。
- VLAN モードは、非 VLAN トランスペアレントに設定する必要があります（グローバル メッシュ パラメータ）。 グローバル メッシュ パラメータの設定（CLI），（642 ページ）を参照してください。 VLAN トランスペアレントは、デフォルトで有効になっています。 非 VLAN 透過として設定するには、グローバル メッシュ パラメータのページで VLAN 透過のオプションをオフにする必要があります。

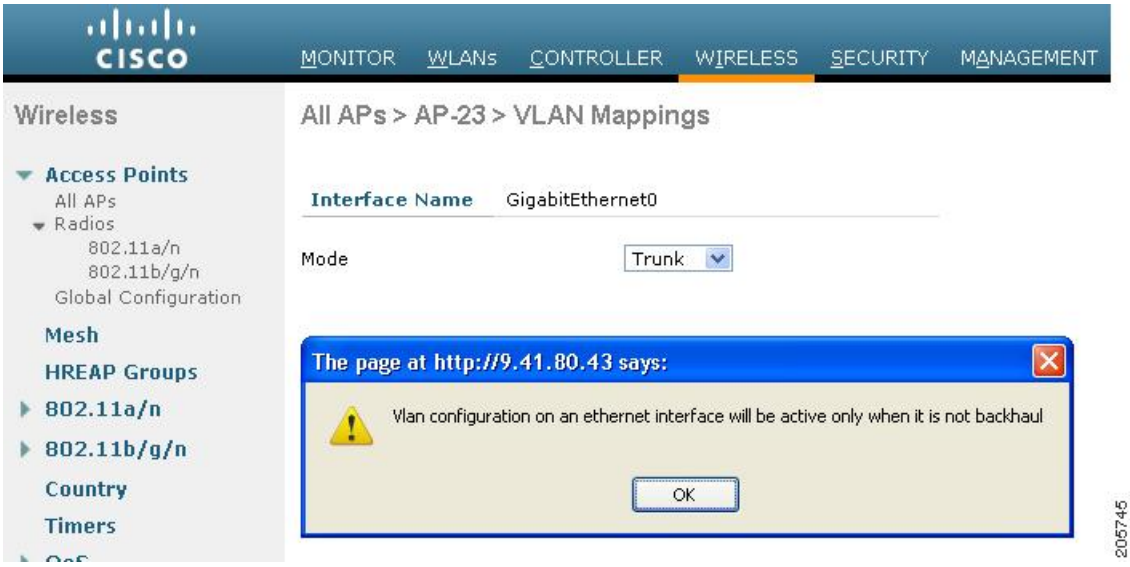
図 *69*：*[Wireless > Mesh]* ページ

- VLAN タギングは、次のようにイーサネット インターフェイスでだけ設定できます。
  - AP1500 では、4 つのポートのうちポート 0（PoE 入力）、ポート 1（PoE 出力）、およびポート 3（光ファイバ）の 3 つをセカンダリ イーサネット インターフェイスとして使用できます。 ポート 2- ケーブルは、セカンダリ イーサネット インターフェイスとして設定できません。

- イーサネット VLAN タギングでは、RAP のポート 0-PoE 入力は、有線ネットワークのスイッチのトランク ポートへの接続に使用します。 MAP のポート 1-PoE 出力は、ビデオ カメラなどの外部デバイスへの接続に使用します。

- バックホール インターフェイス（802.11a 無線）は、プライマリ イーサネット インターフェイスとして機能します。 バックホールはネットワーク内のトランクとして機能し、無線ネットワークと有線ネットワークとの間のすべての VLAN トラフィックを伝送します。 プライマリ イーサネット インターフェイスに必要な設定はありません。
- 屋内メッシュ ネットワークの場合、VLAN タギング機能は、屋外メッシュ ネットワークの場合と同様に機能します。 バックホールとして動作しないアクセス ポートはすべてセカンダリであり、VLAN タギングに使用できます。
- RAP にはセカンダリ イーサネット ポートがないため、VLAN タギングを RAP 上で実装できず、プライマリ ポートがバックホールとして使用されます。 ただし、イーサネット ポートが 1 つの MAP では VLAN タギングを有効にすることができます。これは、MAP のイーサネット ポートがバックホールとして機能せず、結果としてセカンダリ ポートになるためです。
- 設定の変更は、バックホールとして動作するイーサネット インターフェイスに適用されません。 バックホールの設定を変更しようとすると警告が表示されます。 設定は、インターフェイスがバックホールとして動作しなくなった後に適用されます。

図 *70*：バックホールを設定しようとしたときの警告メッセージ表示



- メッシュ ネットワーク内の任意の 802.11a バックホール イーサネット インターフェイスで VLAN タギングをサポートするために設定は必要ありません。
  - これには RAP アップリンク イーサネット ポートが含まれます。 登録メカニズムを使用して、必要な設定が自動的に行われます。

- バックホールとして動作する 802.11a イーサネット リンクへの設定の変更はすべて無視され、警告が表示されます。 イーサネット リンクがバックホールとして動作しなくなると、変更した設定が適用されます。

- AP1500 のポート 02（ケーブル モデム ポート）では、VLAN を設定できません（該当する場合）。 ポート 0（PoE 入力）、1（PoE 出力）、および 3（光ファイバ）では VLAN を設定できます。
- 各セクターでは、最大 16 個の VLAN がサポートされています。 したがって、RAP の子（MAP）によってサポートされている VLAN の累積的な数は最大 16 です。
- RAP に接続されるスイッチ ポートはトランクである必要があります。
  - スイッチのトランク ポートと RAP トランク ポートは一致している必要があります。
  - RAP は常にスイッチのネイティブ VLAN ID 1 に接続する必要があります。 RAP のプライマリ イーサネット インターフェイスは、デフォルトではネイティブ VLAN 1 です。
  - RAP に接続されている有線ネットワークのスイッチ ポート（ポート 0–PoE 入力）は、トランク ポートでタグ付きパケットを許可するように設定する必要があります。 RAP は、メッシュ ネットワークから受信したすべてのタグ付きパケットを有線ネットワークに転送します。
  - メッシュ セクター宛以外の VLAN をスイッチのトランク ポートに設定しないでください。
- MAP イーサネット ポートで設定した VLAN は、管理 VLAN として機能できません。
- メッシュ アクセス ポイントが CAPWAP RUN 状態であり、VLAN 透過モードが無効な場合にのみ、設定は有効です。
- ローミングする場合、または CAPWAP が再び開始される場合は、必ず設定の適用が再び試行されます。

VLAN 登録

メッシュ アクセス ポイントで VLAN をサポートするには、すべてのアップリンク メッシュ アクセス ポイントが、異なる VLAN に属するトラフィックを分離できるよう同じ VLAN をサポートする必要があります。 メッシュ アクセス ポイントが VLAN の要件を通信して親からの応答を得る処理は、VLAN 登録と呼ばれます。

（注） VLAN 登録は自動的に行われます。 ユーザの操作は必要ありません。

VLAN 登録の概要は次のとおりです。

1. メッシュ アクセス ポイントのイーサネット ポートが VLAN で設定されている場合は、ポートから親へその VLAN をサポートすることを要求します。

2 親は、要求をサポートできる場合、その VLAN のブリッジ グループを作成し、要求をさらにその親へ伝搬します。 この伝搬は RAP に達するまで続きます。

3 要求が RAP に達すると、RAP は VLAN 要求をサポートできるかどうかを確認します。 サポートできる場合、RAP は VLAN 要求をサポートするために、ブリッジ グループとサブインターフェイスをアップリンク イーサネット インターフェイスで作成します。

4 メッシュ アクセス ポイントのいずれかの子で VLAN 要求をサポートできない場合、メッシュ アクセス ポイントはネガティブ応答を返します。 この応答は、VLAN を要求したメッシュ アクセス ポイントに達するまでダウンストリーム メッシュ アクセス ポイントに伝搬されます。

5 親からのネガティブ応答を受信した要求元メッシュ アクセス ポイントは、VLAN の設定を延期します。 ただし、将来試みるときのために設定は保存されます。 メッシュの動的な特性を考慮すると、ローミング時やCAPWAP 再接続時に、別の親とそのアップリンク メッシュ アクセス ポイントがその設定をサポートできることがあります。

イーサネット VLAN タギングの有効化（GUI）

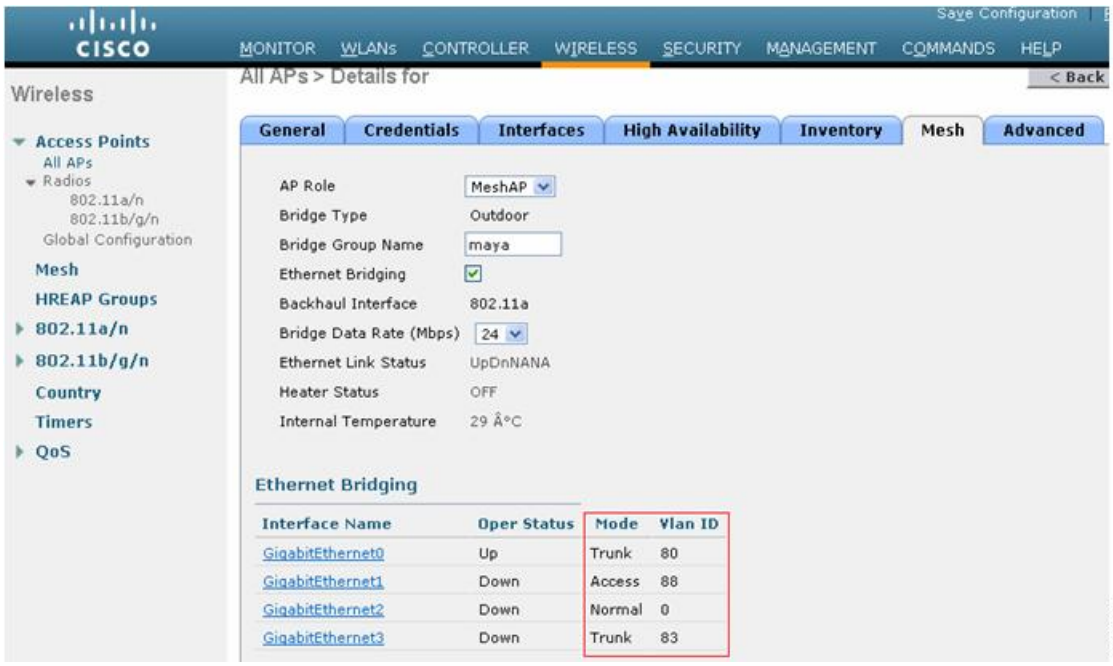
VLAN タギングを設定する前に、イーサネット ブリッジングを有効にする必要があります。イーサネット ブリッジングの設定の項を参照してください。

ステップ 1 イーサネット ブリッジングを有効にしてから、[Wireless] > [All APs] を選択します。

ステップ 2 VLAN タギングを有効にするメッシュ アクセス ポイントの AP 名のリンクをクリックします。

ステップ 3 詳細ページで、[Mesh] タブを選択します。

図 *71*：*[All APs > Details for]*（*[Mesh]*）ページ



ステップ 4 [Ethernet Bridging] チェックボックスをオンにしてこの機能を有効にし、[Apply] をクリックします。ページの最下部の [Ethernet Bridging] セクションに、メッシュ アクセス ポイントの 4 つのイーサネット ポートそれぞれが一覧表示されます。

- MAP のアクセス ポートを設定する場合は、たとえば、[gigabitEthernet1]（ポート 1（PoE 出力））をクリックします。

  1. [Mode] ドロップダウン リストで [Access] を選択します。
  2. VLAN ID を入力します。 VLAN ID には 1 ～ 4095 の任意の値を入力できます。
  3. [Apply] をクリックします。

（注） VLAN ID 1 はデフォルト VLAN として予約されていません。

（注） RAP のすべての従属 MAP 全体で最大 16 の VLAN がサポートされています。

図 *72* : ***VLAN*** アクセス モード

- RAP または MAP のトランク ポートを設定する場合は、[gigabitEthernet0]（ポート 0（PoE 入力））をクリックします。

1. [Mode] ドロップダウン リストで [Trunk] を選択します。
2. 着信トラフィックのネイティブ VLAN ID を指定します。 ネイティブ VLAN ID には 1 ～ 4095 の任意の値を入力できます。 ユーザ VLAN（アクセス）に割り当てた値を割り当てないでください。
3. [Apply] をクリックします。

   トランク VLAN ID フィールドと設定した VLAN のサマリーが、画面下部に表示されます。 トランク VLAN ID フィールドは発信パケット用です。
4. 発信パケットのトランク VLAN ID を指定します。

   タグなしパケットを転送する場合、デフォルトのトランク VLAN ID 値（0）を変更しないでください （MAP-to-MAP ブリッジング、キャンパス環境）。

   タグ付きパケットを転送する場合、未割り当ての VLAN ID（1 ～ 4095）を入力します （RAP から有線ネットワークのスイッチ）。
5. [Add] をクリックして、トランク VLAN ID を許可された VLAN リストに追加します。 新しく追加した VLAN は、ページの [Configured VLANs] セクションの下に表示されます。

（注）　リストから VLAN を削除するには、該当する VLAN の右にある矢印ドロップダウン リストから [Remove] オプションを選択します。

図 *73*：*[All APs > AP > VLAN Mappings]* ページ

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。

イーサネット VLAN タギングの設定（CLI）

- MAP アクセス ポートを設定するには、次のコマンドを入力します。
  config ap ethernet 1 mode access enable *AP1500-MAP 50*

  ここで、*AP1500-MAP* は可変の *AP* 名であり、*50* は可変のアクセス *VLAN ID* です。

- RAP または MAP のトランク ポートを設定するには、次のコマンドを入力します。
  config ap ethernet 0 mode trunk enable *AP1500-MAP 60*

  ここで、*AP1500-MAP* は可変の *AP* 名であり、*60* は可変のネイティブ *VLAN ID* です。

- VLAN をネイティブ VLAN の VLAN 許可リストに追加するには、次のコマンドを入力します。
  config ap ethernet 0 mode trunk add *AP1500-MAP3 65*

  ここで、*AP1500-MAP 3* は可変の *AP* 名であり、*65* は可変の *VLAN ID* です。

イーサネット VLAN タギング設定詳細の表示（CLI）

特定メッシュ アクセス ポイント（*AP Name*）またはすべてのメッシュ アクセス ポイント（*summary*）のイーサネット インターフェイスの VLAN 設定の詳細を表示するには、次のいずれかのコマンドを入力します。

```
(Cisco Controller) >show ap config ethernet

summary         For all APs
<AP Name>       For specific AP
(Cisco Controller) >show ap config ethernet AP-23

Vlan Tagging Information For AP AP-23
  Ethernet 0
    Mode: TRUNK
      Native Vlan 80
      Allowed Vlans: 81 83
  Ethernet 1
    Mode: ACCESS
      Access Vlan 88
  Ethernet 2
    Mode: NORMAL
  Ethernet 3
    Mode: TRUNK
      Native Vlan 83
      Allowed Vlans: 81 87 89
```

205741

VLAN トランスペアレント モードが有効と無効のどちらであるかを確認するには、次のコマンドを入力します。

```
(Cisco Controller) >show mesh config

Mesh Range...................................... 12000
Backhaul with client access status.............. disabled
Background Scanning State....................... enabled

Mesh Security
   Security Mode................................ EAP
   External-Auth................................ disabled
   Use MAC Filter in External AAA server........ disabled
   Force External Authentication................ disabled

Mesh Alarm Criteria
   Max Hop Count................................ 4
   Recommended Max Children for MAP............. 10
   Recommended Max Children for RAP............. 20
   Low Link SNR................................. 12
   High Link SNR................................ 60
   Max Association Number....................... 10
   Association Interval......................... 60 minutes
   Parent Change Numbers........................ 3
   Parent Change Interval....................... 60 minutes

--More-- or (q)uit

Mesh Multicast Mode............................. In-Out
Mesh Full Sector DFS............................ enabled

Mesh Ethernet Bridging VLAN Transparent Mode..... disabled
```

205742

ワークグループ ブリッジとメッシュ インフラストラクチャとの相互運用性

ワークグループ ブリッジ（WGB）は、イーサネット対応デバイスにワイヤレス インフラストラクチャ接続を提供できる小さいスタンドアロンユニットです。無線ネットワークに接続するためにワイヤレスクライアントアダプタを備えていないデバイスは、イーサネットポート経由でWGBに接続できます。 WGB は、ワイヤレス インターフェイスを介してルート AP にアソシエートされます。つまり、有線クライアントはワイヤレス ネットワークにアクセスできます。

WGB は、メッシュ アクセス ポイントに、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレスセグメントを介して有線ネットワークに接続するために使用されます。 WGB クライアントのデータ パケットでは、802.11 ヘッダー（4 つの MAC ヘッダー（通常は 3 つの MAC データ ヘッダー））内に追加 MAC アドレスが含まれます。 ヘッダー内の追加 MAC は、WGB 自体のアドレスです。 この追加 MAC アドレスは、クライアントと送受信するパケットをルーティングするために使用されます。

WGB アソシエーションは、各メッシュ アクセス ポイントのすべての無線でサポートされます。

現在のアーキテクチャでは、自律 AP はワークグループ ブリッジとして機能し、コントローラ接続に唯一の無線インターフェイスが使用され、有線クライアント接続にイーサネット インターフェイスが使用され、ワイヤレス クライアント接続に他の無線インターフェイスが使用されます。（メッシュ インフラストラクチャを使用して）コントローラに接続するには dot11radio 1（5 GHz）を使用でき、有線クライアントにはイーサネット インターフェイスを使用できます。 ワイ

ヤレス クライアント接続には dot11radio 0（2.4 GHz）を使用できます。 要件に応じて、クライアント アソシエーションまたはコントローラ接続に dot11radio 1 または dot11radio 0 を使用できます。

7.0 リリースでは、ワイヤレス インフラストラクチャへのアップリンクを失ったとき、またはローミング シナリオの場合、WGB の 2 番目の無線のワイヤレス クライアントが、WGB によってアソシエート解除されません。

2 つの無線を使用する場合、1 つの無線をクライアント アクセスに使用し、もう 1 つの無線をアクセス ポイントにアクセスするために使用できます。 2 つの独立した無線が 2 つの独立した機能を実行するため、遅延の制御が向上し、遅延が低下します。 また、アップリンクが失われたとき、またはローミング シナリオの場合、WGB の 2 番目の無線のワイヤレス クライアントはアソシエーション解除されません。 一方の無線はルート AP（無線の役割）として設定し、もう一方の無線は WGB（無線の役割）として設定する必要があります。

（注） 一方の無線が WGB として設定された場合、もう一方の無線は WGB またはリピータとして設定できません。

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。

- FlexConnect
- アイドル タイムアウト
- Web 認証：WGB が Web 認証 WLAN にアソシエートする場合、WGB は除外リストに追加され、すべての WGB 有線クライアントが削除されます（Web 認証 WLAN はゲスト WLAN の別名です）。
- WGB 背後の有線クライアントでの MAC フィルタリング、リンク テスト、およびアイドル タイムアウト

ワークグループ ブリッジの設定

ワークグループブリッジ（WGB）は、メッシュ アクセス ポイントに、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレス セグメントを介して有線ネットワークに接続するために使用されます。 IAPP 制御メッセージの他にも、WGB クライアントのデータ パケットでは 802.11 ヘッダー（4 つの MAC ヘッダー（通常は 3 つの MAC データ ヘッダー））内に追加 MAC アドレスが含まれます。 ヘッダー内の追加 MAC は、ワークグループ ブリッジ自体のアドレスです。 この追加 MAC アドレスは、クライアントと送受信するパケットをルーティングするときに使用されます。

WGB アソシエーションは、AP1522 では 2.4 GHz（802.11b/g）および 5 GHz（802.11a）無線、AP1524PS では 2.4 GHz（802.11b）および 4.9 GHz（Public Safety）無線の両方でサポートされています。

サポートされるプラットフォームは、自律 WGB である AP1130、AP1140、AP1240、AP1310、および Cisco 3200 Mobile Router（以降、Cisco 3200 と呼ばれます）です。Cisco 3200 は WGB として設定することにより、メッシュ アクセス ポイントとアソシエートできます。 設定手順について

は、『*Cisco Wireless LAN Controller Configuration Guide, Release 7.0.116.0*』（http://www.cisco.com/en/US/products/ps6366/products_installation_and_configuration_guides_list.html）の第 7 章の項「Cisco Workgroup Bridges」を参照してください。

サポートされるワークグループ ブリッジ モードと容量

サポートされる WGB モードおよび機能は次のとおりです。

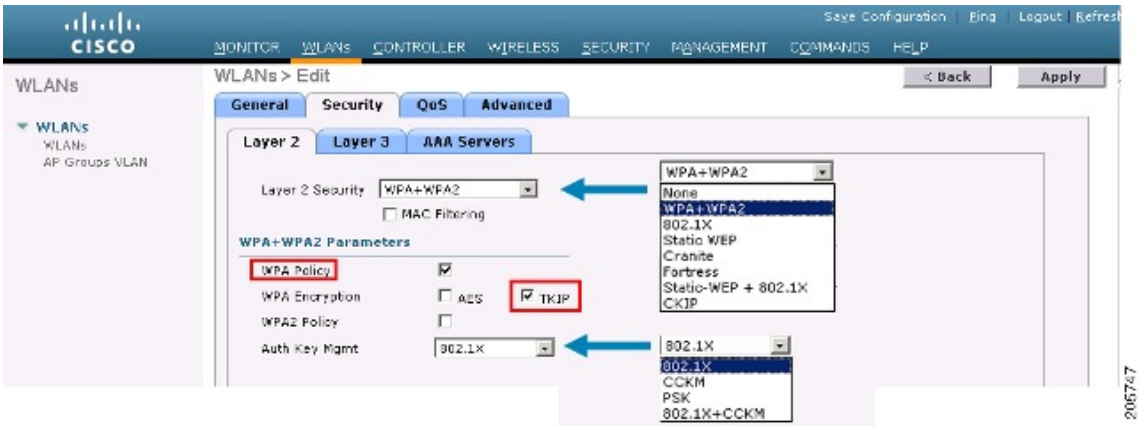
- WGB として設定された自律アクセス ポイントでは Cisco IOS リリース 12.4.25d-JA 以降が実行されている必要があります。

（注） メッシュ アクセス ポイントに 2 つの無線がある場合、いずれかの無線でだけワークグループ ブリッジ モードを設定できます。 2 番目の無線を無効にすることをお勧めします。 AP1524SB などの 3 つの無線を備えたアクセス ポイントでは、ワークグループ ブリッジ モードはサポートされていません。

- クライアント モード WGB（BSS）はサポートされていますが、インフラストラクチャ WGB はサポートされていません。 クライアント モード WGB では VLAN をトランクできませんが、インフラストラクチャ WGB ではトランクできます。
- ACK がクライアントから返されないため、マルチキャスト トラフィックは WGB に確実に転送されるわけではありません。 マルチキャスト トラフィックがインフラストラクチャ WGB にユニキャストされると、ACK が返されます。
- Cisco IOS アクセス ポイントで一方の無線が WGB として設定された場合、もう一方の無線を WGB やリピータにすることができません。
- メッシュ アクセス ポイントでは、アソシエートされた WGB の背後で、ワイヤレス クライアント、WGB、および有線クライアントを含む、最大 200 のクライアントをサポートできます。
- WLAN が WPA1（TKIP）+WPA2（AES）で設定され、対応する WGB インターフェイスがこれらの暗号化の 1 つ（WPA1 または WPA2）で設定された場合、WGB はメッシュ アクセス ポイントとアソシエートできません。

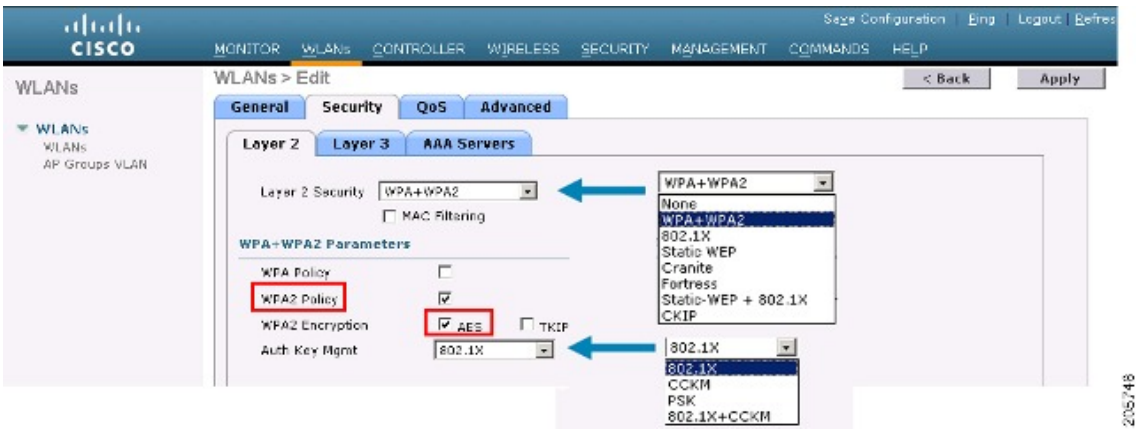
次の図に、WGB（コントローラ GUI）の WPA セキュリティ設定を示します。

図 *74*：*WGB* の *WPA* セキュリティ設定



次の図に、WGB（コントローラ GUI）の WPA-2 セキュリティ設定を示します。

図 *75*：*WGB* の *WPA-2* セキュリティ設定



WGB クライアントのステータスの表示

ステップ 1 [Monitor] > [Clients] の順に選択します。

ステップ 2 クライアント サマリー ページで、クライアントの MAC アドレスをクリックするか、その MAC アドレスを使用してクライアントを検索します。

ステップ 3 表示されるページで、クライアントの種類が WGB と認識されていることを確認します（右端）。

図 *76* : クライアントが *WGB* であると認識されている

ステップ 4 クライアントの MAC アドレスをクリックして、設定の詳細を表示します。

注意事項および制約事項

- メッシュ アクセス ポイントで利用可能な 2 つの 5 GHz 無線で強力なクライアント アクセスを利用できるよう、メッシュ AP インフラストラクチャへのアップリンクには 5 GHz 無線を使用することをお勧めします。 5 GHz 帯域を使用すると、より大きい Effective Isotropic Radiated Power（EIRP）が許可され、品質が劣化しにくくなります。 2 つの無線がある WGB では、5 GHz 無線（無線 1）モードを WGB として設定します。 この無線は、メッシュ インフラストラクチャにアクセスするために使用されます。 2 番目の無線 2.4 GHz（無線 0）モードをクライアント アクセスのルートとして設定します。
- 自律アクセス ポイントでは、SSID を 1 つだけネイティブ VLAN に割り当てることができます。 自律側では、1 つの SSID で複数の VLAN を使用できません。 SSID と VLAN のマッピングは、異なる VLAN でトラフィックを分離するために一意である必要があります。 Unified アーキテクチャでは、複数の VLAN を 1 つの WLAN（SSID）に割り当てることができます。
- アクセス ポイント インフラストラクチャへの WGB のワイヤレス アソシエーションには 1 つの WLAN（SSID）だけがサポートされます。 この SSID はインフラストラクチャ SSID として設定し、ネイティブ VLAN にマッピングする必要があります。
- 動的インターフェイスは、WGB で設定された各 VLAN のコントローラで作成する必要があります。

- アクセス ポイントの 2 番目の無線（2.4 GHz）でクライアント アクセスを設定する必要があります。 両方の無線で同じ SSID を使用し、ネイティブ VLAN にマッピングする必要があります。 異なる SSID を作成した場合は、一意な VLAN と SSID のマッピングの要件のため、その SSID をネイティブ VLAN にマッピングすることはできません。 SSID を別の VLAN にマッピングしようとしても、ワイヤレス クライアントの複数 VLAN サポートはありません。
- WGB でのワイヤレス クライアント アソシエーションでは、WLAN（SSID）に対してすべてのレイヤ 2 セキュリティ タイプがサポートされます。
- この機能は AP プラットフォームに依存しません。 コントローラ側では、メッシュ AP および非メッシュ AP の両方がサポートされます。
- WGB では、20 クライアントの制限があります。 20 クライアントの制限には、有線クライアントとワイヤレス クライアントの両方が含まれます。 WGB が自律アクセス ポイントと対話する場合、クライアントの制限は非常に高くなります。
- コントローラは、WGB の背後にあるワイヤレス クライアントと有線クライアントを同様に扱います。 コントローラからワイヤレス WGB クライアントに対する MAC フィルタリングやリンク テストなどの機能は、サポートされません。
- 必要な場合、WGB ワイヤレス クライアントに対するリンク テストは自律 AP から実行できます。
- WGB にアソシエートされたワイヤレス クライアントに対する複数の VLAN はサポートされません。
- 7.0 リリース以降、WGB の背後にある有線クライアントに対して最大 16 の複数 VLAN がサポートされます。
- WGB の背後にあるワイヤレス クライアントおよび有線クライアントに対してローミングがサポートされます。 アップリンクが失われたとき、またはローミング シナリオの場合、他の無線のワイヤレス クライアントは WGB によってアソシエート解除されません。

無線 0（2.4 GHz）をルート（自律 AP の 1 つの動作モード）として設定し、無線 1（5 GHz）を WGB として設定することをお勧めします。

例：ワークグループ ブリッジの設定

CLI で設定する場合に必須な項目は次のとおりです。

- dot11 SSID（WLAN のセキュリティは要件に基づいて決定できます）。
- 単一ブリッジ グループに両方の無線のサブインターフェイスをマッピングすること。

（注） ネイティブ VLAN は、デフォルトで常にブリッジ グループ 1 にマッピングされます。 他の VLAN の場合、ブリッジ グループ番号は VLAN 番号に一致します。たとえば、VLAN 46 の場合、ブリッジ グループは 46 です。

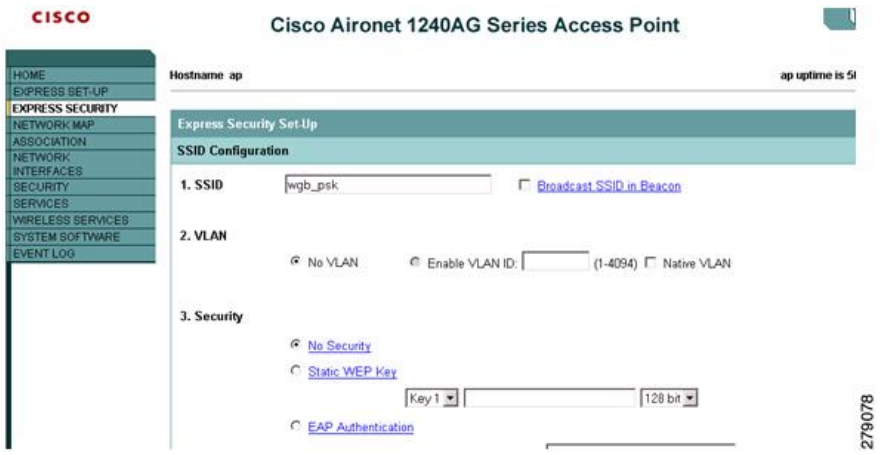
- SSID を無線インターフェイスにマッピングし、無線インターフェイスの役割を定義します。

次の例では、両方の無線で 1 つの SSID（WGBTEST）が使用され、SSID は NATIVE VLAN 51 にマッピングされたインフラストラクチャ SSID です。 すべての無線インターフェイスは、ブリッジ グループ -1 にマッピングされます。

```
WGB1#config t
WGB1(config)#interface Dot11Radio1.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#interface Dot11Radio0.51
WGB1(config-subif)#encapsulation dot1q 51 native
WGB1(config-subif)#bridge-group 1
WGB1(config-subif)#exit
WGB1(config)#dot11 ssid WGBTEST
WGB1(config-ssid)#VLAN 51
WGB1(config-ssid)#authentication open
WGB1(config-ssid)#infrastructiure-ssid
WGB1(config-ssid)#exit
WGB1(config)#interface Dot11Radio1
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role workgroup-bridge
WGB1(config-if)#exit
WGB1(config)#interface Dot11Radio0
WGB1(config-if)#ssid WGBTEST
WGB1(config-if)#station-role root
WGB1(config-if)#exit
```

また、自律 AP の GUI を使用して設定を行うこともできます。 この GUI から VLAN が定義された後に、サブインターフェイスは自動的に作成されます。

図 *77* : *[SSID Configuration]* ページ



WGB アソシエーションの確認

コントローラと WGB のアソシエーションおよび WGB とワイヤレス クライアントのアソシエーションの両方は、自律 AP で **show dot11 associations client** コマンドを入力して確認できます。

```
WGB#show dot11 associations client

802.11 Client Stations on Dot11Radio1:

SSID [WGBTEST] :
```

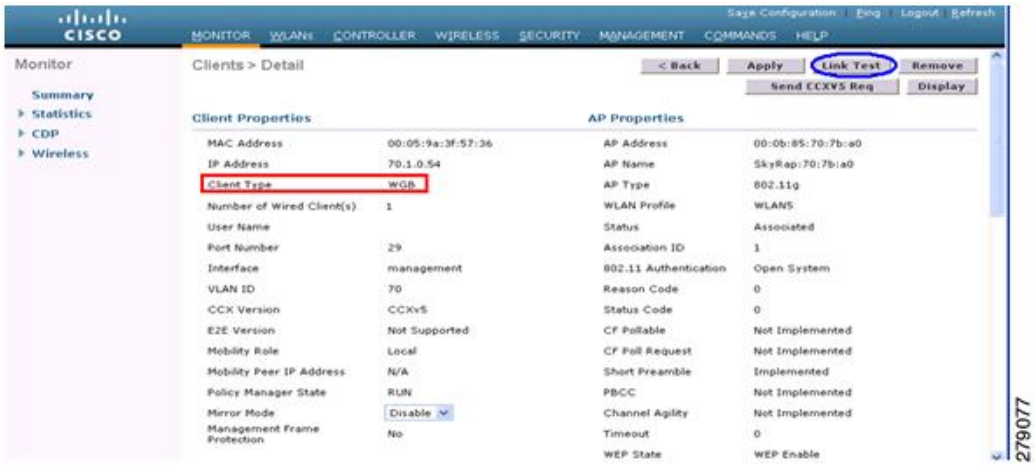
MAC Address	IP Address	Device	Name	Parent	State
0024.130f.920e	209.165.200.225	LWAPP-Parent	RAPSB	-	Assoc

コントローラで、[Monitor] > [Clients] を選択します。 WGB の背後の WGB およびワイヤレス/有線クライアントが更新され、ワイヤレス/有線クライアントは、次の図に示すように、WGB クライアントとして表示されます。

図 *78* : 更新された ***WGB*** クライアント

図 *79* : 更新された ***WGB*** クライアント

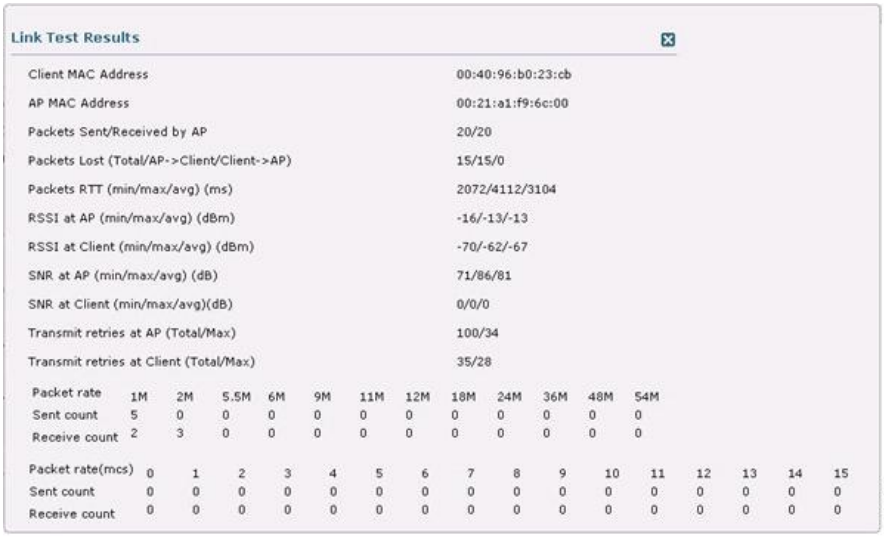
図 *80* : 更新された ***WGB*** クライアント



リンク テストの結果

次の図に、リンク テストの結果を示します。

図 *81*：リンク テストの結果



リンク テストは、コントローラの CLI から次のコマンドを使用して実行することもできます。

```
(Cisco Controller) > linktest client mac address
```

コントローラからのリンク テストは WGB にのみ制限され、コントローラから、WGB に接続された有線またはワイヤレス クライアントに対して WGB 外部で実行することはできません。 WGB 自体から WGB に接続されたワイヤレス クライアントのリンク テストを実行するには、次のコマンドを使用します。

```
ap#dot11 dot11Radio 0 linktest target client mac
Start linktest to 0040.96b8.d462, 100 512 byte packets
ap#
```

POOR (4% lost)	Time (msec)	Strength (dBm)		SNR Quality		Retries	
		In	Out	In	Out	In	Out
Sent: 100	Avg. 22	-37	-83	48	3	Tot. 34	35
Lost to Tgt: 4	Max. 112	-34	-78	61	10	Max. 10	5
Lost to Src: 4	Min. 0	-40	-87	15	3		

```
Rates (Src/Tgt)     24Mb 0/5  36Mb 25/0  48Mb 73/0  54Mb 2/91
Linktest Done in 24.464 msec
```

WGB 有線/ワイヤレス クライアント

また、次のコマンドを使用して、WGB と、Cisco Lightweight 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確認することもできます。

(Cisco Controller) > **show wgb summary**

Number of WGBs..... 2

MAC Address	IP Address	AP Name	Status	WLAN	Auth	Protocol	Clients
00:1d:70:97:bd:e8	209.165.200.225	c1240	Assoc	2	Yes	802.11a	2
00:1e:be:27:5f:e2	209.165.200.226	c1240	Assoc	2	Yes	802.11a	5

(Cisco Controller) > **show client summary**

Number of Clients..... 7

MAC Address	AP Name	Status	WLAN/Guest-Lan	Auth	Protocol	Port	Wired
00:00:24:ca:a9:b4	R14	Associated	1	Yes	N/A	29	No
00:24:c4:a0:61:3a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f4	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:61:f8	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:0a	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:62:42	R14	Associated	1	Yes	802.11a	29	No
00:24:c4:a0:71:d2	R14	Associated	1	Yes	802.11a	29	No

(Cisco Controller) > **show wgb detail** *00:1e:be:27:5f:e2*

Number of wired client(s): 5

MAC Address	IP Address	AP Name	Mobility	WLAN	Auth
00:16:c7:5d:b4:8f	Unknown	c1240	Local	2	No
00:21:91:f8:e9:ae	209.165.200.232	c1240	Local	2	Yes
00:21:55:04:07:b5	209.165.200.234	c1240	Local	2	Yes
00:1e:58:31:c7:4a	209.165.200.236	c1240	Local	2	Yes
00:23:04:9a:0b:12	Unknown	c1240	Local	2	No

クライアント ローミング

Cisco Compatible Extension（CX）バージョン 4（v4）クライアントによる高速ローミングでは、AP1522 および AP1524 の屋外メッシュ展開において最大 70 mph の速度がサポートされています。適用例としては、メッシュ パブリック ネットワーク内を移動する緊急車両の端末との通信を維持する場合があります。

3 つの Cisco CX v4 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：クライアントによるスキャン時間が短縮されます。Cisco CX v4 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 ポイントの特徴を含む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、Cisco CX v4 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ます。 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。
- ローミング理由レポート：Cisco CX v4 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できます。 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。

（注） クライアント ローミングはデフォルトでは有効です。 詳細については、『Enterprise Mobility Design Guide』（http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/eMob4.1.pdf）を参照してください。

WGB ローミングのガイドライン

WGB ローミングのガイドラインは次のとおりです。

- WGBでのローミングの設定：WGBがモバイルである場合は、親アクセスポイントまたはブリッジへのより良好な無線接続をスキャンするよう設定できます。**ap(config-if)#mobile station period 3 threshold 50** コマンドを使用して、ワークグループ ブリッジをモバイル ステーションとして設定します。

  この設定を有効にすると、受信信号強度表示（RSSI）の数値が低いこと、電波干渉が多いこと、またはフレーム損失率が高いことが検出された場合に、WGBは新しい親アソシエーションをスキャンします。 これらの基準を使用して、モバイル ステーションとして設定された WGB は新しい親アソシエーションを検索し、現在のアソシエーションが失われる前に新しい親にローミングします。 モバイル ステーションの設定が無効な場合（デフォルト設定）、WGB は現在のアソシエーションが失われるまで新しいアソシエーションを検索しません。

- WGB での限定チャネル スキャンの設定：鉄道などのモバイル環境では、WGB はすべてのチャネルをスキャンする代わりに、限定チャネルのセットのみをスキャンするよう制限され、WGB のローミングが 1 つのアクセス ポイントから別のアクセス ポイントに切り替わるときにハンドオフによる遅延が減少します。 チャネル数を制限することにより、WGB は必要なチャネルのみをスキャンします。モバイル WGB では、高速かつスムーズなローミングとともに継続的なワイヤレス LAN 接続が実現され、維持されます。 この限定チャネル セットは、ap(config-if)#**mobile station scan** *set of channels* を使用して設定されます。

  このコマンドにより、すべてのチャネルまたは指定されたチャネルに対するスキャンが実行されます。 設定できるチャネルの最大数に制限はありません。 設定できるチャネルの最大数は、無線がサポートできるチャネル数に制限されます。 実行時に、WGB はこの限定チャネル セットのみをスキャンします。 この限定チャネルの機能は、WGB が現在アソシエートされているアクセス ポイントから受け取る既知のチャネル リストにも影響します。 チャネルは、チャネルが限定チャネル セットに含まれる場合にのみ、既知のチャネル リストに追加されます。

設定例

次に、ローミング設定を設定する例を示します。

```
ap(config)#interface dot11radio 1
ap(config-if)#ssid outside
ap(config-if)#packet retries 16
ap(config-if)#station role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station period 3 threshold 50
ap(config-if)#mobile station scan 5745 5765
```

no mobile station scan コマンドを使用すると、すべてのチャネルのスキャンが復元されます。

次の表に、メッシュ アクセス ポイントおよび WGB をサポートする周波数帯域を識別します。

表 *32* : *WGB* 相互運用性チャート

RAP/MAP	WGB								
バックホール	MAR3200			802.11n 屋内 AP		1130/1240		1310	
	4.9 GHz（5、10、20 MHz）	5 GHz	2.4 GHz	5 GHz	2.4 GHz	5 GHz	2.4 GHz	5 GHz	2.4 GHz
1552/1552	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524SB/1524SB	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524PS/1524PS	Yes	No	Yes	No	Yes	No	Yes	No	Yes
1522/1522	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524SB/1522	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1524PS/1522	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1522/1524SB	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
1522/1524PS	Yes	No	Yes	No	Yes	No	Yes	No	Yes
1240/1130	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

トラブルシューティングのヒント

ワイヤレス クライアントが WGB にアソシエートされていない場合は、次の手順を実行して問題をトラブルシューティングします。

1. クライアントの設定を確認し、クライアントの設定が正しいことを確認します。
2. 自律 AP で **show bridge** コマンドの出力を確認し、AP が適切なインターフェイスからクライアント MAC アドレスを参照していることを確認します。
3. 異なるインターフェイスの特定の VLAN に対応するサブインターフェイスが同じブリッジ グループにマッピングされていることを確認します。
4. 必要に応じて、**clear bridge** コマンドを使用してブリッジ エントリをクリアします（このコマンドは、WGB 内のアソシエートされているすべての有線および無線クライアントを削除し、それらのクライアントを再度アソシエートすることを忘れないでください）。
5. **show dot11 association** コマンドの出力を確認し、WGB がコントローラにアソシエートされていることを確認します。

6 WGB で 20 クライアントの制限が超えていないことを確認します。

通常のシナリオでは、**show bridge** コマンドの出力と **show dot11 association** コマンドの出力が期待されたものである場合、ワイヤレス クライアントのアソシエーションは成功です。

屋内メッシュ ネットワークの音声パラメータの設定

メッシュ ネットワークにおける音声およびビデオの品質を管理するために、コントローラで Call Admission Control（CAC; コール アドミッション制御）および QoS を設定できます。

屋内メッシュ アクセス ポイントは 802.11e に対応しており、ローカル 2.4 GHz アクセス無線および 5 GHz バックホール無線で QoS がサポートされます。 CAC は、バックホールおよび CCXv4 クライアントでサポートされています（メッシュ アクセス ポイントとクライアント間の CAC を提供）。

（注） 音声は、屋内メッシュ ネットワークだけでサポートされます。 音声は、メッシュ ネットワークの屋外においてベストエフォート方式でサポートされます。

CAC

CAC を使用すると、無線 LAN で輻輳が発生しているときに、制御された Quality Of Service（QoS）をメッシュ アクセス ポイントで維持することができます。 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、さまざまなネットワーク負荷で QoS を維持するには、CCXv4 以降の CAC が必要です。

（注） CAC は Cisco Compatible Extensions（CCX）v4 以降でサポートされています。『*Cisco Wireless LAN Controller Configuration Guide, Release 7.0*』（http://www.cisco.com/en/US/docs/wireless/controller/7.0/configuration/guide/c70sol.html）の第 6 章を参照してください。

アクセスポイントには、帯域幅ベースの CAC と load-based の CAC という 2 種類の CAC が利用できます。 メッシュ ネットワーク上のコールはすべて帯域幅ベースであるため、メッシュ アクセス ポイントは帯域幅ベースの CAC だけを使用します。

帯域幅に基づく、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信するために必要な帯域幅または共有メディア時間を指定することができます。各アクセスポイントは、使用可能な帯域幅を確認して特定のコールに対応できるかどうかを判断し、そのコールに必要な帯域幅と比較します。 品質を許容できる最大可能コール数を維持するために十分な帯域幅が使用できない場合、メッシュ アクセス ポイントはコールを拒否します。

QoS および DSCP マーキング

ローカル アクセスとバックホールでは、802.11e がサポートされています。 メッシュ アクセス ポイントでは、分類に基づいて、ユーザ トラフィックの優先順位が付けられるため、すべてのユーザ トラフィックがベストエフォートの原則で処理されます。

メッシュのユーザが使用可能なリソースは、メッシュ内の位置によって異なり、ネットワークの 1 箇所に帯域幅制限を適用する設定では、ネットワークの他の部分でオーバーサブスクリプションが発生することがあります。

同様に、クライアントの RF の割合を制限することは、メッシュ クライアントに適していません。制限するリソースはクライアント WLAN ではなく、メッシュ バックホールで使用可能なリソースです。

有線イーサネットネットワークと同様に、802.11 WLAN では、キャリア検知多重アクセス（CSMA）が導入されます。ただし、WLAN は、衝突検出（CD）を使用する代わりに衝突回避（CA）を使用します。つまり、メディアが空いたらすぐに各ステーションが伝送を行う代わりに、WLAN デバイスは衝突回避メカニズムを使用して複数のステーションが同時に伝送を行うのを防ぎます。

衝突回避メカニズムでは、CWmin と CWmax という 2 つの値が使用されます。 CW はコンテンション ウィンドウ（*Contention Window*）を表します。 CW は、インターフレーム スペース（IFS）の後、パケットの転送に参加するまで、エンドポイントが待機する必要がある追加の時間を指定します。 Enhanced Distributed Coordination Function（EDCF）は、遅延に影響を受けるマルチメディア トラフィックのあるエンド デバイスが、CWmin 値と CWmax 値を変更して、メディアに統計的に大きい（および頻繁な）アクセスを行えるようにするモデルです。

シスコのアクセス ポイントは EDCF に似た QoS をサポートします。 これは最大 8 つの QoS のキューを提供します。

これらのキューは、次のようにいくつかの方法で割り当てることができます。

- パケットの TOS / DiffServ 設定に基づく
- レイヤ 2 またはレイヤ 3 アクセス リストに基づく
- VLAN に基づく
- デバイス（IP 電話）の動的登録に基づく

AP1500 は Cisco コントローラとともに、コントローラで最小の統合サービス機能（クライアント ストリームに最大帯域幅の制限がある）と、IP DSCP 値と QoS WLAN 上書きに基づいたより堅牢なディファレンシエーテッド サービス（diffServ）機能を提供します。

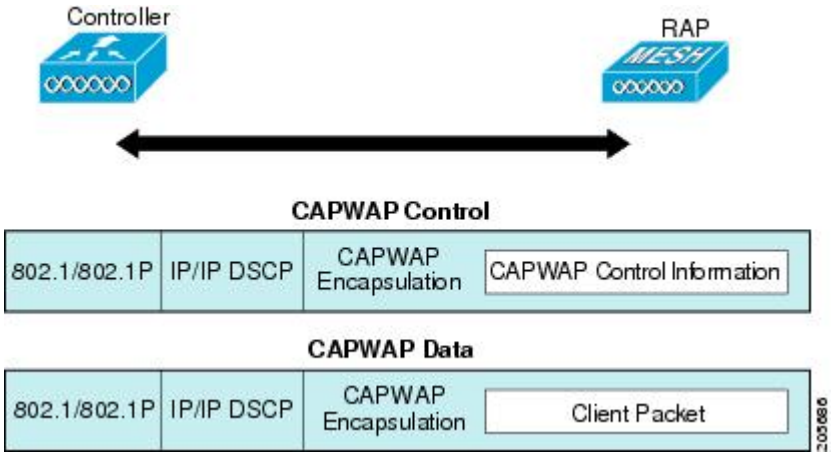
キュー容量に達すると、追加のフレームがドロップされます（テール ドロップ）。

カプセル化

メッシュ システムでは複数のカプセル化が使用されます。これらのカプセル化には、コントローラと RAP 間、メッシュ バックホール経由、メッシュ アクセス ポイントとそのクライアント間の CAPWAP 制御とデータが含まれます。 バックホール経由のブリッジ トラフィック（LAN からの非コントローラ トラフィック）のカプセル化は CAPWAP データのカプセル化と同じです。

コントローラと RAP 間には 2 つのカプセル化があります。 1 つは CAPWAP 制御のカプセル化であり、もう 1 つは CAPWAP データのカプセル化です。 制御インスタンスでは、CAPWAP は制御情報とディレクティブのコンテナとして使用されます。 CAPWAP データのインスタンスでは、イーサネットと IP ヘッダーを含むパケット全体が CAPWAP コンテナ内で送信されます

図 *82*：カプセル化

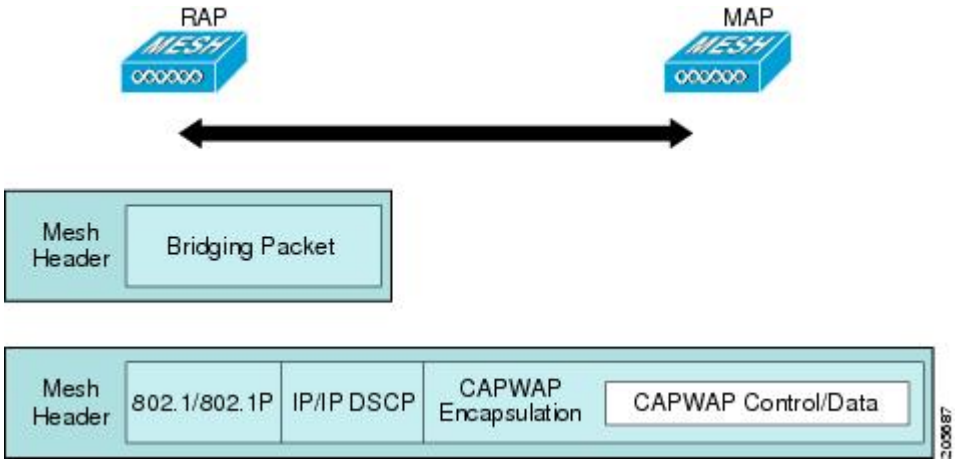


バックホールの場合、MESH トラフィックのカプセル化の 1 つのカプセル化のタイプしかありません。 ただし、2つのタイプのトラフィック（ブリッジ トラフィックと CAPWAP 制御およびデータ トラフィック）がカプセル化されます。 どちらのタイプのトラフィックもプロプライエタリ メッシュ ヘッダーにカプセル化されます。

ブリッジ トラフィックの場合、パケットのイーサネット フレーム全体がメッシュ ヘッダーにカプセル化されます。

すべてのバックホール フレームが MAP から MAP、RAP から MAP、または MAP から RAP でも関係なく適切に処理されます。

図 *83*：メッシュ トラフィックのカプセル化



メッシュ アクセス ポイントでのキューイング

メッシュ アクセス ポイントは高速の CPU を使用して、入力フレーム、イーサネット、およびワイヤレスを先着順に処理します。 これらのフレームは、適切な出力デバイス（イーサネットまたはワイヤレスのいずれか）への伝送のためにキューに格納されます。 出力フレームは、802.11 クライアント ネットワーク、802.11 バックホール ネットワーク、イーサネットのいずれかを宛先にすることができます。

AP1500 は、ワイヤレス クライアント伝送用に 4 つの FIFO をサポートします。 これらの FIFO は 802.11e Platinum、Gold、Sliver、Bronze キューに対応し、これらのキューの 802.11e 伝送ルールに従います。 FIFO では、キューの深さをユーザが設定できます。

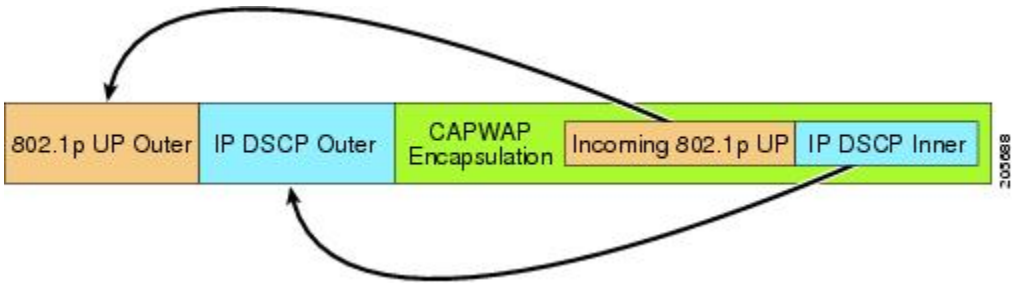
バックホール（別の屋外メッシュ アクセス ポイント宛のフレーム）では、4 つの FIFO を使用しますが、ユーザ トラフィックは、Gold、Siliver、および Bronze に制限されます。 Platinum キューは、CAPWAP 制御トラフィックと音声だけに使用され、CWmin や CWmax などの標準 802.11e パラメータから変更され、より堅牢な伝送を提供しますが、遅延が大きくなります。

Gold キューの CWmin や CWmax などの 802.11e パラメータは、遅延が少なくなるように変更されています。ただし、エラー レートとアグレッシブが若干増加します。 これらの変更の目的は、ビデオ アプリケーションから使いやすいチャネルを提供することです。

イーサネット宛のフレームはFIFOとして、使用可能な最大伝送バッファ プール（256フレーム）までキューに格納されます。 レイヤ 3 IP Differentiated Services Code Point（DSCP）がサポートされ、パケットのマーキングもサポートされます。

データ トラフィックのコントローラから RAP へのパスでは、外部 DSCP 値が着信 IP フレームの DSCP 値に設定されます。 インターフェイスがタグ付きモードである場合、コントローラは、802.1Q VLAN ID を設定し、802.1p UP 着信と WLAN のデフォルトの優先度上限から 802.1p UP（外部）を派生させます。 VLAN ID 0 のフレームはタグ付けされません。

図 *84*：コントローラから *RAP* へのパス



CAPWAP 制御トラフィックの場合、IP DSCP 値は 46 に設定され、802.1p ユーザ優先度（UP）は 7 に設定されます。 バックホール経由のワイヤレス フレームの伝送の前に、ノードのペア化（RAP/MAP）や方向に関係なく、外部ヘッダーの DSCP 値を使用して、バックホール優先度が判断されます。 次の項で、メッシュ アクセス ポイントで使用される 4 つのバックホール キューとバックホール パス QoS に示される DSCP 値のマッピングについて説明します。

表 *33* : バックホール パス *QoS*

DSCP 値	バックホール キュー
2、4、6、8 ～ 23	Bronze
26、32 ～ 63	Gold
46 ～ 56	Platinum
その他すべての値（0 を含む）	Silver

（注） Platinum バックホール キューは CAPWAP 制御トラフィック、IP 制御トラフィック、音声パケット用に予約されています。 DHCP、DNS、および ARP 要求も Platinum QoS レベルで伝送されます。 メッシュ ソフトウェアは、各フレームを調査し、それが CAPWAP 制御フレームであるか、IP 制御フレームであるかを判断して、Platinum キューが CAPWAP 以外のアプリケーションに使用されないようにします。

MAP からクライアントへのパスの場合、クライアントが WMM クライアントか通常のクライアントかに応じて、2 つの異なる手順が実行されます。 クライアントが WMM クライアントの場合、外部フレームの DSCP 値が調査され、802.11e プライオリティ キューが使用されます。

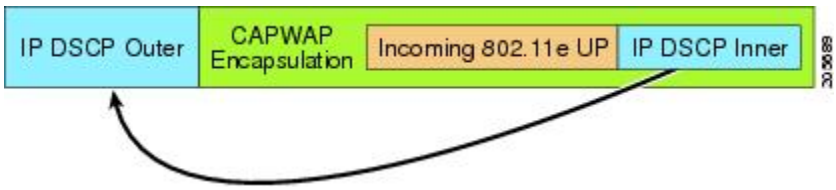
表 *34* : *MAP* からクライアントへのパスの *QoS*

DSCP 値	バックホール キュー
2、4、6、8 ～ 23	Bronze
26、32 ～ 45、47	Gold
46、48 ～ 63	Platinum
その他すべての値（0 を含む）	Silver

クライアントが WMM クライアントでない場合、WLAN の上書き（コントローラで設定された）によって、パケットが伝送される 802.11e キュー（Bronze、Gold、Platinum、または Silver）が決定されます。

メッシュ アクセス ポイントのクライアントの場合、メッシュ バックホールまたはイーサネットでの伝送に備えて、着信クライアント フレームが変更されます。 WMM クライアントの場合、MAP が着信 WMM クライアント フレームから外部 DSCP 値を設定する方法を示します。

図 *85* : *MAP* から *RAP* へのパス



着信 802.11e ユーザ優先度および WLAN の上書き優先度の最小値が、次の表に示す情報を使用して変換され、IP フレームの DSCP 値が決定されます。 たとえば、着信フレームの優先度の値が Gold 優先度を示しているが、WLAN が Silver 優先度に設定されている場合は、最小優先度の Silver を使用して DSCP 値が決定されます。

表 *35* : *DSCP* とバックホール キューのマッピング

DSCP 値	802.11e UP	バックホール キュー	パケット タイプ
2、4、6、8 ～ 23	1、2	Bronze	最小の優先度のパケット（存在する場合）
26、32 ～ 34	4、5	Gold	ビデオ パケット
46 ～ 56	6、7	Platinum	CAPWAP 制御、AWPP、DHCP/DNS、ARP パケット、音声パケット
その他すべての値（0 を含む）	0、3	Silver	ベスト エフォート、CAPWAP データ パケット

着信 WMM 優先度がない場合、デフォルトの WLAN 優先度を使用して、外部ヘッダーの DSCP 値が生成されます。 フレームが（AP で）生成された CAPWAP 制御フレームの場合は、46 の DSCP 値が外部ヘッダーに配置されます。

5.2 コード拡張では、DSCP 情報が AWPP ヘッダーに保持されます。

Platinum キューを経由する DHCP/DNS パケットと ARP パケットを除き、すべての有線クライアント トラフィックは 5 の最大 802.1p UP 値に制限されます。

WMM 以外のワイヤレス クライアント トラフィックは、その WLAN のデフォルトの QoS 優先度を取得します。 WMM ワイヤレス クライアント トラフィックには 802.11e の最大値の 6 を設定することができますが、それらはその WLAN に設定された QoS プロファイル未満である必要があ

ります。 アドミッション制御を設定した場合、WMM クライアントは TSPEC シグナリングを使用し、CAC によって許可されている必要があります。

CAPWAPP データ トラフィックはワイヤレス クライアント トラフィックを伝送し、ワイヤレス クライアント トラフィックと同じ優先度を持ち、同じように扱われます。

DSCP 値が決定されたので、さらに、RAP から MAP へのバックホール パスの先述したルールを使用して、フレームを伝送するバックホール キューが決定されます。 RAP からコントローラに伝送されるフレームはタグ付けされません。 外部 DSCP 値は最初に作成されているため、そのままになります。

ブリッジ バックホール パケット

ブリッジ サービスの処理は通常のコントローラベースのサービスと少し異なります。 ブリッジ パケットは、CAPWAP カプセル化されないため、外部 DSCP 値がありません。 そのため、メッシュ アクセス ポイントによって受信された IP ヘッダーの DSCP 値を使用して、メッシュ アクセス ポイントからメッシュ アクセス ポイント（バックホール）までのパスに示されたようにテーブルがインデックス化されます。

LAN 間のブリッジ パケット

LAN 上のステーションから受信されたパケットは、決して変更されません。 LAN 優先度の上書き値はありません。 したがって、LAN では、ブリッジ モードで適切に保護されている必要があります。 メッシュ バックホールに提供されている唯一の保護は、Platinum キューにマップされる CAPWAP 以外の制御フレームは Gold キューに降格されます。

パケットはメッシュへの着信時にイーサネット入口で受信されるため、LAN に正確に伝送されます。

AP1500 上のイーサネット ポートと 802.11a 間の QoS を統合する唯一の方法は、DSCP によってイーサネット パケットをタグ付けすることです。 AP1500 は DSCP を含むイーサネット パケットを取得し、それを適切な 802.11e キューに格納します。

AP1500 では、DSCP 自体をタグ付けしません。

- AP1500 は、入力ポートで DSCP タグを確認し、イーサネット フレームをカプセル化して、対応する 802.11e 優先度を適用します。
- AP1500 は、出力ポートでイーサネット フレームのカプセル化を解除し、DSCP フィールドをそのままにして、そのフレームを回線上に配置します。

ビデオ カメラなどのイーサネット デバイスは、QoS を使用するために、DSCP 値でビットをマークする機能を持つ必要があります。

（注） QoS は、ネットワーク上で輻輳が発生したときにだけ関連します。

メッシュ ネットワークでの音声使用のガイドライン

- 音声は、リリース5.2、6.0、7.0、および7.0.116.0の屋内メッシュ ネットワークでのみサポートされます。 屋外の場合、音声は、メッシュ インフラストラクチャにおいてベストエフォート方式でサポートされます。
- 音声がメッシュ ネットワークで動作している場合、コールは3 ホップ以上を通過してはいけません。 音声で 3 ホップ以上を必要としないように、各セクターを設定する必要があります。
- 音声ネットワークの RF の考慮事項は次のとおりです。
  - 2 ～ 10 % のカバレッジ ホール
  - 15 ～ 20 % のセル カバレッジ オーバーラップ
  - 音声がデータ要件より 15 dB 以上高い RSSI 値および SNR 値を必要とする
  - すべてのデータ レートの -67 dBm の RSSI が 11b/g/n および 11a/n の目標である
  - AP に接続するクライアントにより使用されるデータ レートの SNR は 25 dB である必要がある
  - パケット エラー レートの値が 1 % 以下の値になるように設定する必要がある
  - 最小使用率のチャネル（CU）を使用する必要がある
- [802.11a/n（または 802.11b/g/n）> *Global* parameters] ページで、次のことを行う必要があります。
  - Dynamic Transmit Power Control（DTPC）を有効にする
  - 11 Mbps 未満のすべてのデータ レートを無効にする
- [802.11a/n or 802.11b/g/n > *Voice* parameters] ページで、次のことを行う必要があります。
  - 負荷に基づく CAC を無効にする
  - WMM が有効化されている CCXv4 または v5 クライアントに対してアドミッション コントロール（ACM）を有効にする。 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。
  - 最大 RF 帯域幅を 50 % に設定する
  - 予約済みローミング帯域幅を 6 % に設定する
  - トラフィック ストリーム メトリックを有効にする
- [802.11a/n or 802.11b/g/n > *EDCA* parameters] ページで、次のことを行う必要があります。
  - インターフェイスの EDCA プロファイルを [Voice Optimized] に設定する
  - 低遅延 MAC を無効にする

- [QoS > *Profile*] ページで、次のことを行う必要があります。
  - 音声プロファイルを作成して有線 QoS プロトコル タイプとして 802.1Q を選択する
- [WLANs > *Edit* > QoS] ページで、次のことを行う必要があります。
  - バックホールの QoS として [Platinum]（音声）および [Gold]（ビデオ）を選択する
  - WMM ポリシーとして [Allowed] を選択する
- [WLANs > *Edit* > QoS] ページで、次のことを行う必要があります。
  - 高速ローミングをサポートする場合、認可（*auth*）キー管理（*mgmt*）で [CCKM] を選択します。 詳細については、「クライアント ローミング」の項を参照してください。
- [x > y] ページで、次のことを行う必要があります。
  - Voice Active Detection（VAD）を無効にする

メッシュ ネットワークでの音声コールのサポート

次の表に、クリーンで理想的な環境での実際のコールを示します。

表 *36*：*802.11a* 無線および *802.11b/g* 無線で可能な *1520* シリーズのコール[13]

No. of Calls	802.11a 無線	802.11b/g 無線
RAP	12	12
MAP1	7	10
MAP2	4	8

次の表に、クリーンで理想的な環境での実際のコールを示します。

表 *37*：*802.11a/n* 無線および *802.11b/g/n* 無線で可能な *1550* シリーズのコール[14]

No. of Calls	802.11a/n 無線 20 MHz	802.11a/n 無線 40 MHz	802.11b/g/n バックホール無線 20 MHz	802.11b/g/n バックホール無線 40 MHz
RAP	20	35	20	20
MAP1（最初のホップ）	10	20	15	20
MAP2（2番目のホップ）	8	15	10	15

コールを発信する間、7921 電話のコールの MOS スコアを確認します（次の表を参照してください）。 3.5 ～ 4 の MOS スコアが許容可能です。

表 *38*：*MOS* 評点

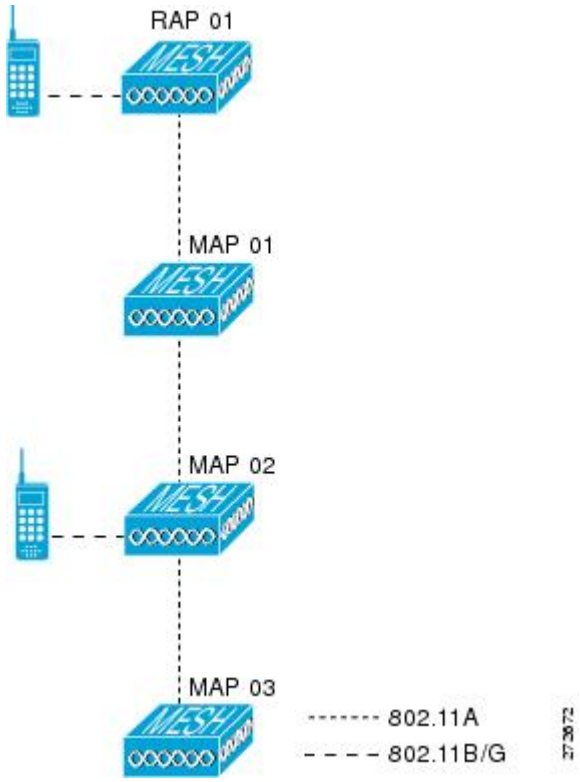
MOS 評価	ユーザ満足度
> 4.3	たいへん満足している
4.0	満足している
3.6	一部のユーザが満足していない
3.1	多くのユーザが満足していない
< 2.58	—

メッシュ ネットワークの音声詳細の表示（CLI）

この項のコマンドを使用して、メッシュ ネットワークの音声およびビデオコールの詳細を表示します。

（注） CLI コマンドを使用して出力を表示する場合は、次の図を参照してください。

図 *86* : メッシュ ネットワークの例



- 各RAPでの音声コールの合計数と音声コールに使用された帯域幅を表示するには、次のコマンドを入力します。

  show mesh cac summary

  以下に類似した情報が表示されます。

```
AP Name          Slot#   Radio  BW Used/Max  Calls
------------    -------  -----  -----------  -----
SB_RAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    2
SB_MAP1              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP2              0   11b/g     0/23437    0
                     1   11a       0/23437    0
SB_MAP3              0   11b/g     0/23437    0
                     1   11a      0/23437    0?
```

- ネットワークのメッシュ ツリー トポロジおよび各メッシュ アクセス ポイントと無線の音声コールとビデオ リンクの帯域幅使用率（使用/最大）を表示するには、次のコマンドを入力します。

  show mesh cac bwused {**voice** | **video**} *AP_name*

以下に類似した情報が表示されます。

```
AP Name        Slot#    Radio       BW Used/Max
-------------- -------  -----       -----------
SB_RAP1          0      11b/g        1016/23437
                 1      11a          3048/23437
|SB_MAP1         0      11b/g        0/23437
                 1      11a          3048/23437
||  SB_MAP2      0      11b/g        2032/23437
                 1      11a          3048/23437
||| SB_MAP3      0      11b/g        0/23437
                 1      11a          0/23437
```

（注） [AP Name] フィールドの左側の縦棒（|）は、MAP のその RAP からのホップ カウントを示します。

（注） 無線タイプが同じ場合、各ホップでのバックホール帯域幅使用率（bw使用/最大）は同じです。たとえば、メッシュ アクセス ポイント *map1*、*map2*、*map3*、および *rap1* はすべて同じ無線バックホール（802.11a）上にあるので、同じ帯域幅（3048）を使用しています。 コールはすべて同じ干渉ドメインにあります。 そのドメインのどの場所から発信されたコールも、他のコールに影響を与えます。

- ネットワークのメッシュ ツリー トポロジを表示し、メッシュ アクセス ポイント無線によって処理中の音声コール数を表示するには、次のコマンドを入力します。

  show mesh cac access *AP_name*

  以下に類似した情報が表示されます。

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） メッシュ アクセス ポイント無線で受信された各コールによって、該当のコール サマリー カラムが 1 つずつ増加されます。 たとえば、*map2* の 802.11b/g 無線でコールが受信されると、その無線の *calls* カラムにある既存の値に 1 が加えられます。 上記の例の場合、*map2* の 802.11b/g 無線でアクティブなコールは、新しいコールだけです。 新しいコールが受信されるときに 1 つのコールがアクティブである場合、値は 2 になります。

- ネットワークのメッシュ ツリー トポロジを表示し、動作中の音声コールを表示するには、次のコマンドを入力します。

show mesh cac callpath *AP_name*

以下に類似した情報が表示されます。

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        1
|   SB_MAP1          0      11b/g      0
                     1      11a        1
||  SB_MAP2          0      11b/g      1
                     1      11a        1
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） コール パス内にある各メッシュ アクセス ポイント無線の *Calls* カラムは 1 ずつ増加します。 たとえば、*map2* (**show mesh cac call path** *SB_MAP2*) で発信され、*map1* を経由して *rap1* で終端するコールの場合、1 つのコールが *map2* 802.11b/g および 802.11a 無線の *calls* カラムに加わり、1 つのコールが *map1* 802.11a バックホール無線の *calls* カラムに加わり、1 つのコールが *rap1* 802.11a バックホール無線の *calls* カラムに加わります。

- ネットワークのメッシュ ツリー トポロジ、帯域幅の不足のためメッシュ アクセス ポイント無線で拒否される音声コール、拒否が発生した対応するメッシュ アクセス ポイント無線を表示するには、次のコマンドを入力します。

  show mesh cac rejected *AP_name*

  以下に類似した情報が表示されます。

```
AP Name             Slot#   Radio     Calls
-------------      -------  -----    -----
SB_RAP1              0      11b/g      0
                     1      11a        0
|   SB_MAP1          0      11b/g      0
                     1      11a        0
||  SB_MAP2          0      11b/g      1
                     1      11a        0
||| SB_MAP3          0      11b/g      0
                     1      11a        0
```

（注） コールが *map2* 802.11b/g 無線で拒否された場合、*Calls* カラムは 1 ずつ増加します。

- 指定のアクセス ポイントでアクティブな Bronze、Silver、Gold、Platinum、および管理キューの数を表示するには、次のコマンドを入力します。 各キューのピークおよび平均長と、オーバーフロー数が表示されます。

  show mesh queue-stats *AP_name*

  以下に類似した情報が表示されます。

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
```

```
Platinum    0          4          0.001
Bronze      0          0          0.000
Management  0          0          0.000
```

Overflows：キュー オーバーフローによって破棄されたパケットの総数。

Peak Length：定義された統計期間中にキューで待機していたパケットの最大数。

Average Length：定義された統計期間中にキューで待機していたパケットの平均数。

ビデオのメッシュ マルチキャストの抑制の有効化

コントローラ CLI を使用して 3 種類のメッシュ マルチキャスト モードを設定し、すべてのメッシュ アクセス ポイントでビデオ カメラ ブロードキャストを管理できます。 イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

メッシュ マルチキャスト モードは、ブリッジング対応アクセス ポイント MAP および RAP が、メッシュ ネットワーク内のイーサネット LAN 間でマルチキャストを送信する方法を決定します。メッシュ マルチキャスト モードは非 CAPWAP マルチキャスト トラフィックのみを管理します。CAPWAP マルチキャスト トラフィックは異なるメカニズムで管理されます。

次の 3 つのメッシュ マルチキャスト モードがあります。

- regular モード：データは、ブリッジング対応 RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにマルチキャストされます。
- in-only モード：MAP がイーサネットから受信するマルチキャスト パケットは RAP のイーサネット ネットワークに転送されます。 追加の転送は行われず、これにより、RAP によって受信された CAPWAP 以外のマルチキャストはメッシュ ネットワーク内の MAP イーサネット ネットワーク（それらの発信ポイント）に返送されず、MAP から MAP へのマルチキャストはフィルタで除去されるため発生しません。

（注） HSRP 設定がメッシュ ネットワークで動作中の場合は、in-out マルチキャスト モードを設定することをお勧めします。

- in-out モード：RAP と MAP は別々の方法でマルチキャストを行います。
  - in-out モードはデフォルトのモードです。
  - マルチキャスト パケットが、イーサネット経由で MAP で受信されると、それらは RAP に送信されますが、それらはイーサネット経由で他の MAP に送信されず、MAP から MAP へのパケットは、マルチキャストからフィルタで除去されます。
  - マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。 in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

（注） 802.11bクライアントがCAPWAPマルチキャストを受信する必要がある場合、マルチキャストをメッシュ ネットワーク上だけでなく、コントローラ上でグローバルにイネーブルにする必要があります（**config network multicast global enable** CLI コマンドを使用）。 マルチキャストをメッシュ ネットワーク外部の 802.11b クライアントに伝送する必要がない場合は、グローバルなマルチキャスト パラメータを無効にする必要があります（**config network multicast global disable** コマンドを使用）。

メッシュ ネットワークでのマルチキャストの有効化（CLI）

メッシュ ネットワークでマルチキャスト モードを有効にしてメッシュ ネットワーク外からのマルチキャストを受信するには、次のコマンドを入力します。

config network multicast global enable

config mesh multicast {**regular** | **in** | **in-out**}

メッシュ ネットワークのみでマルチキャスト モードを有効にする（マルチキャストはメッシュ ネットワーク外の 802.11b クライアントに伝送する必要がない）には、次のコマンドを入力します。

config network multicast global disable

config mesh multicast {**regular** | **in** | **in-out**}

（注） コントローラ GUI を使用してメッシュ ネットワークのマルチキャストをイネーブルにすることはできません。

IGMP スヌーピング

IGMP スヌーピングを使用すると、特別なマルチキャスト転送により、RF 使用率が向上し、音声およびビデオ アプリケーションでのパケット転送が最適化されます。

メッシュ アクセス ポイントは、クライアントがマルチキャスト グループに登録されているメッシュ アクセス ポイントに関連付けられている場合にだけ、マルチキャスト パケットを伝送します。 そのため、IGMP スヌーピングが有効な場合、指定したホストに関連するマルチキャスト トラフィックだけが転送されます。

コントローラ上で IGMP スヌーピングをイネーブルにするには、次のコマンドを入力します。

configure network multicast igmp snooping enable

クライアントは、メッシュ アクセス ポイントを経由してコントローラに転送される IGMP *join* を送信します。 コントローラは、*join* を代行受信し、マルチキャスト グループ内のクライアントの

テーブル エントリを作成します。 次にコントローラはアップストリーム スイッチまたはルータを経由して、IGMP *join* をプロキシします。

次のコマンドを入力して、ルータで IGMP グループのステータスをクエリーできます。

```
router# show ip gmp groups
IGMP Connected Group Membership

Group Address    Interface   Uptime  Expires    Last Reporter
233.0.0.1        Vlan119     3w1d    00:01:52   10.1.1.130
```

レイヤ 3 ローミングの場合、IGMP クエリーはクライアントの WLAN に送信されます。 コントローラはクライアントの応答を転送する前に変更し、ソース IP アドレスをコントローラの動的インターフェイス IP アドレスに変更します。

ネットワークは、コントローラのマルチキャスト グループの要求をリッスンし、マルチキャストを新しいコントローラに転送します。

音声の詳細については、次のマニュアルを参照してください。

- 『Video Surveillance over Mesh Deployment Guide』：http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080b02511.shtml
- 『Cisco Unified Wireless Network Solution: VideoStream Deployment Guide』：http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080b6e11e.shtml

メッシュ AP のローカルで有効な証明書

7.0 リリースまでは、メッシュ AP は、コントローラを認証したり、コントローラに join するためにコントローラにより認証を受けたりするために、製造元がインストールした証明書（MIC）しかサポートしていませんでした。 CA の制御、ポリシーの定義、有効な期間の定義、生成された証明書の制限および使用方法の定義、および AP とコントローラでインストールされたこれらの証明書の取得を行うために、独自の公開鍵インフラストラクチャ（PKI）を用意する必要がある場合がありました。 これらのユーザ生成証明書またはローカルで有効な証明書（LSC）が AP とコントローラにある場合、デバイスはこれらの LSC を使用して join、認証、およびセッション キーの派生を行います。 5.2 リリース以降では通常の AP がサポートされ、7.0 リリース以降ではメッシュ AP もサポートされるようになりました。

7.0.116.0 リリースでは、次の機能が追加されました。

- AP が LSC 証明書を使用してコントローラに join できない場合の MIC へのグレースフル フォールバック：ローカル AP は、コントローラで設定された回数（デフォルト値は 3）、コントローラに join しようとします。 これらの試行後に、AP は LSC を削除し、MIC を使用してコントローラに join しようとします。

  メッシュ AP は、孤立タイマーが切れ、AP がリブートされるまで LSC を使用してコントローラに join しようとします。 孤立タイマーは 40 分に設定されます。 リブート後に、AP は MIC を使用してコントローラに join しようとします。 40 分後に AP が MIC を使用して再びコントローラに join できない場合は、AP がリブートされ、LSC を使用してコントローラに join しようとします。

（注） メッシュ AP の LSC は削除されません。 LSC は、コントローラで無効な場合にのみメッシュ AP で削除され、その結果、AP がリブートされます。

- MAP の無線プロビジョニング

注意事項および制約事項

- この機能により、AP からどの既存の証明書も削除されません。 AP では LSC 証明書と MIC 証明書の両方を使用できます。
- AP が LSC を使用してプロビジョニングされると、AP は起動時に MIC 証明書を読み取りません。 LSC から MIC に変更するには、AP をリブートする必要があります。 AP は、LSC を使用して join できない場合に、フォールバックのためにこの変更を行います。
- AP で LSC をプロビジョニングするために、AP で無線をオフにする必要はありません。このことは、無線でプロビジョニングを行うことができるメッシュ AP にとって重要です。
- メッシュ AP では dot1x 認証が必要なため、サーバ（設定に応じてコントローラまたはサードパーティ サーバ）で CA 証明書と ID 証明書が必要です。
- LSC プロビジョニングはイーサネット経由の場合のみサポートされます。イーサネットを介してコントローラにメッシュ AP を接続し、LSC 証明書をプロビジョニングする必要があります。 LSC がデフォルトになると、AP は LSC 証明書を使用して無線でコントローラに接続できます。

メッシュ AP の LSC と通常の AP の LSC の違い

CAPWAP AP は、AP モードに関係なく、join 時に LSC を使用して DTLS のセットアップを行います。 また、メッシュ AP は、親 AP からメッシュ セキュリティのための証明書を使用します（コントローラ（または、外部 AAA サーバ）と dot1x 認証が行われます）。 LSC を使用してメッシュ AP がプロビジョニングされたら、この目的のために LSC を使用する必要があります。これは、MIC が読み込まれないためです。

メッシュ AP は、静的に設定された dot1x プロファイルを使用して認証します。

このプロファイルは、証明書の発行元として「cisco」を使用するようハードコーディングされています。 このプロファイルは、メッシュ認証にベンダー証明書を使用できるよう設定可能にする必要があります（**config local-auth eap-profile cert-issuer vendor "prfMaP1500LlEAuth93"** コマンドを入力します）。

メッシュ AP の LSC を有効または無効にするには、**config mesh lsc enable/disable** コマンドを入力する必要があります。 このコマンドを実行すると、すべてのメッシュ AP がリブートされます。

（注） 7.0 リリースでは、メッシュの LSC は、非常に限定された石油およびガス業界のお客様向けに提供されています。 これは、隠し機能です。 **config mesh lsc enable/disable** は隠しコマンドです。 また、**config local-auth eap-profile cert-issuer vendor "prfMaP1500Ll/EAuth93"** コマンドは通常のコマンドですが、「prfMaP1500LlEAuth93」プロファイルは隠しプロファイルであり、コントローラに格納されず、コントローラのリブート後に失われます。

LSC AP での証明書検証プロセス

LSC でプロビジョニングされた AP には LSC 証明書と MIC 証明書の両方がありますが、LSC 証明書がデフォルトの証明書になります。 検証プロセスは次の 2 つの手順から構成されます。

ステップ 1 コントローラが AP に MIC デバイス証明書を送信し、AP が MIC CA を使用してその証明書を検証します。

ステップ 2 AP は LSC デバイス証明書をコントローラに送信し、コントローラは LSC CA を使用してその証明書を検証します。

LSC の設定（CLI）

ステップ 1 LSC を有効にし、コントローラで LSC CA 証明書をプロビジョニングします。

ステップ 2 次のコマンドを入力します。
config local-auth eap-profile cert-issuer vendor *prfMaP1500LlEAuth93*

ステップ 3 次のコマンドを入力して、機能をオンにします。
config mesh lsc {**enable** | **disable**}

ステップ 4 同じ証明書サーバからコントローラ（または、他の任意の認証サーバ）に CA および ID 証明書をインストールします。

ステップ 5 イーサネットを介してメッシュ AP に接続し、LSC 証明書のためにプロビジョニングします。

ステップ 6 メッシュ AP で証明書を取得し、LSC 証明書を使用してコントローラに join できます。

図 *87*：ローカルで有効な証明書

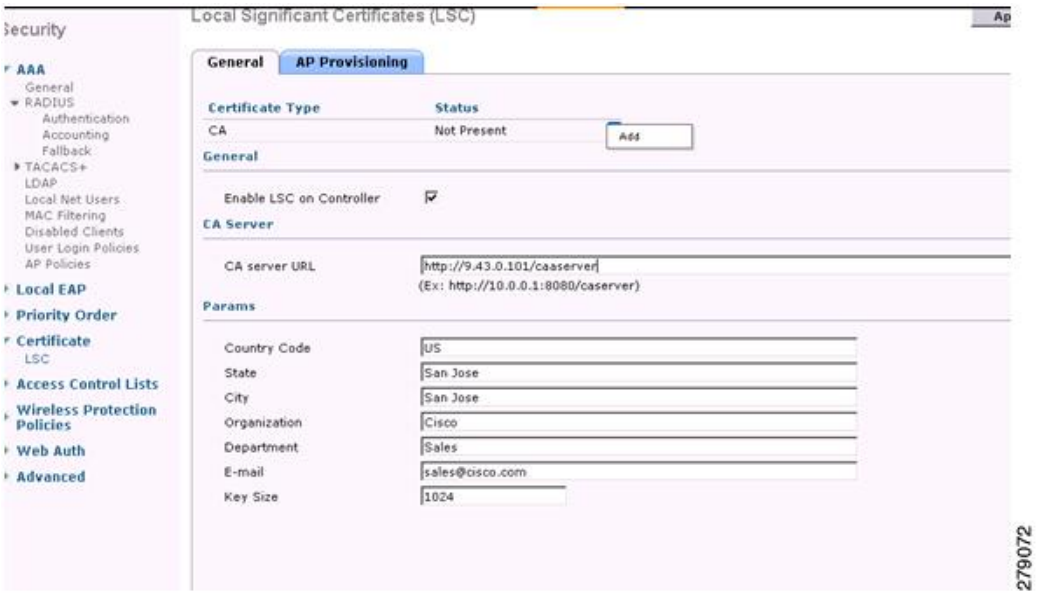
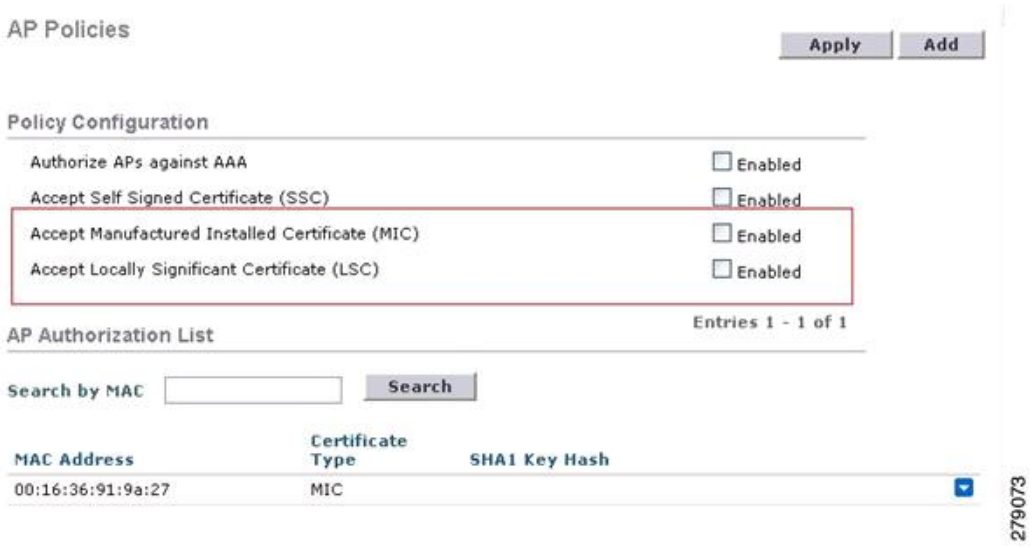


図 *88*：*AP* ポリシーの設定



LSC 関連のコマンド

LSC に関連するコマンドは次のとおりです。

- **config certificate lsc** {**enable** | **disable**}
  - **enable**：システムで LSC を有効にします。
  - **disable**：システムで LSC を無効にします。 LSC デバイス証明書を削除する場合や、AP にメッセージを送信して LSC デバイス証明書を削除し、LSC を無効にする場合は、このキーワードを使用します。その結果、以降の join を MIC/SSC を使用して行えるようになります。 MIC/SSC に切り替わっていない AP を使用できるようにするために、WLC での LSC CA 証明書の削除は、CLI を使用して明示的に行う必要があります。

- **config certificate lsc ca-server** *URL-Path*

  このコマンドは、証明書を取得するために CA サーバへの URL を設定します。 URL には、ドメイン名または IP アドレスのいずれか、ポート番号（通常は 80）、および CGI-PATH が含まれます。 次に例を示します。

  http://ipaddr:port/cgi-path

  CA サーバは 1 つだけ設定できます。 CA サーバは LSC をプロビジョニングするよう設定する必要があります。

- **config certificate lsc ca-server delete**

  このコマンドは、WLC で設定された CA サーバを削除します。

- **config certificate lsc ca-cert** {**add** | **delete**}

  このコマンドは、次のように、WLC の CA 証明書データベースに対して LSC CA 証明書を追加または削除します。

  - **add**：SSCEP getca 操作を使用して、設定された CA サーバで CA 証明書を問い合わせ、WLC にログインし、WLC データベースに証明書を永久的にインストールします。 インストールされたら、この CA 証明書は AP から受信された LSC デバイス証明書を検証するために使用されます。
  - **delete**：WLC データベースから LSC CA 証明書を削除します。

- **config certificate lsc subject-params** *Country State City Orgn Dept Email*

  このコマンドは、コントローラと AP で作成およびインストールされるデバイス証明書のパラメータを設定します。

  これらすべての文字列は、最大 3 バイトを使用する国を除き 64 バイトです。 Common Name は、イーサネット MAC アドレスを使用して自動的に生成されます。 Common Name は、コントローラ デバイス証明書要求を作成する前に提供する必要があります。

  上記のパラメータは LWAPP ペイロードとして AP に送信されるため、AP はこれらのパラメータを使用して certReq を生成できます。 CN は、現在の MIC/SSC の「Cxxxx-MacAddr」形式を使用して AP で自動的に生成されます。ここで、xxxx は製品番号です。

- **config certificate lsc other-params** *keysize validity*

  キーサイズおよび検証の設定にはデフォルト値が指定されています。 したがって、これらの値を設定することは必須ではありません。

  キーサイズの範囲は、360 ～ 2048（デフォルト値は 2048 ビット）です。

  検証期間は、1 ～ 20 年（デフォルト値は 10 年）の間で設定できます。

- **config certificate lsc ap-provision** {**enable** | **disable**}

  このコマンドは、AP が SSC/MIC を使用して join した場合に、AP で LSC のプロビジョニングを有効または無効にします。 有効な場合は、join し、LSC があるすべての AP がプロビジョニングされます。

  無効な場合は、自動的なプロビジョニングが行われません。 このコマンドは、LSC がすでにある AP に影響を与えます。

- **config certificate lsc ra-cert** {**add** | **delete**}

  このコマンドの使用は、CA サーバが Cisco IOS CA サーバである場合にお勧めします。 WLC は RA を使用して証明書要求を暗号化し、通信をセキュアにすることができます。 RA 証明書は現在、MSFT などの他の外部 CA サーバによりサポートされていません。

  - **add**：SCEP 操作を使用して、設定された CA サーバで RA 証明書を問い合わせ、その証明書を WLC データベースにインストールします。 このキーワードは、CA により署名された certReq を取得するために使用されます。
  - **delete**：WLC データベースから LSC RA 証明書を削除します。

- **config auth-list ap-policy lsc** {**enable** | **disable**}

  LSC の取得後に、AP は WLC に join しようとします。 AP が WLC に join しようとする前に、WLC コンソールでこのコマンドを実行する必要があります。 このコマンドの実行は必須です。 デフォルトでは、**config auth-list ap-policy lsc** コマンドは無効な状態にあり、AP は LSC を使用して WLC に join できません。

- **config auth-list ap-policy mic** {**enable** | **disable**}

  MIC の取得後に、AP は WLC に join しようとします。 AP が WLC に join しようとする前に、WLC コンソールでこのコマンドを実行する必要があります。 このコマンドの実行は必須です。 デフォルトでは、**config auth-list ap-policy mic** コマンドは有効な状態にあります。 有効な状態のため、AP が join できない場合は、WLC 側に「LSC/MIC AP is not allowed to join by config」というログ メッセージが表示されます。

コントローラ CLI show コマンド

WLC **show** コマンドは、次のとおりです。

- **show certificate lsc summary**

  このコマンドは、WLC にインストールされた LSC 証明書を表示します。 RA 証明書もすでにインストールされている場合は、CA 証明書、デバイス証明書、および RA 証明書（オプション）を表示します。 また、LSC が有効であるか有効でないかも示されます。

- **show certificate lsc ap-provision**

  このコマンドは、AP のプロビジョニングのステータス、プロビジョニングが有効であるか無効であるか、プロビジョニング リストが存在するか存在しないかを表示します。

- **show certificate lsc ap-provision details**

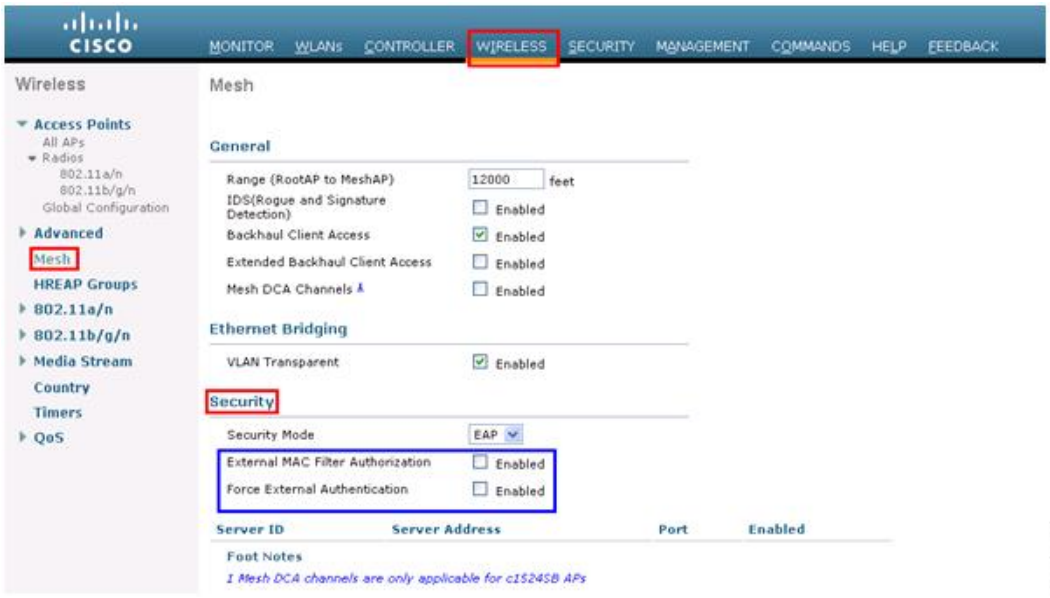
  このコマンドは、AP プロビジョニング リストに存在する MAC アドレスのリストを表示します。

コントローラ GUI セキュリティ設定

この設定はこの機能に直接関連しませんが、この設定を使用すると、LSC を使用してプロビジョニングされた AP に関する必要な動作を実現できます。

次の図に、メッシュ AP MAC 認可と EAP に対する 3 つのケースを示します。

図 *89*：メッシュ *AP MAC* 認可と *EAP* に対する *3* つのケース



- ケース 1：ローカル MAC 認可とローカル EAP 認証

  RAP/MAP の MAC アドレスをコントローラの MAC フィルタ リストに追加します。

  例：

```
(Cisco Controller) > config macfilter mac-delimiter colon
(Cisco Controller) > config macfilter add 00:0b:85:60:92:30 0 management
```

- ケース 2：外部 MAC 認可とローカル EAP 認証

  WLC で次のコマンドを入力します。

```
(Cisco Controller) > config mesh security rad-mac-filter enable
```

または

GUI ページで外部 MAC フィルタ認可のみをオンにし、次のガイドラインに従います。

- RAP/MAP の MAC アドレスをコントローラの MAC フィルタ リストに追加しません。
- WLC で、外部 RADIUS サーバの詳細を設定します。
- WLC で、**config macfilter mac-delimiter colon** コマンド設定を入力します。
- 外部 RADIUS サーバで、RAP/MAP の MAC アドレスを次の形式で追加します。
  User name: 11:22:33:44:55:66 Password: 11:22:33:44:55:66

- ケース 3：外部 EAP 認証

  WLC で外部 RADIUS サーバの詳細を設定し、コントローラで次の設定を適用します。

  ```
  (Cisco Controller) > config mesh radius-server index enable
  (Cisco Controller) > config mesh security force-ext-auth enable
  ```

  EAP 認証の形式（<*platform name string*>-<*Ethernet mac address hex string*>）で、ユーザ ID およびパスワードを AAA サーバに追加します。

  Cisco IOS AP の場合は、次の形式になります。

  username: c1240-112233445566 および *password: c1240-112233445566*（1240 プラットフォーム AP の場合）

  username: c1520-112233445566 および *password: c1520-112233445566*（1520 プラットフォーム AP の場合）

  1510 VxWorks ベースの AP の場合は、次の形式になります。

  username: 112233445566 および *password: 112233445566*

展開ガイドライン

- ローカル認証を使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラをインストールする必要があります。
- 外部 AAA サーバを使用する場合は、ベンダーの CA およびデバイス証明書を使用してコントローラをインストールする必要があります。
- メッシュ セキュリティが証明書発行元として「vendor」を使用するよう設定する必要があります。
- MAP は、バックアップ コントローラにフォール バックするときに LSC から MIC に切り替わることができません。
- メッシュ AP に対して LSC を有効または無効にするには、**config mesh lsc** {**enable** | **disable**} コマンドが必要です。 このコマンドを実行すると、すべてのメッシュ AP がリブートされます。 現時点では、このコマンドを無効にすると、非メッシュ AP もリブートされることがあります。

スロット バイアス オプション

スロット バイアス オプションについて

1524SB AP の電源投入時に、信号の強度に応じて、アップリンクにスロット 1 またはスロット 2 のいずれかを使用できます。 AWPP は両方のスロットを等しく扱います。 MAP の場合は、スロット 2 が優先される（バイアスを受ける）アップリンク スロット（つまり、親 AP に接続するために使用されるスロット）になります。 スロット 1 は、優先されるダウンリンク スロットになります。 ユーザが両方の無線スロットを使用でき、アップリンク バックホールにスロット 1 が使用される場合は、15 分タイマーが開始されます。 15 分後に、AP は、アップリンク バックホールにスロット 2 を再び使用できるようスロット 2 のチャネルをスキャンします。 このプロセスはスロット バイアスと呼ばれます。

適切なリニア機能を使用するためにスロット 2 で指向性アンテナを使用することをお勧めします。また、強いアップリンクを使用するためにスロット 2 を選択することをお勧めします。 ただし、モビリティのために両方のバックホール無線で指向性アンテナが使用される場合があることがあります。 AP の電源投入時に、いずれかの方向で親を選択できます。 スロット 1 が選択された場合は、15 分後に AP がスキャン モードに移行しないようにする必要があります。つまり、スロット バイアスを無効にする必要があります。

スロット バイアスの無効化

AP がスロット 1 で安定するようにスロット バイアスを無効にするには、**config mesh slot-bias disable** を使用します。

スロット バイアスをディセーブルにするには、次のコマンドを入力します。

```
(Cisco Controller) > config mesh slot-bias disable
```

（注） スロット バイアスはデフォルトで有効になります。

注意事項および制約事項

- **config mesh slot-bias disable** コマンドはグローバル コマンドであり、同じコントローラにアソシエートされたすべての 1524SB AP に適用できます。
- スロット バイアスは、スロット 1 とスロット 2 の両方が使用可能である場合にのみ適用できます。 動的周波数選択（DFS）のため、スロット無線に利用可能なチャネルがない場合は、他のスロットがアップリンクとダウンリンク両方の役割を担います。
- ハードウェアの問題のため、スロット 2 が利用可能でない場合でも、スロット バイアスは通常どおり機能します。 スロット バイアスを無効にするか、アンテナを修理して是正処置を取ってください。

- 15 分タイマーは、スロット 1 およびスロット 2 が使用可能である場合（動作するチャネルがある場合）にのみ開始されます（スロット バイアス）。
- 15 分タイマーは、DFS のため、スロット 2 がチャネルを見つけることができない場合は開始されません。この結果、スロット 1 はアップリンクとダウンリンクを引き継ぎます。
- DFS のため、スロット 1 に動作するチャネルがない場合、スロット 2 はスロット 1 を引き継ぎます。
- スロット 2 でハードウェア障害が発生した場合は、スロット バイアスが開始され、アップリンクにスロット 1 が選択されます。
- スロット バイアスを無効にすると、円滑な運用のために予防措置を取ることができます。

スロット バイアスに関連するコマンド

スロット バイアスに関連するコマンドは次のとおりです。

- スロットが使用されているのがアップリンクなのかダウンリンクなのかを確認するには、次のコマンドを入力します。

```
(Cisco Controller) > show mesh config

Mesh Range...................................... 12000
Mesh Statistics update period.................. 3 minutes
Backhaul with client access status............. enabled
Backhaul with extended client access status..... disabled
Background Scanning State...................... enabled
Backhaul Amsdu State........................... enabled
Mesh Security
   Security Mode............................... EAP
   External-Auth............................... disabled
   Use MAC Filter in External AAA server....... disabled
   Force External Authentication.............. disabled
Mesh Alarm Criteria
   Max Hop Count............................... 4
   Recommended Max Children for MAP............ 10
   Recommended Max Children for RAP............ 20
   Low Link SNR................................ 12
   High Link SNR............................... 60
   Max Association Number...................... 10
   Association Interval........................ 60 minutes
   Parent Change Numbers....................... 3
   Parent Change Interval...................... 60 minutes
Mesh Multicast Mode............................ In-Out
Mesh Full Sector DFS........................... enabled
Mesh Ethernet Bridging VLAN Transparent Mode..... enabled
Mesh DCA channels for serial backhaul APs....... disabled
Mesh Slot Bias................................. disabled
```

- アップリンクにスロット 1 が使用されていることを確認するには、次の手順を実行します。

  コントローラに次のコマンドを入力して、AP のデバッグをイネーブルにします。

```
(Cisco Controller) > debug ap enable AP_name
```

  コントローラに次のコマンドを入力します。

```
(Cisco Controller) > debug ap command show mesh config AP_name
(Cisco Controller) > debug ap command show mesh adjacency parent AP_name
```

優先される親の選択

MAPに対して優先される親を設定できます。 この機能を使用すると、細かい制御が可能になり、メッシュ環境でリニア トポロジを適用できます。 AWPP を省略し、優先される親への移行を強制できます。

注意事項および制約事項

子 AP は、次の基準に基づいて優先親を選択します。

- 優先される親は最良の親です。
- 優先される親には少なくとも 20 dB のリンク SNR があります（他の親はどんなに優れていても無視されます）。
- 優先される親には 12 dB ～ 20 dB の範囲内のリンク SNR がありますが、他の親が非常に優れていることはありません（つまり、SNR が 20 % 以上優れている）。 SNR が 12 dB 未満の場合、設定は無視されます。
- 優先される親はブラックリストに掲載されません。
- 優先される親は、12 dB ～ 20 dB の範囲内の（DFS）のため、サイレント モードになりません。
- 優先される親は同じブリッジ グループ名（BGN）に属します。 設定された優先される親が同じ BGN に属さず、他の親が利用可能でない場合、子はデフォルトの BGN を使用して親 AP に join します。

（注） スロット バイアスと優先される親の選択機能はお互い独立しています。 ただし、優先される親が設定されている場合は、スロット1またはスロット2（APが最初に確認した方）を使用して親への接続が行われます。 MAP でアップリンクにスロット 1 が選択されると、スロット バイアスが実行されます。 スロット 1 が選択されることがすでにわかっている場合は、スロット バイアスを無効にすることをお勧めします。

優先される親の設定

優先される親を設定するには、次のコマンドを入力します。

`(Cisco Controller) >` **config mesh parent preferred** *AP_name MAC*
値は次のとおりです。

- *AP_name* は、指定する必要がある子 AP の名前です。
- *MAC* は、指定する必要がある優先される親の MAC アドレスです。

（注） 優先される親を設定する場合、目的の親に対して実際のメッシュ ネイバーの MAC アドレスを指定してください。この MAC アドレスはベース無線の MAC アドレスで、最後の文字が f になります。たとえば、ベース無線の MAC アドレスが 00:24:13:0f:92:00 の場合、優先される親として 00:24:13:0f:92:0f を指定する必要があります。これが、メッシュ ネイバー関係に使用される実際の MAC アドレスです。

次に、MAP1SB アクセス ポイントの優先される親を設定する例を示します。00:24:13:0f:92:00 は、優先される親の MAC アドレスです。

```
(Cisco Controller) > config mesh parent preferred MAP1SB 00:24:13:0f:92:0f
```

優先される親の選択に関連するコマンドは次のとおりです。

- 設定された親を削除するには、次のコマンドを入力します。

```
(Cisco Controller) > config mesh parent preferred AP_name none
```

- 子 AP の優先親として設定された AP に関する情報を取得するには、次のコマンドを入力します。

```
(Cisco Controller) > show ap config general AP_name
```

次に、MAP1SB アクセス ポイントの設定情報を取得する例を示します。00:24:13:0f:92:00 は優先親の MAC アドレスです。

```
(Cisco Controller) > show ap config general MAP1SB

Cisco AP Identifier.............................. 9
Cisco AP Name.................................... MAP1SB
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...................................... 12:12:12:12:12:12
IP Address Configuration......................... DHCP
IP Address....................................... 209.165.200.225
IP NetMask....................................... 255.255.255.224
CAPWAP Path MTU.................................. 1485
Domain.......................................
Name Server...................................
Telnet State..................................... Disabled
Ssh State........................................ Disabled
Cisco AP Location................................ default location
Cisco AP Group Name.............................. default-group
Primary Cisco Switch Name........................ 4404
Primary Cisco Switch IP Address.................. 209.165.200.230
Secondary Cisco Switch Name......................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name....................... 4404
Tertiary Cisco Switch IP Address................. 3.3.3.3
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Global: Disabled, Local: Disabled
```

```
AP subMode ..................................... WIPS
Remote AP Debug ................................ Disabled
S/W  Version ................................... 5.1.0.0
Boot  Version .................................. 12.4.10.0
Mini IOS Version ............................... 0.0.0.0
Stats Reporting Period ......................... 180
LED State....................................... Enabled
PoE Pre-Standard Switch......................... Enabled
PoE Power Injector MAC Addr..................... Disabled
Power Type/Mode................................. PoE/Low Power (degraded mode)
Number Of Slots................................. 2
AP Model........................................ AIR-LAP1252AG-A-K9
IOS Version..................................... 12.4(10:0)
Reset Button.................................... Enabled
AP Serial Number................................ serial_number
AP Certificate Type............................. Manufacture Installed
Management Frame Protection Validation.......... Enabled (Global MFP Disabled)
AP User Mode.................................... CUSTOMIZED
AP username..................................... maria
AP Dot1x User Mode.............................. Not Configured
AP Dot1x username............................... Not Configured
Cisco AP system logging host.................... 255.255.255.255
AP Up Time...................................... 4 days, 06 h 17 m 22 s
AP LWAPP Up Time................................ 4 days, 06 h 15 m 00 s
Join Date and Time.............................. Mon Mar 3 06:19:47 2008

Ethernet Port Duplex............................ Auto
Ethernet Port Speed............................. Auto
AP Link Latency................................. Enabled
 Current Delay.................................. 0 ms
 Maximum Delay.................................. 240 ms
 Minimum Delay.................................. 0 ms
 Last updated (based on AP Up Time)............. 4 days, 06 h 17 m 20 s
Rogue Detection................................. Enabled
AP TCP MSS Adjust............................... Disabled
Mesh preferred parent........................... 00:24:13:0f:92:00
```

同一チャネルの干渉

隠しノードの干渉以外に、同一チャネルの干渉もパフォーマンスに影響する可能性があります。同一チャネルの干渉は、同じチャネルの隣接する無線がローカル メッシュ ネットワークのパフォーマンスに干渉するときに発生します。 この干渉は、CSMA によるコリジョンまたは過度の遅延という形で現れます。いずれの場合でも、メッシュ ネットワークのパフォーマンスが低下します。適切なチャネル管理をすれば、ワイヤレス メッシュ ネットワーク上の同一チャネルの干渉は最小化できます。

メッシュ アクセス ポイントのメッシュ統計情報の表示

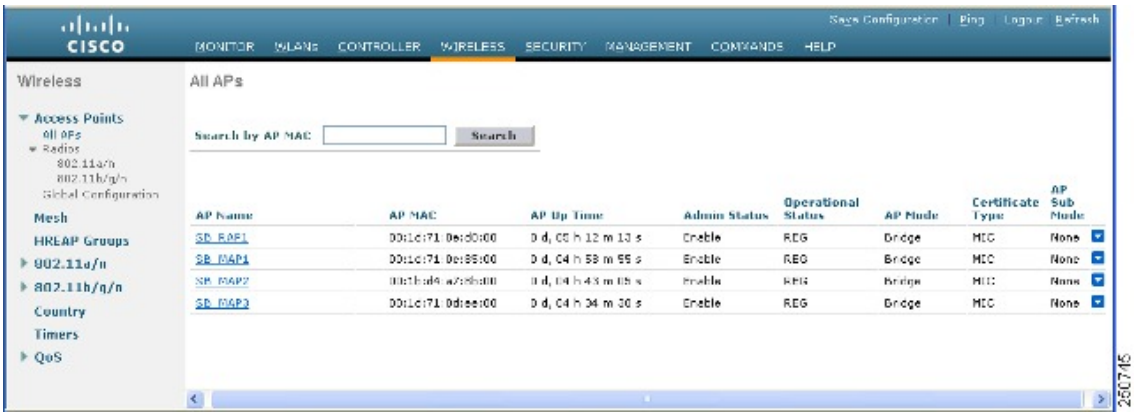
この項では、コントローラの GUI または CLI を使用して、特定のメッシュ アクセス ポイントのメッシュ統計情報を表示する方法について説明します。

（注） コントローラの GUI の [All APs > Details] ページでは、統計情報タイマー間隔の設定を変更できます。

メッシュ アクセス ポイントのメッシュ統計情報の表示（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。

図 ***90*** : ***[All APs]*** ページ



ステップ 2 特定のメッシュ アクセス ポイントの統計情報を表示するには、目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Statistics] を選択します。 選択したメッシュ アクセス ポイントの [All APs > *AP Name* > Statistics] ページが表示されます

図 *91*：*[All APs > Access Point Name > Statistics]* ページ

このページには、メッシュ ネットワークでのメッシュ アクセス ポイントのロール、メッシュ アクセス ポイントが属するブリッジ グループの名前、アクセス ポイントが動作するバックホール インターフェイス、および物理スイッチ ポート数が表示されます。 このメッシュ アクセス ポイントのさまざまなメッシュ統計情報も表示されます。 次の表に、各統計情報について説明します。

表 *39*：メッシュ アクセス ポイントの統計情報

統計情報	パラメータ	説明
Mesh Node Stats	Malformed Neighbor Packets	ネイバーから受信した不正な形式のパケットの数。不正な形式のパケットの例には、不正な形式のショート DNS パケットや不正な形式の DNS 応答といったトラフィックの悪意のあるフラッドがあります。
	Poor Neighbor SNR Reporting	信号対雑音比がバックホール リンクで 12 dB 未満になった回数。
	Excluded Packets	除外したネイバー メッシュ アクセス ポイントから受信したパケットの数。
	Insufficient Memory Reporting	メモリ不足になった状態の数。
	Rx Neighbor Requests	ネイバー メッシュ アクセス ポイントから受信したブロードキャストおよびユニキャストの要求数。
	Rx Neighbor Responses	ネイバーメッシュアクセスポイントから受信した応答数。
	Tx Neighbor Requests	ネイバー メッシュ アクセス ポイントに送信したブロードキャストおよびユニキャストの要求数。
	Tx Neighbor Responses	ネイバー メッシュ アクセス ポイントに送信した応答数。
	Parent Changes Count	メッシュ アクセス ポイント（子）が別の親に移動した回数。
	Neighbor Timeouts Count	ネイバー タイムアウト回数。

統計情報	パラメータ	説明
Queue Stats	Gold Queue	定義された統計期間中にGold（ビデオ）キューで待機していたパケットの平均および最大数。
	Silver Queue	定義された統計期間中にSilver（ベストエフォート）キューで待機していたパケットの平均および最大数。
	Platinum Queue	定義された統計期間中にPlatinum（音声）キューで待機していたパケットの平均および最大数。
	Bronze Queue	定義された統計期間中にBronze（バックグラウンド）キューで待機していたパケットの平均および最大数。
	Management Queue	定義された統計期間中に管理キューで待機していたパケットの平均および最大数。

統計情報	パラメータ	説明
Mesh Node Security Stats	Transmitted Packets	選択したメッシュアクセスポイントによってセキュリティネゴシエーション中に送信されたパケット数。
	Received Packets	選択したメッシュアクセスポイントによってセキュリティネゴシエーション中に受信されたパケット数。
	Association Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生したアソシエーション要求の失敗数。
	Association Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生したアソシエーション要求のタイムアウト回数。
	Association Requests Successful	選択したメッシュ アクセス ポイントとその親の間で発生したアソシエーション要求の成功数。
	Authentication Request Failures	選択したメッシュ アクセス ポイントとその親の間で発生した認証要求の失敗数。
	Authentication Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生した認証要求のタイムアウト回数。
	Authentication Requests Successful	選択したメッシュ アクセス ポイントとその親の間の認証要求の成功数。
	Reassociation Request Failures	選択したメッシュ アクセス ポイントとその親の間の再アソシエーション要求の失敗数。
	Reassociation Request Timeouts	選択したメッシュ アクセス ポイントとその親の間の再アソシエーション要求のタイムアウト回数。
	Reassociation Requests Successful	選択したメッシュ アクセス ポイントとその親の間の再アソシエーション要求の成功数。
	Reauthentication Request Failures	選択したメッシュ アクセス ポイントとその親の間の再認証要求の失敗数。
	Reauthentication Request Timeouts	選択したメッシュ アクセス ポイントとその親の間で発生した再認証要求のタイムアウト回数。
	Reauthentication Requests Successful	選択したメッシュ アクセス ポイントとその親の間で発生した再認証要求の成功数。

統計情報	パラメータ	説明
	Unknown Association Requests	親メッシュ アクセス ポイントが子から受信した不明なアソシエーション要求の数。 不明なアソシエーション要求は、子が不明なネイバー メッシュ アクセス ポイントの場合によくみられます。
	Invalid Association Requests	親メッシュ アクセス ポイントが選択した子メッシュ アクセスポイントから受信した無効なアソシエーション要求の数。 この状況は、選択した子が有効なネイバーであるが、アソシエーションが許可される状態ではないときに発生することがあります。
Mesh Node Security Stats（続き）	Unknown Reauthentication Requests	親メッシュ アクセス ポイントが子から受信した不明な再認証要求の数。 この状況は、子メッシュ アクセス ポイントが不明なネイバーであるときに発生することがあります。
	Invalid Reauthentication Requests	親メッシュ アクセス ポイントが子から受信した無効な再認証要求の数。 この状況は、子が有効なネイバーであるが、再認証に適した状態でないときに発生することがあります。
	Unknown Reassociation Requests	親メッシュ アクセス ポイントが子から受信した不明な再アソシエーション要求の数。 この状況は、子メッシュ アクセスポイントが不明なネイバーであるときに発生することがあります。
	Invalid Reassociation Requests	親メッシュ アクセス ポイントが子から受信した無効な再アソシエーション要求の数。 この状況は、子が有効なネイバーであるが、再アソシエーションに適した状態でないときに発生することがあります。

メッシュ アクセス ポイントのメッシュ統計情報の表示（CLI）

コントローラのCLIを使用して、特定のメッシュ アクセス ポイントのメッシュ統計情報を表示するには、次のコマンドを使用します。

- 特定のメッシュ アクセス ポイントのアソシエーションと認証、再アソシエーションと再認証に関して、失敗、タイムアウト、および成功の数などのパケット エラー統計情報を表示するには、次のコマンドを入力します。

show mesh security-stats *AP_name*

以下に類似した情報が表示されます。

```
AP MAC : 00:0B:85:5F:FA:F0
Packet/Error Statistics:
----------------------------
x Packets 14, Rx Packets 19, Rx Error Packets 0

Parent-Side Statistics:
-------------------------
Unknown Association Requests 0
Invalid Association Requests 0
Unknown Re-Authentication Requests 0
Invalid Re-Authentication Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0
Unknown Re-Association Requests 0
Invalid Re-Association Requests 0

Child-Side Statistics:
-------------------------
Association Failures 0
Association Timeouts 0
Association Successes 0
Authentication Failures 0
Authentication Timeouts 0
Authentication Successes 0
Re-Association Failures 0
Re-Association Timeouts 0
Re-Association Successes 0
Re-Authentication Failures 0
Re-Authentication Timeouts 0
Re-Authentication Successes 0
```

- キュー内のパケット数をキューのタイプ別に表示するには、次のコマンドを入力します。

  show mesh queue-stats *AP_name*

  以下に類似した情報が表示されます。

```
Queue Type  Overflows  Peak length  Average length
 ----------  ---------  -----------  --------------
 Silver      0          1            0.000
 Gold        0          4            0.004
 Platinum    0          4            0.001
 Bronze      0          0            0.000
 Management  0          0            0.000
```

  Overflows：キュー オーバーフローによって破棄されたパケットの総数。

  Peak Length：定義された統計期間中にキューで待機していたパケットの最大数。

  Average Length：定義された統計期間中にキューで待機していたパケットの平均数。

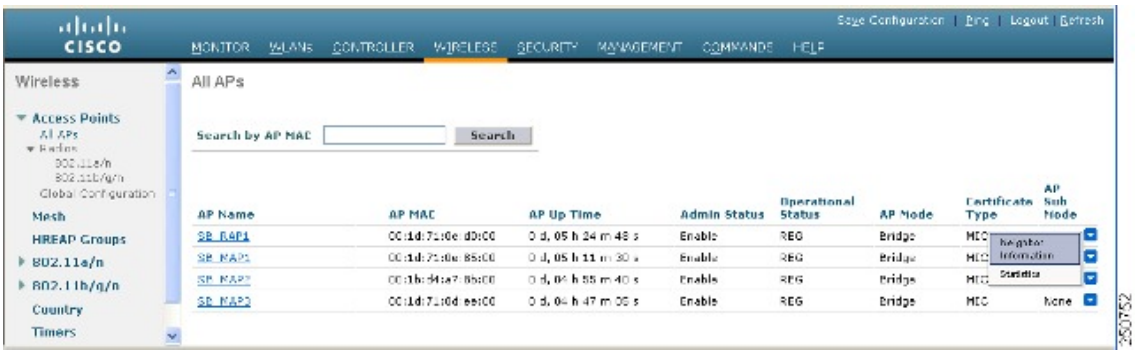
メッシュ アクセス ポイントのネイバー統計情報の表示

この項では、コントローラの GUI または CLI を使用して、選択したメッシュ アクセス ポイントのネイバー統計情報を表示する方法について説明します。 さらに、選択したメッシュ アクセス ポイントとその親とのリンク テストの実行方法についても説明します。

メッシュ アクセス ポイントのネイバー統計情報の表示（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。

図 *92*：*[All APs]* ページ



ステップ 2 特定のメッシュ アクセス ポイントのネイバー統計情報を表示するには、目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Neighbor Information] を選択します。 選択されたメッシュ アクセス ポイントの [All APs > *Access Point Name* > Neighbor Info] ページが表示されます。

図 *93*：*[All APs > Access Point Name > Neighbor Info]* ページ

このページには、メッシュ アクセス ポイントの親、子、およびネイバーが表示されます。 また、各メッシュ アクセス ポイントの名前と無線 MAC アドレスが表示されます。

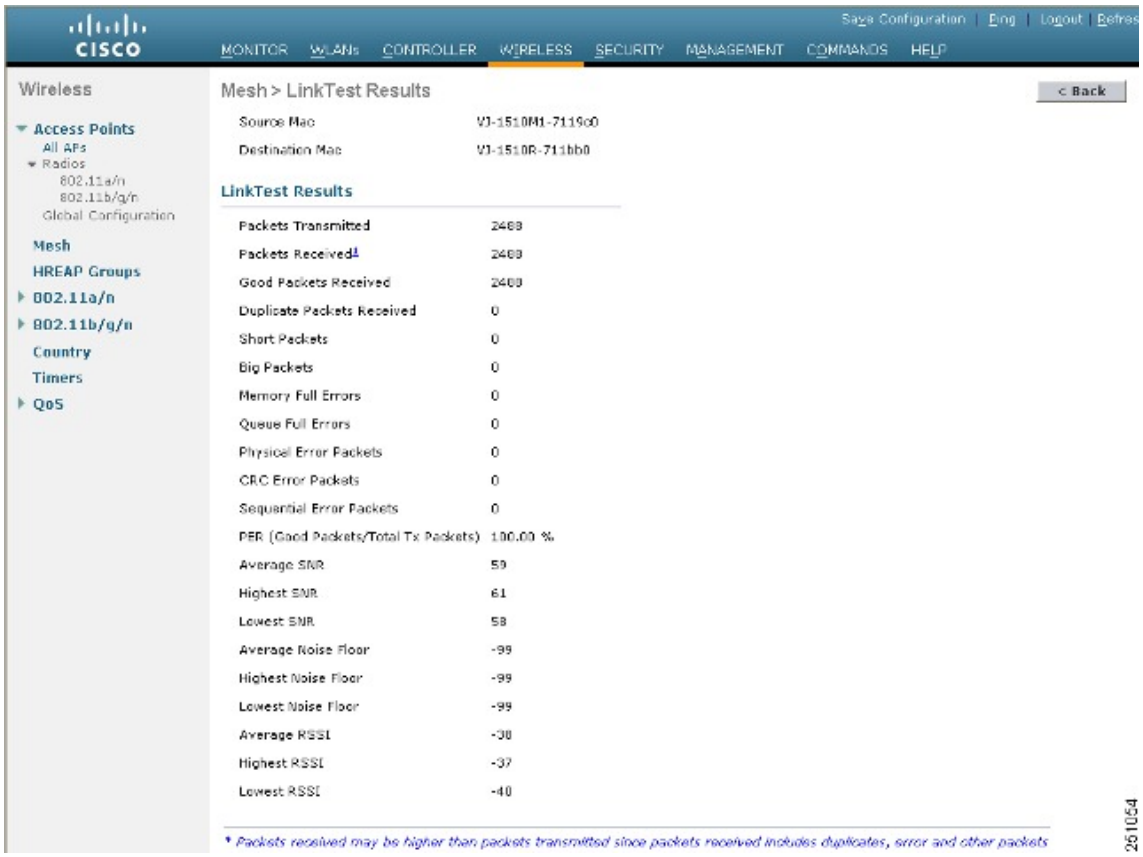
ステップ 3 メッシュアクセスポイントとその親または子とのリンクテストを実行するには、以下の手順に従います。

a) 親または目的の子の青のドロップダウン矢印の上にカーソルを移動し、[LinkTest] を選択します。 ポップアップ ウィンドウが表示されます。

図 *94*：*Link Test* ページ

b) [Submit] をクリックしてリンク テストを開始します。 リンク テストの結果が [Mesh > LinkTest Results] ページに表示されます。

図 *95*：*[Mesh > LinkTest Results]* ページ



c) [Back] をクリックして、[All APs > *Access Point Name* > Neighbor Info] ページに戻ります。

ステップ 4 このページで任意のメッシュ アクセス ポイントの詳細を表示するには、次の手順を実行します。

a) 目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Details] を選択します。 [All APs > *Access Point Name* > Link Details > Neighbor Name] ページが表示されます。

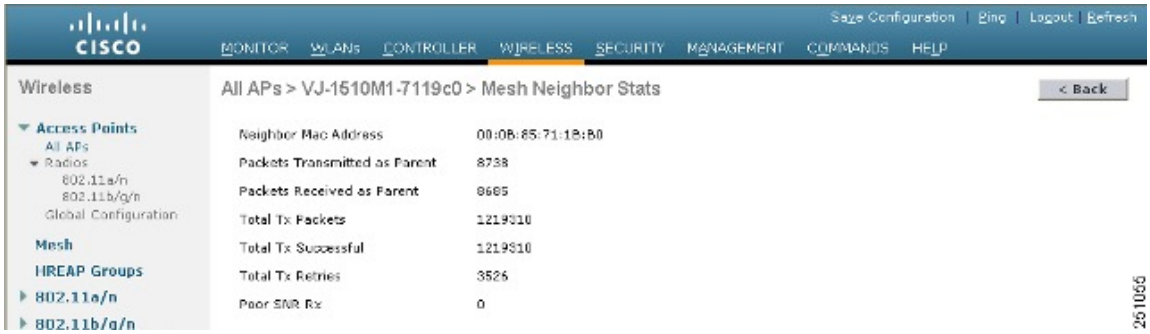
図 *96*：*[All APs > Access Point Name > Link Details > Neighbor Name]* ページ

b) [Back] をクリックして、[All APs > *Access Point Name* > Neighbor Info] ページに戻ります。

ステップ 5 このページで任意のメッシュ アクセス ポイントの統計情報を表示するには、次の手順を実行します。

a) 目的のメッシュ アクセス ポイントの青のドロップダウン矢印の上にカーソルを移動し、[Stats] を選択します。 [All APs > *Access Point Name* > Mesh Neighbor Stats] ページが表示されます。

図 *97*：*[All APs > Access Point Name > Mesh Neighbor Stats]* ページ



b) [Back] をクリックして、[All APs > *Access Point Name* > Neighbor Info] ページに戻ります。

メッシュ アクセス ポイントのネイバー統計情報の表示（CLI）

コントローラ CLI を使用して、特定のメッシュ アクセスポイントのネイバー統計情報を表示するには、次のコマンドを実行します。

- 特定のメッシュ アクセス ポイントのメッシュ ネイバーを表示するには、次のコマンドを入力します。

show mesh neigh {**detail** | **summary**} *AP_Name*

概要の表示を指定すると、次のような情報が表示されます。

```
AP Name/Radio Mac   Channel Snr-Up Snr-Down Link-Snr Flags  State
-----------------   ------- ------ -------- -------- ------  -------
mesh-45-rap1        165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
00:0B:85:80:ED:D0   149      5      6        5       0x1a60  NEED UPDATE BEACON DEFAULT
00:17:94:FE:C3:5F   149    7      0        0      0x860      BEACON
```

- メッシュ アクセス ポイントとそのネイバーとのリンクのチャネルおよび Signal to Noise Ratio（SNR）を表示するには、次のコマンドを入力します。

  show mesh path *AP_Name*

  以下に類似した情報が表示されます。

```
AP Name/Radio Mac  Channel Snr-Up Snr-Down Link-Snr Flags  State
-----------------  ------- ------ -------- -------- ------  -------
mesh-45-rap1       165     15     18       16       0x86b  UPDATED NEIGH PARENT BEACON
mesh-45-rap1 is a Root AP.
```

- ネイバー メッシュ アクセス ポイントによって伝送されるパケットのパケット エラーの割合を表示するには、次のコマンドを入力します。

  show mesh per-stats *AP_Name*

  以下に類似した情報が表示されます。

```
Neighbor MAC Address 00:0B:85:5F:FA:F0
Total Packets transmitted: 104833
Total Packets transmitted successfully: 104833
Total Packets retried for transmission: 33028

Neighbor MAC Address 00:0B:85:80:ED:D0
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0

Neighbor MAC Address 00:17:94:FE:C3:5F
Total Packets transmitted: 0
Total Packets transmitted successfully: 0
Total Packets retried for transmission: 0
```

パケット エラー レートの割合 = 1 –（伝送に成功したパケット数/伝送したパケットの総数）

屋内アクセス ポイントのメッシュ アクセス ポイントへの変換

ステップ 1 Autonomous アクセス ポイント（k9w7 イメージ）を Lightweight アクセス ポイントに変換します。このプロセスの詳細については、http://cisco-images.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html を参照してください。

ステップ 2 次のように、Lightweight アクセス ポイントをメッシュ アクセス ポイント（MAP）またはルート アクセス ポイント（RAP）のいずれかに変換します。

（注） 屋内メッシュ アクセス ポイント（1130 および 1240）は RAP または MAP のいずれかとして機能できます。 デフォルトではすべて MAP として設定されます。

コントローラの CLI を使用してアクセス ポイントをメッシュ アクセス ポイントに変換するには、次のいずれかの手順を実行します。

Lightweight アクセス ポイントを MAP に変換するには、次のコマンドを入力します。

config ap mode bridge *Cisco_AP*

メッシュ アクセス ポイントはリロードされます。

Lightweight アクセス ポイントを RAP に変換するには、次の CLI コマンドを入力します。

config ap mode bridge *Cisco_AP*

config ap role rootAP *Cisco_AP*

メッシュ アクセス ポイントはリロードされ、RAP として動作するように設定されます。

- GUI を使用してアクセス ポイントをメッシュ アクセス ポイントに変換するには、次の手順を実行します。

1. [Wireless] を選択し、変換する 1130 または 1240 屋内アクセス ポイントの [AP Name] のリンクをクリックします。
2. [General Properties] パネルの [AP Mode] ドロップダウン リストから [Bridge] を選択します。

   アクセス ポイントがリブートされます。
3. [Mesh] パネルの [AP Role] ドロップダウン リストから [RootAP] または [MeshAP] のいずれかを選択します。
4. [Apply] をクリックして、変更を確定します。
5. [Save Configuration] をクリックして、変更を保存します。

屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更

Cisco 1130 および 1240 シリーズ屋内メッシュ アクセス ポイントは RAP または MAP のいずれかとして機能できます。

屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更（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 変更する 1130 または 1240 シリーズ アクセス ポイントの名前をクリックします。

ステップ 3 [Mesh] タブをクリックします。

ステップ 4 [AP Role] ドロップダウン リストから [MeshAP] または [RootAP] を選択し、アクセス ポイントをそれぞれ MAP または RAP として指定します。

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されます。

ステップ 6 [Save Configuration] をクリックして、変更を保存します。

（注） MAP を RAP に変更する場合は、MAP とコントローラ間でファスト イーサネット接続を使用することをお勧めします。

（注） RAP から MAP への変換の後、コントローラへの MAP の接続は、ファスト イーサネット接続ではなく、ワイヤレス バックホール経由になります。 MAP が無線で join できるよう、MAP が起動される前に、変更される RAP のファスト イーサネット接続が解除されていることを確認する必要があります。

（注） MAP の電源を電源装置またはパワー インジェクタのいずれかで提供することをお勧めします。MAP の電源として PoE を使用することをお勧めしません。

屋内メッシュ アクセス ポイントの MAP および RAP ロールの変更（CLI）

ステップ 1 屋内アクセス ポイントのロールを MAP から RAP、または RAP から MAP に変更するには、次のコマンドを入力します。

config ap role {**rootAP** | **meshAP**} *Cisco_AP*

ロールの変更後に、アクセス ポイントはリブートされます。

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

屋内メッシュアクセスポイントの非メッシュLightweightアクセス ポイントへの変換（1130AG、1240AG）

コントローラの CLI で変換コマンドを入力した後、または Cisco WCS のコントローラで該当する手順を実行した後に、アクセス ポイントはリブートされます。

（注） メッシュ（ブリッジ）から非メッシュ（ローカル）アクセス ポイントに変換する場合は、コントローラに対してファスト イーサネット接続を使用することをお勧めします。 バックホールが無線である場合、変換後にイーサネットを有効にして、アクセス イメージをリロードする必要があります。

（注） ルート アクセス ポイントを Lightweight アクセス ポイントに変換すると、すべての従属メッシュ アクセス ポイントでコントローラに対する接続が失われます。 メッシュ アクセス ポイントは、隣接する別のルート アクセス ポイントに接続できるまでクライアントを処理できません。 同様に、ネットワークに対する接続を維持するため、クライアントは隣接する別のメッシュ アクセス ポイントに接続されることがあります。

- コントローラの CLI を使用して屋内メッシュ アクセス ポイント（MAP または RAP）を非メッシュ Lightweight アクセス ポイントに変換するには、次のコマンドを入力します。

  config ap mode local *Cisco_AP*

  アクセス ポイントはリロードされます。

- GUI を使用して屋内メッシュ アクセス ポイント（MAP または RAP）を非メッシュ Lightweight アクセス ポイントに変換するには、次の手順を実行します。

  1. [Wireless] を選択し、変換する 1130 または 1240 屋内アクセス ポイントの [AP Name] のリンクをクリックします。
  2. [General Properties] パネルの [AP Mode] ドロップダウン リストから [Local] を選択します。
  3. [Apply] をクリックして、変更を適用します。
  4. [Save Configuration] をクリックして、変更を保存します。

- Cisco WCS を使用して屋内メッシュ アクセス ポイント（MAP または RAP）を非メッシュ Lightweight アクセス ポイントに変換するには、次の手順を実行します。

  1. [Configure] > [Access Points] の順に選択し、変換する 1130 または 1240 屋内アクセス ポイントの [AP Name] のリンクをクリックします。
  2. [General Properties] パネルで、AP モードとして [Local] を選択します（左側）。
  3. [Save] をクリックします。

Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定

屋外アクセス ポイント（1522、1524PS）は、2.4 GHz アクセスおよび 5 GHz バックホールだけでなく、Public Safety 用のチャネル（4.9 GHz）で Cisco 3200 シリーズ モバイル アクセス ルータ（MAR）と相互運用することができます。

Cisco 3200 は車載ネットワークを作成します。車載ネットワークでは、PC、監視カメラ、デジタル ビデオカメラ、プリンタ、PDA、スキャナなどの装置が、メインのインフラストラクチャへと接続されている携帯電話ベースまたは WLAN ベースのサービスなどのワイヤレス ネットワークを共有できます。これにより、警察車両などの車載展開から収集されたデータをワイヤレス インフラストラクチャ全体に統合できます。1130、1240、および 1520 シリーズ メッシュ アクセス ポイントと 3200 シリーズ モバイル アクセス ルータ間の具体的な相互運用性の詳細については、次の表を参照してください。

表 *40*：メッシュ アクセス ポイントおよび *MAR 3200* の相互運用性

メッシュ アクセス ポイントのモデル	MAR のモデル
1522[15]	c3201[16]、c3202[17]、c3205[18]
1524PS	c3201、c3202
1130、1240（ユニバーサル アクセスが有効な屋内メッシュ アクセス ポイントとして設定）	c3201、c3205

15 802.11a 無線または 4.9 GHz 帯域で MAR に接続する場合、1522 でユニバーサル アクセスを有効にする必要があります。
16 モデル c3201 は、802.11b/g 無線（2.4 GHz）を搭載した MAR です。
17 モデル c3202 は、4.9 GHz サブ帯域無線を搭載した MAR です。
18 モデル c3205 は、802.11a 無線（5.8GHz サブ帯域）を搭載した MAR です。

注意事項および制約事項

- バックホールでクライアント アクセスを有効にする必要があります（メッシュ グローバル パラメータ）。
- メッシュ ネットワーク内のすべてのメッシュ アクセス ポイント（MAP）でグローバルに Public Safety への対応を有効にする必要があります。
- 1522 または 1524PS のチャネル番号の割り当ては、Cisco 3200 の無線インターフェイスの番号の割り当てと一致する必要があります。

- チャネル 20（4950 GHz）～ 26（4980 GHz）およびサブ帯域チャネル 1 ～ 19（5 および 10 MHz）は MAR の相互運用に使用します。 この設定の変更はコントローラで行います。 アクセス ポイントの設定は変更されません。
- チャネル割り当ては RAP のみに対して行います。 MAP へのアップデートは、RAP によって伝搬されます。

MAR 3200 のデフォルトのチャネル幅は、5 MHz です。 次のいずれかを実行する必要があります。

- チャネル幅を 10 または 20 MHz に変更し、WGB が 1520 シリーズ メッシュ アクセス ポイントとアソシエートできるようにします。
- 次のように、1522 または 1524PS のチャネルを 5 MHz（チャネル 1 ～ 10）または 10 MHz 帯域（チャネル 11 ～ 19）のチャネルに変更します。
  - コントローラの CLI を使用する場合は、チャネルを設定する前に、802.11a 無線を無効にする必要があります。 チャネルの設定後、無線を再度有効にします。
  - GUI を使用する場合は、チャネルの設定時に 802.11a 無線を有効および無効にする必要はありません。
  - Cisco MAR 3200 は 5、10、または 20 MHz 帯域内でチャネルをスキャンできますが、複数の帯域にわたってスキャンすることはできません。

Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定（GUI）

ステップ 1 クライアント アクセスのバックホールを有効にするには、[Wireless] > [Mesh] の順にクリックして、[Mesh] ページを開きます。

ステップ 2 [Backhaul Client Access] チェックボックスをオンにして、802.11a 無線でのワイヤレス クライアント アソシエーションを許可します。

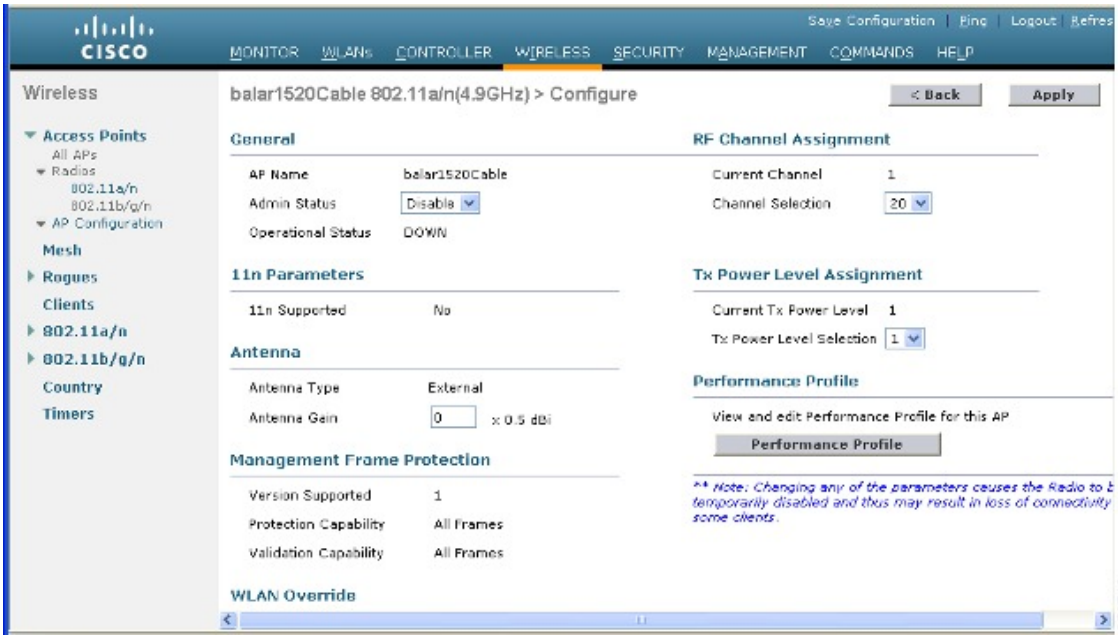
ステップ 3 [Apply] をクリックして、変更を確定します。

ステップ 4 ネットワーク上のすべてのメッシュ アクセス ポイントをリブートするよう求められた場合は、[OK] をクリックします。

ステップ 5 [Wireless] > [Access Points] > [Radios] > [802.11a/n] の順に選択して、[802.11a/n Radios] ページを開きます。

ステップ 6 カーソルを適切な RAP 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 (4.9 GHz) > Configure] ページが表示されます。

図 *98*：*[802.11 a/n (4.9GHz) > Configure]* ページ



ステップ 7 [RF Channel Assignment] セクションの [Assignment Method] で [WLC Controlled] オプションを選択し、1 ～ 26 の間から任意のチャネルを選択します。

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。

Cisco 3200 シリーズ モバイル アクセス ルータと一緒に動作するメッシュ アクセス ポイントの設定（CLI）

ステップ 1 1522 および 1524PS メッシュ アクセス ポイントでクライアント アクセス モードを有効にするには、次のコマンドを入力します。
config mesh client-access enable

ステップ 2 Public Safety をグローバルで有効にするには、次のコマンドを入力します。
config mesh public-safety enable *all*

ステップ 3 Public Safety チャネルを有効にするには、次のコマンドを入力します。

- 1522 アクセス ポイントの場合、次のコマンドを入力します。

  config 802.11a disable *Cisco_MAP*

  config 802.11a channel ap *Cisco_MAP channel_number*

  config 802.11a enable *Cisco_MAP*

- 1524PS の場合、次のコマンドを入力します。

  config 802.11–a49 disable *Cisco_MAP*

  config 802.11–a49 channel ap *Cisco_MAP channel_number*

  config 802.11–a49 enable *Cisco_MAP*

（注） 5 GHz 無線を有効にするには、**config 802.11–a58 enable** *Cisco_MAP* コマンドを入力します。

（注） 1522 および 1524PS メッシュ アクセス ポイントの両方で、有効なチャネル番号の値は 1 ～ 26 です。

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 設定を検証するには、次のコマンドを入力します。
show mesh public-safety

show mesh client-access

show ap config 802.11a summary（1522 アクセス ポイントの場合）

show ap config 802.11–a49 summary（1524PS アクセス ポイントの場合）

（注） 5 GHz 無線の設定の詳細を表示するには、**show config 802.11-a58 summary** と入力します。

第 10 章

コントローラ ソフトウェアと設定の管理

この章では、コントローラにおける設定とソフトウェア バージョンの管理方法について説明します。

- コントローラ ソフトウェアのアップグレード，745 ページ
- コントローラとのファイルのやり取り，764 ページ
- 設定の保存，782 ページ
- 設定ファイルの編集，783 ページ
- コントローラの設定のクリア，784 ページ
- コントローラ設定の消去，784 ページ
- コントローラのリセット，785 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、コントローラのアソシエート アクセス ポイント上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。 一方、ソフトウェア リリース 4.0.206.0 以降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対象数の増加により、アップグレードに要する時間は顕著に削減されているはずです。 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。

（注） 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 GUI および CLI の両方から WLAN オーバーライド機能が削除されました。 コントローラが WLAN オーバーライド用に設定され、コントローラ ソフトウェア リリース 5.2 以降にアップグレードする場合、コントローラにより WLAN 設定が削除され、すべての WLAN がブロードキャストされます。 アクセス ポイント グループを設定して、特定の WLAN のみを送信するように指定できます。 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。

コントローラ ソフトウェアのアップグレードに関するガイドライン

- 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_rn_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 メニューは次のようになっています。

```
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 メニューは次のようになっています。

```
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**}

  それぞれの説明は次のとおりです。

  - **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
  - 証明書に関係する機能の有効化（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。
- コントローラ ソフトウェアでは、リカバリ イメージを削除して十分なスペースを作ることで、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るようにしてます。この機能は、8MB のフラッシュを備えたアクセス ポイントにのみ影響を及ぼします（1100、1200、および 1310 シリーズ アクセス ポイント）。 すべての比較的新しいアクセス ポイントには、8MB を超える大型フラッシュが搭載されています。

（注） 2007 年 8 月現在で、サイズの大きなアクセス ポイントのイメージはありませんでしたが、新機能が追加され、アクセス ポイントのイメージ サイズはこれからも拡大し続けます。

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）にアクセスします。
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）コントローラの 802.11a/n ネットワークおよび 802.11b/g/n 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 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 リストから、[TFTP] または [FTP] を選択します。

ステップ 9 [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 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。

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 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 コントローラがリブートしたら、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* で 802.11a/n ネットワークおよび 802.11b/g/n ネットワークを無効に場合は、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。

a) Cisco Software Center（http://www.cisco.com/cisco/software/navigator.html）にアクセスします。

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）コントローラの 802.11a/n ネットワークおよび 802.11b/g/n 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 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。
以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Code
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ <directory path>
TFTP Filename............................ xxx.aes

This may take some time.
Are you sure you want to start? (y/N) n
Transfer Canceled
```

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}**
- **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。
以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Code
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ <directory path>
TFTP Filename............................ xxx.aes

Are you sure you want to start? (y/n) y
TFTP Code transfer starting.
TFTP receive complete... extracting components.
Writing new bootloader to flash.
Making backup copy of RTOS.
Writing new RTOS to flash.
Making backup copy of Code.
Writing new Code to flash.
TFTP File transfer operation completed successfully.
  Please restart the switch (reset system) for update to complete.
```

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 802.11a/n ネットワークおよび 802.11b/g/n ネットワークを無効に場合は、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 ポイントのリブ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

アクセスのポイント 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。
  - ダウンロードされたイメージは、コントローラのバックアップ イメージになります。 **config boot backup** コマンドを使用して、現在のブート イメージをバックアップ イメージに変更します。 これにより、システム障害が発生した場合、コントローラは最後に動作していたコントローラのイメージを使用して起動します。
  - ユーザは、**config ap image predownload primary all** コマンドを使用して、アップグレードされたイメージをプレダウンロードします。 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。 これは、**show ap image all** コマンドを使用して確認できます。

- ユーザは **config boot primary** コマンドを使用してブート イメージを手動でプライマリに変更し、コントローラをリブートしてアップグレード イメージをアクティブにします。

  または

- ユーザは **swap** キーワードを使用して、スケジュールされたリブートを発行します。 ここで **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。

- コントローラをリブートすると、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 request 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 join request で応答し、コントローラが実行しているイメージ バージョンを返します。
  - 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、コントローラをリロードした後でコントローラに join します。

注意事項および制約事項

- 同時にプレダウン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。

  プレダウン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、再度プレダウンロードが試行されます。

- プレダウンロードのコマンドを入力する前に、アクティブなコントローラのブート 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。 この手順を実行することで、コント

ローラが何らかの理由でリブートされた場合、アップグレード イメージが部分的にダウンロードされるのではなく、以前の実行イメージで確実にバックアップされます。

- 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、プレダウンロード 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ンロード 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は有効ではなくなり、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す。 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、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.
```

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。

a) Cisco Software Center（http://www.cisco.com/cisco/software/navigator.html）にアクセスします。
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 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）コントローラの 802.11a/n ネットワークおよび 802.11b/g/n 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 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 リストから、[TFTP] または [FTP] を選択します。

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 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] をクリックして確定します。

ステップ 19 [Apply] をクリックして、変更を確定します。

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。

a) Cisco Software Center（http://www.cisco.com/cisco/software/navigator.html）にアクセスします。

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 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）コントローラの 802.11a/n ネットワークおよび 802.11b/g/n 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 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 リストから、[TFTP] または [FTP] を選択します。

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] をクリックして確定します。

ステップ 20 [Apply] をクリックして、変更を確定します。

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）にアクセスします。

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）コントローラの 802.11a/n ネットワークおよび 802.11b/g/n 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示されま

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 ポイントのリブ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ブートをスケジュールします。

- 次のコマンドを入力して、デバイスをリブ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、デバイスがリブ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ブ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

コントローラ ソフトウェア リリース 6.0 以降では、GUI または CLI のいずれかを使用して、ログイン バナー ファイルをダウンロードできます。 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。
- サードパーティの TFTP または FTP サーバと WCS 内蔵 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 WCS 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。 コントローラの GUI または CLI を使用してログイン バナーをクリアする方法については、ログイン バナーのクリア（GUI）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 TFTP または FTP サーバ上にあるデフォルトのディレクトリにログイン バナー ファイルをコピーします。

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、[Login Banner] を選択します。

ステップ 4 [Transfer Mode] ドロップダウン リストから、[TFTP] または [FTP] を選択します。

ステップ 5 [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 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。

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、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}

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 と答えます。
以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Login Banner
TFTP Server IP........................... 10.10.10.10
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /
TFTP Filename............................ banner.txt

This may take some time.
Are you sure you want to start? (y/N) y

TFTP Login Banner transfer starting.

TFTP receive complete... checking login banner.

Successfully installed new login banner file
```

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。
- サードパーティの TFTP または FTP サーバと WCS 内蔵 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 WCS 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 デバイスの証明書を TFTP または FTP 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、[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 リストから、[TFTP] または [FTP] を選択します。

ステップ 6 [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 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**}

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。
以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Vendor Dev Cert
TFTP Server IP........................... 10.10.10.4
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /tftpboot/username/
TFTP Filename............................ filename.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 the new certificate.
```

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。
- サードパーティの TFTP または FTP サーバと WCS 内蔵 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 WCS 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 CA 証明書を TFTP または FTP 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] 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 リストから、[TFTP] または [FTP] を選択します。

ステップ 5 [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 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**}

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、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。
以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Vendor CA Cert
TFTP Server IP........................... 10.10.10.4
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path................................ /tftpboot/username/
TFTP Filename............................ filename.pem
This may take some time.
Are you sure you want to start? (y/N) y

TFTP EAP CA cert transfer starting.

Certificate installed.
Reboot the switch to use the new certificate.
```

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、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。
- サードパーティの TFTP または FTP サーバと WCS 内蔵 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 WCS 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 [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}

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。
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................................... /tftpboot/username/
TFTP Filename..................................... manual.pac
Data Type...................................... PAC
PAC User....................................... username
PAC Validity................................... 10 days
PAC Password................................... password

Are you sure you want to start? (y/N) y

PAC transfer starting.

File transfer operation completed successfully.
```

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 リストから、[TFTP] または [FTP] を選択します。

ステップ 5 [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 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、設定ファイルを TFTP または FTP 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}

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、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 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 リストから、[TFTP] または [FTP] を選択します。

ステップ 5 [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 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**}

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 または FTP 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 または FTP 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ブートされます。 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 11 章

ユーザ アカウントの管理

この章で説明する内容は、次のとおりです。

- ゲスト アカウントの作成について，787 ページ
- 注意事項および制約事項，788 ページ
- Lobby Ambassador アカウントの作成，788 ページ
- ゲスト ユーザ アカウントの表示，791 ページ
- Web 認証証明書の入手，792 ページ
- Web 認証プロセス，794 ページ
- デフォルトの Web 認証ログイン ページの選択，796 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，804 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 ページの選択，804 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，806 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，810 ページ
- 有線ゲスト アクセスの設定，813 ページ
- 有線ゲスト アクセスの設定，816 ページ
- IPv6 クライアントのゲスト アクセスのサポート，823 ページ

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。

注意事項および制約事項

ローカルユーザ データベースは、最大エントリ数が 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 エントリ、除外リスト エントリ、およびアクセス ポイントの認可リスト エントリで共有します。 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、oscic、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は使用しないでください。

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す。

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になります。

（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

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。

Web 認証証明書の入手

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。

a) [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。

b) 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。

a) 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。

b) [Download SSL Certificate] チェックボックスをオンにします。

c) [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。

d) 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。

e) [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。

f) [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）。

g) [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。

h) [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。

i) 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。

a) 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。

注意事項および制約事項

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 *99*：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。

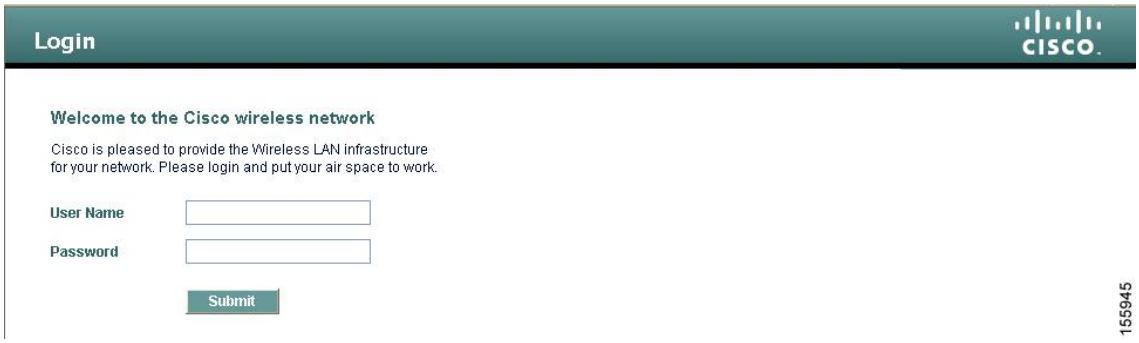
ユーザが [Yes] をクリックして続行した後（または、クライアントのブラウザにセキュリティ警告が表示されない場合）、Web 認証システムのログイン ページが表示されます。

セキュリティ警告が表示されないようにするには、次の手順を実行します。

1. [Security Alert] ページで [View Certificate] をクリックします。
2. [Install Certificate] をクリックします。
3. [Certificate Import Wizard] が表示されたら、[New] をクリックします。
4. [Place all certificates in the following store] を選択して、[Browse] をクリックします。
5. [Select Certificate Store] ページの下部で、[Show Physical Stores] チェックボックスをオンにします。
6. [Trusted Root Certification Authorities] フォルダを展開して、[Local Computer] を選択します。
7. [OK] をクリックします。
8. [Next] > [Finish] の順にクリックします。
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。
   a. 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。
10. PC をリブートします。 次回 Web 認証を試みるときには、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 *100* : デフォルトの *Web* 認証ログイン ページ



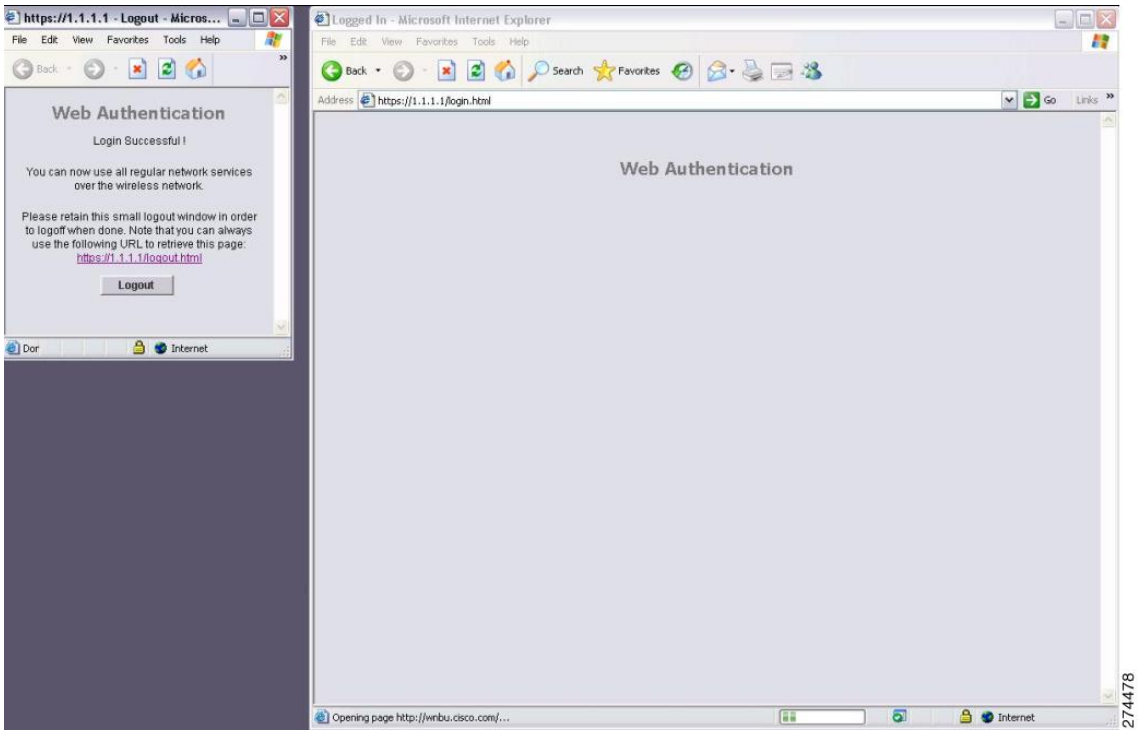
デフォルトのログイン ページには、Cisco ロゴや Cisco 特有のテキストが表示されます。 Web 認証システムが次のいずれかを表示するように選択できます。

- 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 *101*：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、仮想ゲートウェイ アドレスの URL（https://1.1.1.1/logout.html）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）。

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。

注意事項および制約事項

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の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 [disabled] です。

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ド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。 デフォルトのヘッドラインは、「Welcome to the Cisco wireless network」です。ヘッド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 サーバと WCS 内蔵 TFTP 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 サーバは Cisco WCS と同じコンピュータ上で実行できません。

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

以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Login Image
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename............................ <filename.jpg|.gif|.png>
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```

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），（809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
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");
      }
      else if(args.statusCode == 2){
       alert("You are not configured to authenticate against web portal. No further action
 is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the username is
 already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }
      else if(args.statusCode == 6){
        alert("Invalid email address format. Please try again.");
      }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25"
MAXLENGTH="63" VALUE="">
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password" name="password"
 SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
```

```
</html>
```

ユーザのインターネットブラウザがカスタマイズされたログインページにリダイレクトされるときに、次のパラメータが URL に追加されます。

- **ap_mac**：無線ユーザ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。
- **switch_url**：ユーザの資格情報を記録するコントローラの URL。
- **redirect**：認証に成功した後、ユーザがリダイレクトされる URL。
- **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。

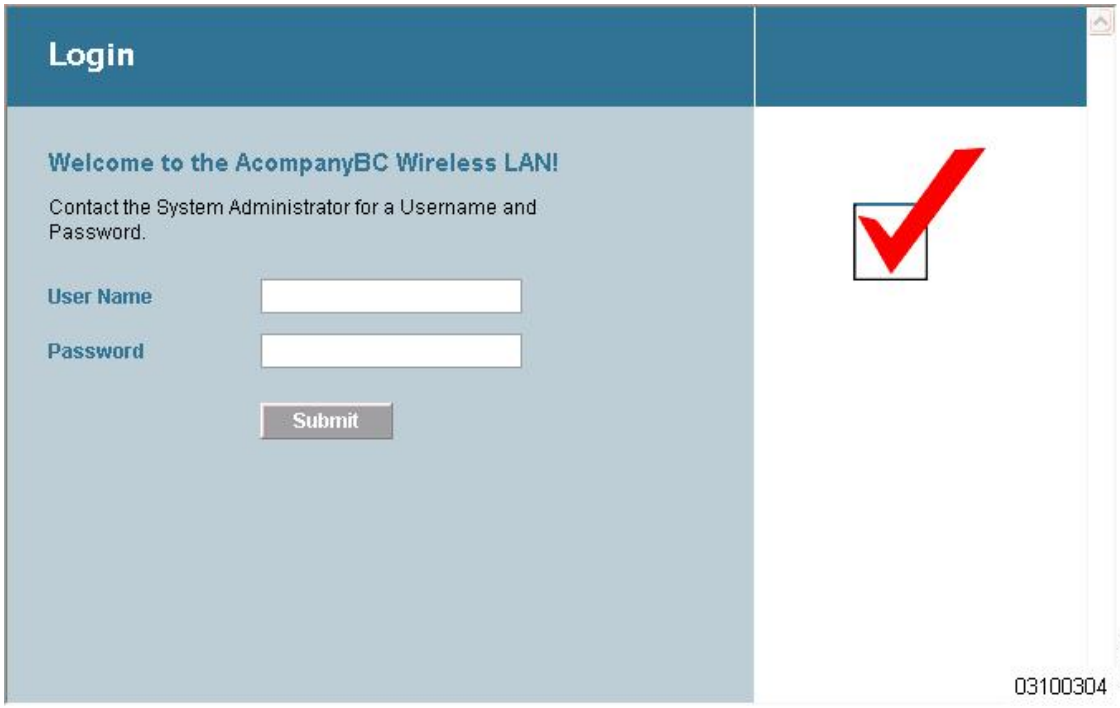
- ステータス コード 1：「You are already logged in. No further action is required on your part.」
- ステータス コード 2：「You are not configured to authenticate against web portal. No further action is required on your part.」
- ステータス コード 3：「The username specified cannot be used at this time. Perhaps the username is already 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

次の図は、変更されたデフォルトの Web 認証ログイン ページの例を示しています。

図 *102*：変更されたデフォルトの *Web* 認証ログイン ページの例



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*

  以下に類似した情報が表示されます。

```
Mode..................................... TFTP
Data Type................................ Login Image
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ /
TFTP Filename............................ Logo.gif
This may take some time.
Are you sure you want to start? (y/n) y
TFTP Image transfer starting.
Image installed.
```

- **config custom-web redirecturl** *url*

show custom-web

```
Cisco Logo.................. Disabled
CustomLogo.................. 00_logo.gif
Custom Title................ Welcome to the AcompanyBC Wireless LAN!
Custom Message ............. Contact the System Administrator for a Username and
Password.
Custom Redirect URL......... http://www.AcompanyBC.com
Web Authentication Mode..... Disabled
Web Authentication URL........ Disabled
```

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。

注意事項および制約事項

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

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），（809 ページ）の項の指示に従って、設定を確認します。

その他の関連資料

ACL の詳細については、セキュリティ ソリューションの設定，（227 ページ）を参照してください。

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

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 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。

（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。

注意事項および制約事項

- 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。

その他の関連資料

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。

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 ファイルのダウンロードで TFTP サーバを使用できることを確認します。

ステップ2 ログイン ページが含まれる .tar ファイルを TFTP 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3 [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4 [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5 [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6 [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8 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9 [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10 [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11 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 12 [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 13 [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 14 [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 15 [Apply] をクリックして、変更を確定します。
ステップ 16 [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 17 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。

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 ファイルのダウンロードで TFTP サーバを使用できることを確認します。デフォルトの Web 認証ログイン ページの選択（CLI），（798 ページ）のステップ *8* にある TFTP サーバのセットアップのガイドラインを参照してください。
ステップ 2 ログイン ページが含まれる .tar ファイルを TFTP 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 3 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*
ステップ 4 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 5 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 6 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 7 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 8 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 9 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 10 **save config** コマンドを入力して、設定を保存します。

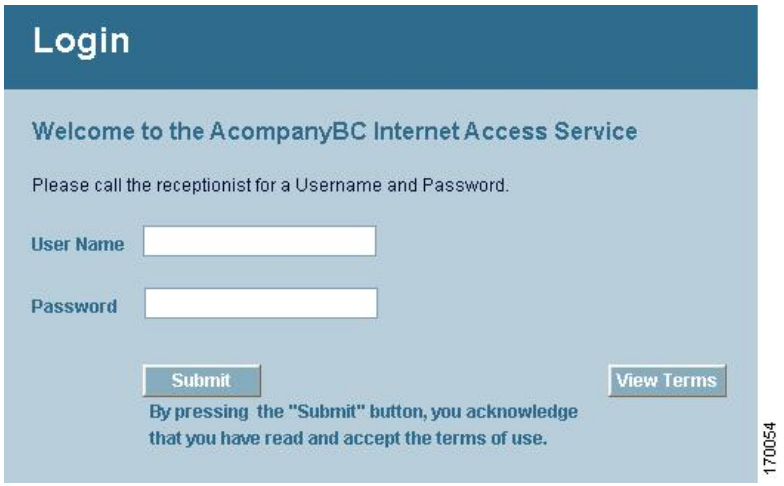
その他の関連資料

Web 認証プロセスを参照してください。

例：カスタマイズされた Web 認証ログイン ページ

次の図は、カスタマイズされた Web 認証ログイン ページの例を示しています。

図 *103*：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）

show custom-web 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を確認します。 この例は、設定がデフォルト値に設定された際に表示される情報を示しています。

```
Cisco Logo..................................... Enabled
CustomLogo..................................... Disabled
Custom Title................................... Disabled
Custom Message................................. Disabled
Custom Redirect URL............................ Disabled
Web Authentication Mode........................ Disabled
Web Authentication URL......................... Disabled
```

この例は、設定が変更された際に表示される情報を示しています。

```
Cisco Logo..................................... Disabled
CustomLogo..................................... 00_logo.gif
Custom Title................................... Welcome to the AcompanyBC Wireless LAN!
Custom Message................................. Contact the System Administrator for a
              Username and Password.
Custom Redirect URL.....................
Web Authentication Mode........................ Internal
Web Authentication URL.......................... Disabled
```

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。 768 ビットは、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。 768 ビットは、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

有線ゲスト アクセスの設定

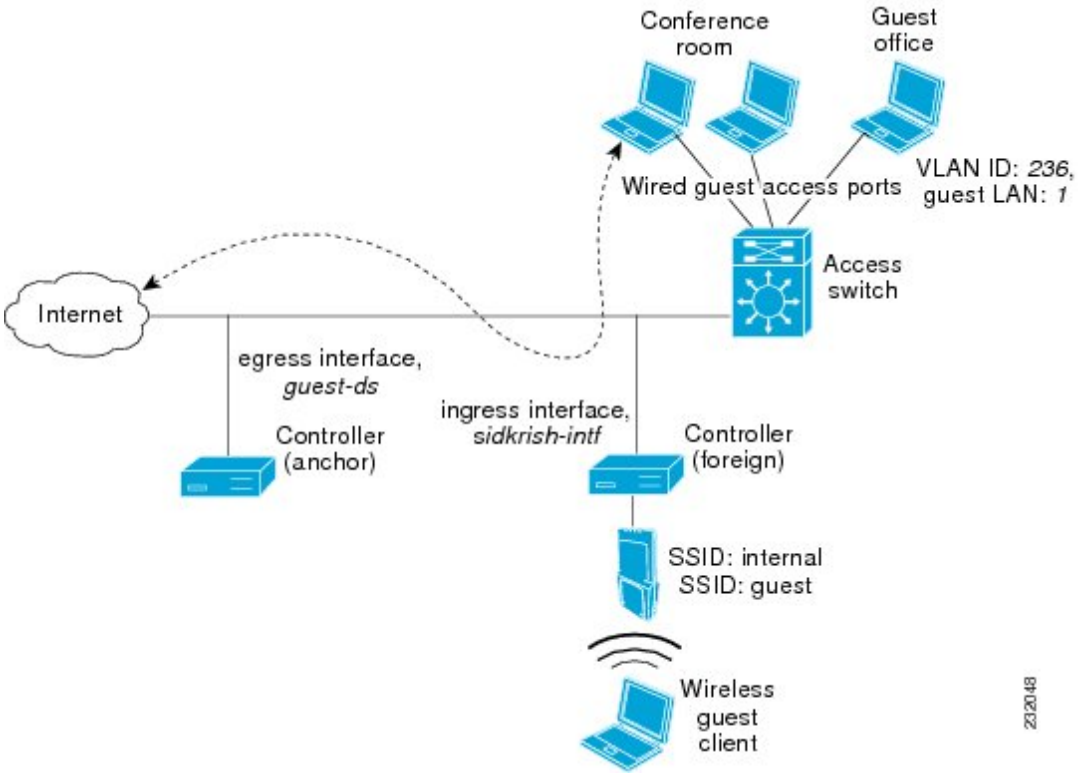
有線ゲスト アクセスについて

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。

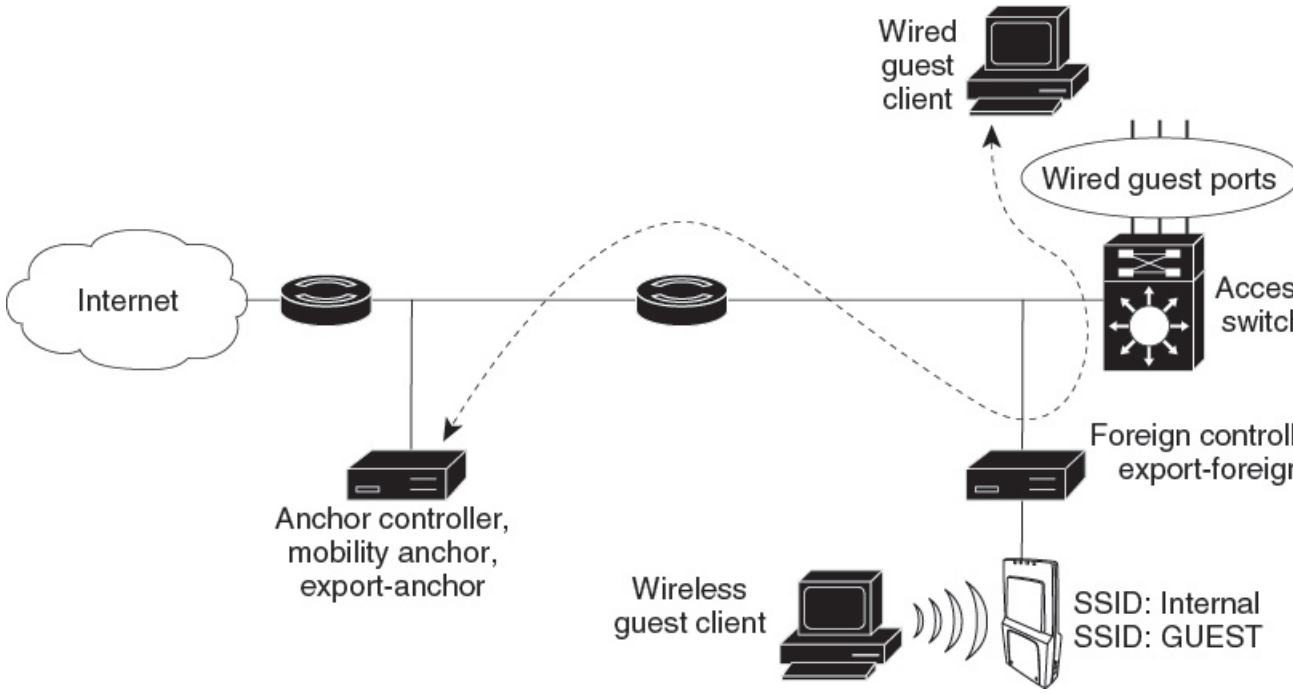
有線ゲスト アクセス ポートは最初、レイヤ 2 アクセス スイッチ上で、または有線ゲスト アクセス トラフィック用のVLANインターフェイスで設定されているスイッチ ポート上で終端します。有線ゲスト トラフィックはその後、アクセス スイッチからコントローラへトランクされます。このコントローラは、アクセス スイッチ上で有線ゲスト アクセス VLAN にマップされているインターフェイスを使用して設定されます。

図 *104* : *1* つのコントローラを使用した有線ゲスト アクセスの例



2 つのコントローラが使用されている場合、有線ゲスト トラフィックをアクセス スイッチから受信する外部コントローラは、アンカーコントローラへそのトラフィックを転送します。 このトラフィックを処理するために、外部コントローラとアンカー コントローラとの間で双方向 EoIP トンネルが確立されます。

図 *105*： *2* つのコントローラを使用した有線ゲスト アクセスの例



（注） 2つのコントローラが展開されるとき、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。

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。

注意事項および制約事項

- 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

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。 768 ビットは、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。 768 ビットは、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 番めの（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 none***guest_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 none***guest_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。 768 ビットは、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 認証ページの情報は、**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。

show custom-web all コマンドに対しては、次のような情報が表示されます。

```
Radius Authentication Method..................... PAP
Cisco Logo....................................... Enabled
CustomLogo....................................... None
Custom Title..................................... None
Custom Message................................... None
Custom Redirect URL.............................. None
Web Authentication Type..............            External
External Web Authentication URL............       http:\9.43.0.100\login.html

External Web Server list
Index IP Address
----- ---------------
1    9.43.0.100
2   0.0.0.0
3   0.0.0.0
4  0.0.0.0
5  0.0.0.0
...
20  0.0.0.0

Configuration Per Profile:

WLAN ID: 1
 WLAN Status..................................... Enabled
 Web Security Policy............................. Web Based Authentication
 Global Status................................... Disabled
 WebAuth Type.................................... Customized
 Login Page...................................... login1.html
 Loginfailure page name.......................... loginfailure1.html
 Logout page name................................ logout1.html

WLAN ID: 2
WLAN Status..................................... Enabled
 Web Security Policy............................. Web Based Authentication
```

```
 Global Status.............................. Disabled
 WebAuth Type............................... Internal
 Loginfailure page name..................... None
 Logout page name........................... None

WLAN ID: 3
WLAN Status................................ Enabled
 Web Security Policy........................ Web Based Authentication
 Global Status.............................. Disabled
 WebAuth Type............................... Customized
 Login Page................................. login.html
 Loginfailure page name..................... LF2.html
 Logout page name........................... LG2.html
```

show custom-web guest-lan *guest_lan_id* コマンドに対しては、次のような情報が表示されます。

```
Guest LAN ID: 1
Guest LAN Status........................... Disabled
Web Security Policy........................ Web Based Authentication
Global Status.............................. Enabled
WebAuth Type............................... Internal
Loginfailure page name..................... None
Logout page name........................... None
```

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

以下に類似した情報が表示されます。

```
Interface Name                  Port Vlan Id  IP Address      Type    Ap Mgr Guest
------------------------------- ---- -------- --------------- ------- ------ -----
ap-manager                      1    untagged 1.100.163.25    Static  Yes    No

management                      1    untagged 1.100.163.24    Static  No     No

service-port                    N/A  N/A      172.19.35.31    Static  No     No

virtual                         N/A  N/A      1.1.1.1         Static  No     No

wired                           1    20       10.20.20.8      Dynamic No     No

wired-guest                     1   236         10.20.236.50     Dynamic No       Yes
```

（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*

以下に類似した情報が表示されます。

```
Interface Name................................. wired-guest
MAC Address.................................... 00:1a:6d:dd:1e:40
IP Address..................................... 0.0.0.0
```

```
DHCP Option 82................................. Disabled
Virtual DNS Host Name.......................... Disabled
AP Manager..................................... No
Guest Interface................................ No
```

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*

以下に類似した情報が表示されます。

```
Guest LAN Identifier........................... 1
Profile Name................................... guestlan
Network Name (SSID)............................ guestlan
Status......................................... Enabled
AAA Policy Override............................ Disabled
Number of Active Clients....................... 1
Exclusionlist Timeout.......................... 60 seconds
Session Timeout................................ Infinity
Interface...................................... wired
Ingress Interface.............................. wired-guest
WLAN ACL....................................... unconfigured
DHCP Server.................................... 10.20.236.90
DHCP Address Assignment Required............... Disabled
Quality of Service............................. Silver (best effort)
Security
 Web Based Authentication...................... Enabled
 ACL........................................... Unconfigured
 Web-Passthrough............................... Disabled
 Conditional Web Redirect...................... Disabled
 Auto Anchor................................... Disabled
Mobility Anchor List
GLAN ID IP Address Status
------- --------------- ------
```

（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

以下に類似した情報が表示されます。

```
Number of Clients.............................. 1
MAC Address        AP Name Status         WLAN   Auth   Protocol    Port   Wired
------------------- ------- ----------- ----- ----- --------- ----- ------
00:16:36:40:ac:58     N/A     Associated     1        No     802.3     1   Yes
```

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*

以下に類似した情報が表示されます。

```
Client MAC Address............................. 00:40:96:b2:a3:44
```

```
Client Username ..............................  N/A
AP MAC Address................................  00:18:74:c7:c0:90
Client State..................................  Associated
Wireless LAN Id...............................  1
BSSID.........................................  00:18:74:c7:c0:9f
Channel.......................................  56
IP Address....................................  192.168.10.28
Association Id................................  1
Authentication Algorithm......................  Open System
Reason Code...................................  0
Status Code...................................  0
Session Timeout...............................  0
Client CCX version............................  5
Client E2E version............................  No E2E support
Diagnostics Capability........................  Supported
S69 Capability................................  Supported
Mirroring.....................................  Disabled
QoS Level.....................................  Silver
...
```

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 12 章

Radio Resource Management の設定

この章で説明する内容は、次のとおりです。

- Radio Resource Management について，825 ページ
- 注意事項および制約事項，830 ページ
- RRM の設定，830 ページ
- Off-Channel Scanning Defer の設定，834 ページ
- RRM ネイバー ディスカバリ パケットの設定，852 ページ
- RF グループの設定，853 ページ
- RRM の無効化，858 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，865 ページ
- CCX 無線管理機能の設定，867 ページ

Radio Resource Management について

Radio Resource Management（RRM）ソフトウェアはコントローラに組み込まれており、無線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、コントローラ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 Received Signal Strength Indicator（RSSI; 受信信号強度インジケータ）と Signal-to-Noise Ratio（SNR; 信号対雑音比）。

- 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コントローラや 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

コントローラは、リアルタイムの無線 LAN 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。

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 ポイントを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] テキスト ボックスを設定するには、[Tx Power Control] ページで RRM に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。

コントローラによる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ネルの使用を変更します。 たとえば、チャネル 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ネルを回避できます。すべての非オーバーラップ チャ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。
- 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ネルを割り当てることができます。

- 負荷：チャ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ディセーブルになっています。

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。

5.1 より前のコントローラ ソフトウェア リリース場合、DCA では 20 MHz チャネルを使用する無線だけがサポートされています。 コントローラ ソフトウェア リリース 5.1 以降のリリースの場合、DCA のサポートは、5 GHz 帯域の 802.11n 40 MHz チャネルに拡張されています。 40 MHz のチャネライゼーションでは、無線は瞬間的に高いデータ レート（場合によっては、20 MHz チャネルの 2.25 倍）を達成できます。 コントローラ ソフトウェア リリース 5.1 以降のリリースの場合、DCA を 20 MHz で動作させるか 40 MHz で動作させるか選択できます。

（注） 2.4GHz 帯域の 40 MHz チャネルを使用している無線は、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。

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 チャネル計画に収束するために 10 回の高感度な（チャ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。

（注） 送信電力制御およびDCAが複数のコントローラ環境（RFドメインに基づく）で動作できますが、カバレッジ ホールの検出はコントローラごとに実行されます。 コントローラ ソフトウェア リリース 5.2 以降のリリースの場合、カバレッジ ホールの検出は WLAN ごとに無効にできます。

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。

注意事項および制約事項

- 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、ワイヤレス LAN コントローラではなく、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。 コントローラからスペクトラム チャネルや電力を管理しようとしたり、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。

RRM の設定

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。

（注） 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。

（注） 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、コントローラのリブートの結果として、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、監視チャネル、および監視間隔です。

RF グループ モードの設定（GUI）

ステップ 1 [Wireless] > [802.11a/n] 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 ボックスから、このコントローラ用に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、このコントローラをグループ 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。 すべてのコントローラは自身のアクセス 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、他のコントローラのメンバになることはできません。

（注） 高い優先順位を持つコントローラが使用可能な場合は、より低い優先順位を持つコントローラは、グループ リーダーのロールを担うことはできません。 ここで優先順位は、コントローラの処理能力に関連しています。

（注） コントローラが自動 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 このコントローラに対して、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 [Controller Name] テキスト ボックスに、このグループにメンバとして追加するコントローラを入力します。

2 [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。

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す。

ステップ 5 [Apply] をクリックして変更内容を保存します。

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、このコントローラをグループ 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。 すべてのコントローラは自身のアクセス 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、他のコントローラのメンバになることはできません。

（注） 高い優先順位を持つコントローラが使用可能な場合は、より低い優先順位を持つコントローラは、グループ リーダーのロールを担うことはできません。 ここで優先順位は、コントローラ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（モードが「leader」に設定されている場合）のスタティック メンバとしてコントローラを追加または削除します。

- **config advanced {802.11a | 802.11b} group-member add** *controller_name controller_ip_address*
- **config advanced {802.11a | 802.11b}** *group-member* **remove** *controller_nam*e *controller_ip_address*

ステップ 3 RF グループ化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 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] または [802.11b/g/n] > [RRM] > [TPC] の順に選択して、[802.11a/n（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。
- [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、コントローラの動的電力割り当てモードを指定します。

- [Automatic]：コントローラによって、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、必要に応じて更新されます。 768 ビットは、デフォルト値です。
- [On Demand]：コントローラによって、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、必要に応じてコントローラ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、すぐに送信電力の評価と更新が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]：コントローラによって、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）場合は変更できます。
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 に下げるのが有用です。 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、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。

Off-Channel Scanning Defer の設定

Off-Channel Scanning Defer 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、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、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 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ネル選択に関する情報を収集する RRM を使用するときに重要となります。 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）の WLAN への割り当ては、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に影響します。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。

コントローラ GUI で 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、この機能を設定することもできます。

動的チャネル割り当ての設定（GUI）

コントローラ GUI を使用して RRM スキャンに使用されるチャネルを選択する際に、動的チャネル割り当て（DCA）アルゴリズムで考慮されるチャネルを、指定するには、次の手順を実行します。

（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 1 802.11a または 802.11b/g ネットワークを次のように無効にします。

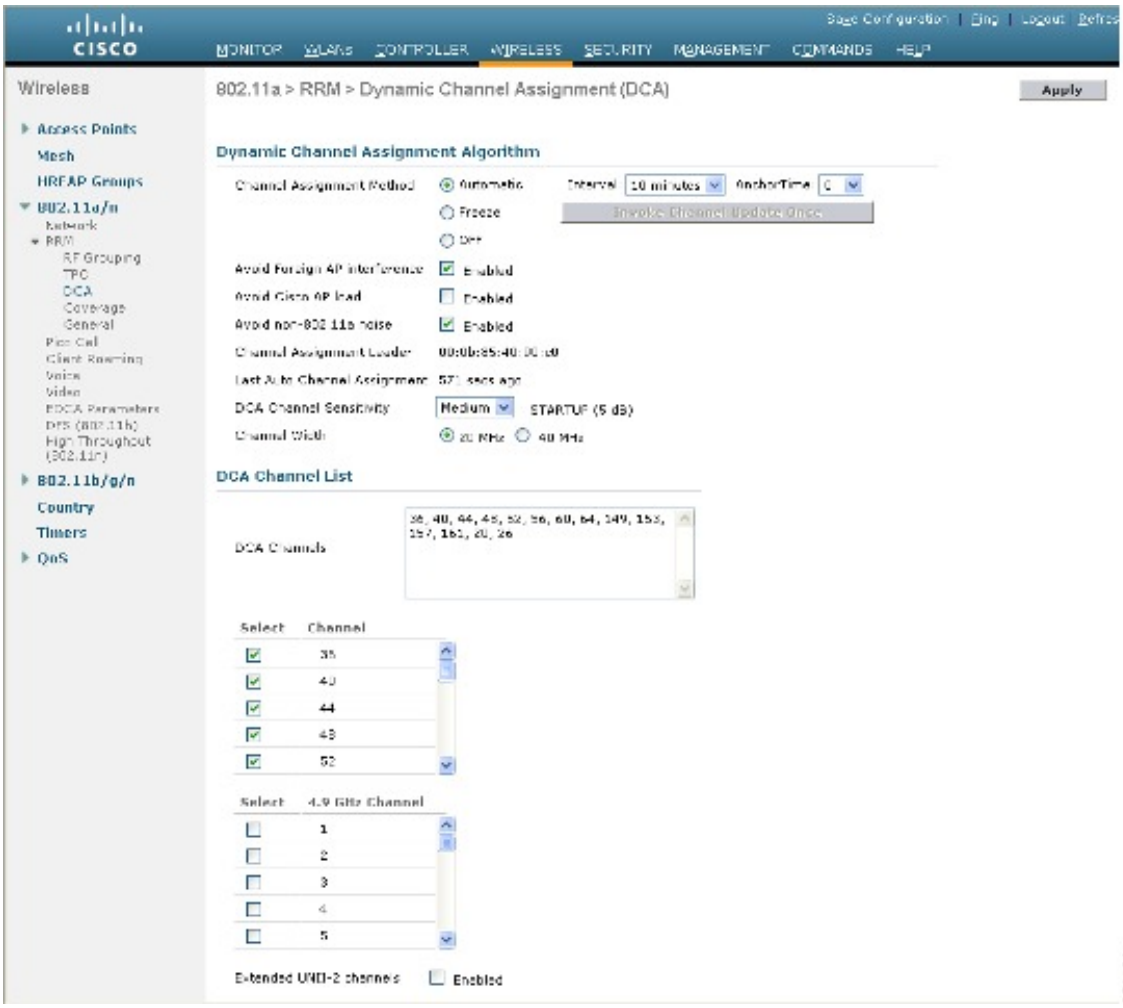
a) [Wireless] > [802.11a/n] または [802.11b/g/n] > [Network] の順に選択して、[802.11a（または 802.11b/g）Global Parameters] ページを開きます。

b) [802.11a（または 802.11b/g）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックして、変更を確定します。

ステップ 2 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [DCA] の順に選択して、[802.11a（または 802.11b/g） > RRM > Dynamic Channel Assignment (DCA)] ページを開きます。

図 *106*：*[802.11a > RRM > Dynamic Channel Assignment (DCA)]* ページ



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、コントローラの DCA モードを指定します。

- [Automatic]：コントローラによって、join しているすべてのアクセス ポイントのチャ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。 768 ビットは、デフォルト値です。
- [Freeze]：必要に応じて、コントローラによって、join しているすべてのアクセス ポイントのチャネル割り当ての評価と更新が行われます（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、すぐにチャネル割り当ての評価と更新が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。 コントローラのチャネルおよびパワーの動的設定を無効にする手順については、チャネルおよび電力の動的割り当ての無効化（GUI），（864 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） コントローラが 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、コントローラの RRM アルゴリズムで、Lightweight アクセス ポイントにチャ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ネルをアクセス ポイントが回避するようにチャ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、コントローラの RRM アルゴリズムで、チャ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、コントローラの RRM アルゴリズムで、Lightweight アクセス ポイントにチャ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選択して、コントローラが持続する non-WiFi 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 *41*：*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 ネットワークの場合のみ、次のいずれかの [channel width] 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ネル帯域幅を指定します。

- [20 MHz]：20 MHz のチャネル帯域幅（デフォルト）
- [40 MHz]：40 MHz のチャネル帯域幅

（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 つの隣接チャネルを選択します（たとえば、プライマリ チャネルとして 36、拡張チャネルとして 40）。 チャネルを 1 つだけしか選択しない場合、そのチャネルは 40 MHz のチャ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 チャネルおよび拡張チャネルも構成できます。

（注） グローバルに設定した DCA チャ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、チャネル 116、140、および 165 を他のチャネルと組み合わせることはできません。

このページには、次のような変更できないチャネル パラメータの設定も表示されます。

- [Channel Assignment Leader]：チャ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、コントローラが非 DFS チャ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す。

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ネルが表示されます。 チャネルを選択するには、[Select] カラムでそのチャネルのチェックボックスをオンにします。チャネルの選択を解除するには、チャ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 チャネル（100、104、108、112、116、132、136、および 140）は、チャネル 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 チャネル リストにこれらのチャ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、これらのチャネルが DCA チャネル リストに含まれていることを確認します。 チャネル リストにこれらのチャネルを含めるには、[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。 チャネルの選択を解除するには、チャ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] をクリックして、変更を確定します。

ステップ 16 802.11a または 802.11b/g ネットワークを次のように再度有効にします。

1. [Wireless] > [802.11a/n] 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。
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、チャネルが変更された無線の MAC アドレス、前のチャネルと新規のチャネル、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）

（注） コントローラ ソフトウェア リリース 5.2 以降のリリースの場合、カバレッジ ホールの検出は WLAN 単位で無効にできます。

ステップ 1 802.11a または 802.11b/g ネットワークを次のように無効にします。

a) [Wireless] > [802.11a/n] 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）Network Status] チェックボックスをオフにします。

c) [Apply] をクリックして、変更を確定します。

ステップ 2 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [Coverage] の順に選択して、[802.11a（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コントローラ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 秒間隔でコントローラ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 秒間隔でコントローラ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（コントローラの 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。 コントローラでは、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。 コントローラでは、カバレッジ ホールが修正可能かどうかが判断され、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] をクリックして、変更を確定します。

ステップ 9 802.11a または 802.11b/g ネットワークを次のように再度有効にします。

a) [Wireless] > [802.11a/n] 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）Network Status] チェックボックスをオンにします。

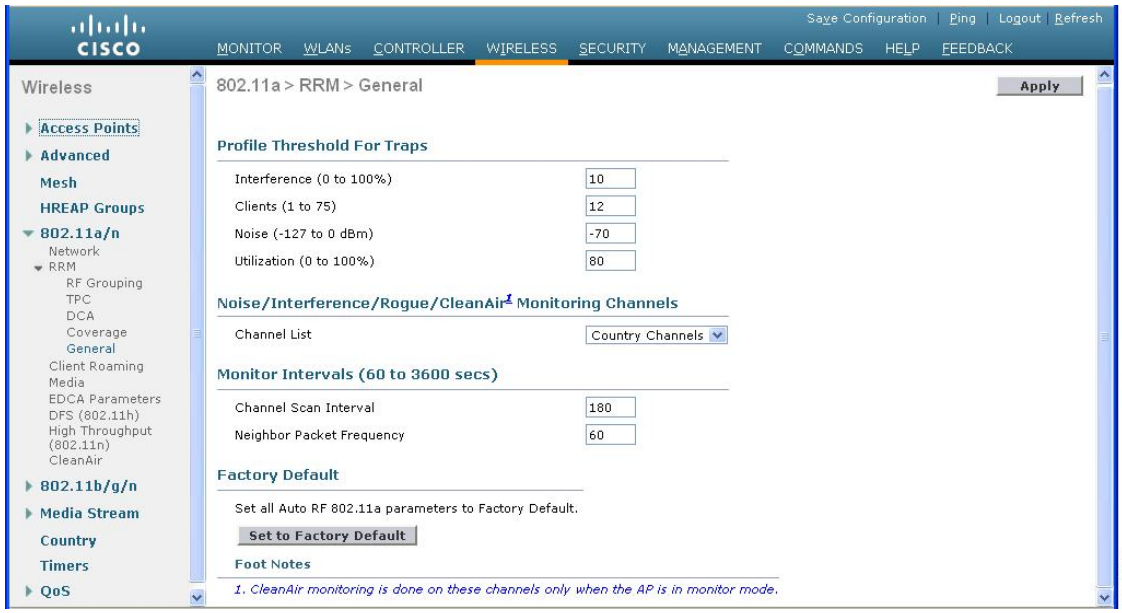
c) [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

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）

ステップ 1 [Wireless] > [802.11a/n] または [802.11b/g/n] > [RRM] > [General] の順に選択して、[802.11a（または 802.11b/g） > RRM > General] ページを開きます。

図 *107*：*[802.11a > RRM > General]* ページ



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 ポイントからコントローラに 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ネルで、RRM によるチャネル スキャンが実行されます。使用国で有効でないチャネルも対象となります。
- [Country Channels]：使用国内の D チャネルのみで、RRM によるチャネル スキャンが実行されます。768 ビットは、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ネル セットのみで、RRM によるチャネル 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 で使用するチャネル セットを指定できます。これを行うには、動的チャ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ネルでスキャンを実行する時間間隔の合計（秒）を入力します。 スキャン プロセス全体の所要時間はチャネル、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） コントローラで 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） コントローラで 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） コントローラ ソフトウェア リリース 4.1.185.0 以降のリリースでは、アクセス ポイント無線が既存のネイバーからネイバーパケットを60分以内に受信しない場合、コントローラによってネイバー リストからそのネイバーが削除されます。 4.1.185.0 より前のコントローラ ソフトウェア リリースでは、コントローラが応答しないネイバー無線をネイバー リストから削除するまでの待機時間は 20 分だけです。

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。

（注） コントローラの 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、802.11a 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、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。

- すべての 802.11a または 802.11b/g 無線の伝送パワーが定期的に RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

  config {802.11a | 802.11b} txPower global auto

- すべての 802.11a または 802.11b/g 無線の伝送パワーが一度だけ RRM によって自動的に再設定されるようにするには、次のコマンドを入力します。

  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するには、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。

  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。

- デフォルトの送信電力設定を手動で変更するには、次のコマンドを入力します。

  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 に下げるの

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、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。

- Transmit Power Control Version 2 をチャネルごとに設定するには、次のコマンドを入力します。

  config advanced {**802.11a** | **802.11b**} **tpcv2-per-chan** {**enable** | **disable**}

ステップ 4　動的チャネル割り当て（DCA）を設定するには、次のいずれかの操作を行います。

- アベイラビリティおよび干渉に基づいて、すべての 802.11a または 802.11b/g チャネルが RRM によって自動的に設定されるようにするには、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **channel global auto**

- アベイラビリティおよび干渉に基づいて、すべての 802.11a または 802.11b/g チャネルが一度だけ RRM によって自動的に再設定されるようにするには、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **channel global once**

- RRM を無効にし、すべてのチャネルをデフォルト値に設定するには、次のコマンドを入力します。

  config {**802.11a** | **802.11b**} **channel global off**

- DCA に使用するチャネル 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）　コントローラが 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。

- **config advanced** {**802.11a** | **802.11b**} **channel dca sensitivity** {**low** | **medium** | **high**}：DCA アルゴリズムでチャ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 *42*：*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**}：5 GHz 帯域におけるすべての 802.11n 無線の DCA チャネル幅を設定します。

  値は次のとおりです。

  ◦ **20** は 802.11n 無線のチャネル幅を 20 MHz に設定します。 768 ビットは、デフォルト値です。

  ◦ **40** は 802.11n 無線のチャネル幅を 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 チャネルとして 36、拡張チャネルとして 40）。 1 つのチャネルしか設定しないと、そのチャネルは 40 MHz チャ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 チャネルおよび拡張チャネルも構成できます。

  （注） グローバルに設定した DCA チャネル幅の設定を無効にする場合は、**config 802.11a chan_width** *Cisco_AP* {**20** | **40**} コマンドを使用して 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。 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。

- **config advanced {802.11a | 802.11b} channel outdoor-ap-dca {***enable* | *disable***}**：非 DFS チャネルのチェックを回避するためにコントローラ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）　コントローラ ソフトウェア リリース 5.2 以降のリリースの場合、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コントローラ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 秒間隔でそれらがコントローラに報告されます。
- **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。 コントローラでは、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、**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。 コントローラでは、カバレッジホールが修正可能かどうかが判断され、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。

```
802.11a Client Beacon Measurements:
    disabled
```

- **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。

```
Automatic Channel Assignment
  Channel Assignment Mode....................... ONCE
  Channel Update Interval....................... 600 seconds
  Anchor time (Hour of the day)................. 20
  Channel Update Count.......................... 0
  Channel Update Contribution................... S.IU
  Channel Assignment Leader..................... 00:0b:85:40:90:c0
  Last Run...................................... 532 seconds ago
  DCA Sensitivity Level......................... MEDIUM (20 dB)
  DCA 802.11n Channel Width..................... 40 MHz
  Channel Energy Levels
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Channel Dwell Times
    Minimum..................................... unknown
    Average..................................... unknown
    Maximum..................................... unknown
  Auto-RF Allowed Channel List.................. 36,40
```

```
  Auto-RF Unused Channel List..................... 44,48,52,56,60,64,100,104,
    ..................................... 108,112,116,132,136,140,149,
 ..................................... 153,157,161,165,190,196
  DCA Outdoor AP option..................... Disabled
```

- **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。

```
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode........... Enabled
  802.11a Coverage Voice Packet Count............ 10 packets
  802.11a Coverage Voice Packet Percentage....... 20%
  802.11a Coverage Voice RSSI Threshold.......... -75 dBm
  802.11a Coverage Data Packet Count............. 10 packets
  802.11a Coverage Data Packet Percentage........ 20%
  802.11a Coverage Data RSSI Threshold........... -80 dBm
  802.11a Global coverage exception level........ 25%
  802.11a Global client minimum exception lev. 3 clients
```

- **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。

```
RF Event and Performance Logging
  Channel Update Logging......................... Off
  Coverage Profile Logging....................... Off
  Foreign Profile Logging........................ Off
  Load Profile Logging........................... Off
  Noise Profile Logging.......................... Off
  Performance Profile Logging.................... Off
  TxPower Update Logging...................... Off
```

- **monitor**：シスコの無線監視に関する情報を表示します。

```
Default 802.11a AP monitoring
  802.11a Monitor Mode........................... enable
  802.11a Monitor Channels....................... Country channels
  802.11a AP Coverage Interval................... 180 seconds
  802.11a AP Load Interval....................... 60 seconds
  802.11a AP Noise Interval...................... 180 seconds
  802.11a AP Signal Strength Interval......... 60 seconds
```

- **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。

```
Default 802.11a AP performance profiles
  802.11a Global Interference threshold.......... 10%
  802.11a Global noise threshold................. -70 dBm
  802.11a Global RF utilization threshold........ 80%
  802.11a Global throughput threshold............ 1000000 bps
  802.11a Global clients threshold............... 12 clients
```

- **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。

```
802.11a Advanced Receiver Settings
 RxStart  : Signal Threshold..................... 15
 RxStart  : Signal Jump Threshold................ 5
 RxStart  : Preamble Power Threshold............. 2
 RxRestart: Signal Jump Status................... Enabled
 RxRestart: Signal Jump Threshold................ 10
 TxStomp  : Low RSSI Status...................... Enabled
 TxStomp  : Low RSSI Threshold................... 30
 TxStomp  : Wrong BSSID Status................... Enabled
 TxStomp  : Wrong BSSID Data Only Status......... Enabled
 RxAbort  : Raw Power Drop Status................ Disabled
 RxAbort  : Raw Power Drop Threshold............. 10
 RxAbort  : Low RSSI Status...................... Disabled
```

```
 RxAbort  : Low RSSI Threshold.................. 0
 RxAbort  : Wrong BSSID Status.................. Disabled
 RxAbort  : Wrong BSSID Data Only Status........ Disabled
 ------------------------------------------....
 pico-cell-V2 parameters in dbm units:..........

 RxSensitivity: Min,Max,Current RxSense Thres.... 0,0,0
 CCA Threshold: Min,Max,Current Clear Channel.... 0,0,0
Tx Pwr: Min,Max,Current Transmit Power for A.... 0,0,0
 ------------------------------------------....
```

- **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。

```
AP Name     MAC Address        Admin State  Operation State Channel TxPower
-------- ------------------ ------------- --------------- -------- -------
AP1140     00:22:90:96:5b:d0    ENABLED                 DOWN          64*     1(*)
AP1240     00:21:1b:ea:36:60    ENABLED            DOWN               161*       1(*)
AP1130     00:1f:ca:cf:b6:60    ENABLED      REGISTERED        48*          1(*)
```

- **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。

```
Leader Automatic Transmit Power Assignment
  Transmit Power Assignment Mode................. AUTO
  Transmit Power Update Interval................. 600 seconds
  Transmit Power Threshold....................... -70 dBm
  Transmit Power Neighbor Count.................. 3 APs
  Min Transmit Power............................. -10 dBm
  Max Transmit Power............................. 30 dBm
  Transmit Power Update Contribution............. SNI..
  Transmit Power Assignment Leader............... rangans (9.6.137.10)
  Last Run....................................... 507 seconds ago
  TPC Mode....................................... Version 1
  TPCv2 Target RSSI.............................. -67 dBm
  TPCv2 VoWLAN Guide RSSI........................ -67.0 dBm
  TPCv2 SOP...................................... -85.0 dBm
  TPCv2 Default Client Ant Gain..................   0.0 dBi
  TPCv2 Path Loss Decay Factor...................   3.6
  TPCv2 Search Intensity......................... 10 Iterations
```

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。

RRM ネイバー ディスカバリ パケットの設定

Cisco Neighbor Discovery Packet（NDP）は、ネイバーの無線情報に関する情報を提供する、RRM および他のワイヤレス アプリケーション用の基本的なツールです。 ネイバーディスカバリ パケットを暗号化するようにコントローラを設定できます。

この機能によって、PCI 仕様に準拠できるようになります。

RRM NDP および RF グループ化について

RF グループは、同じ暗号化メカニズムを持つコントローラ間でのみ形成することができます。つまり、暗号化されているコントローラにアソシエートされたアクセス ポイントは、暗号化されていないコントローラにアソシエートされたアクセス ポイントとネイバーになれません。 2 つのコントローラとそれらのアクセス ポイントは、互いをネイバーとして認識せず、RF グループを形成することはできません。 暗号化設定が一致していない静的 RF グループ設定に 2 つのコントローラを割り当てることができます。この場合、不一致のコントローラに属するアクセスポイントが、互いをグループのネイバーとして認識しないため、2 つのコントローラは単一の RF グループとして機能しません。

注意 7.0.116.0 リリースと前のリリースの相互動作：NDP 機能は 7.0.116.0 リリースから導入されたため、これらの場合の RF グループ形成が保証されるのは透過設定だけです。 以前のコントローラのリリースには、NDP 暗号化メカニズムはありません。

注意 リリース 7.0.116.0 間：同じ RF グループにするコントローラは、同じ保護設定にする必要があります。

RRM NDP の設定（CLI）

コントローラ CLI を使用して RRM NDP を設定するには、次のコマンドを入力します。

config advanced 802.11{**a**|**b**} **monitor ndp-mode** {**protected** | **transparent**}

このコマンドでは NDP モードが設定されます。 デフォルトでは、モードは「transparent」に設定されます。 次のオプションを使用できます。

- protected：パケットは暗号化されます。
- transparent：パケットはそのまま送信されます。

ディスカバリ タイプを表示するには、次のコマンドを使用します。

show advanced 802.11{a|b} monitor

RF グループの設定

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 の実行を調整するコントローラ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 グループにコントローラ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コントローラの機能を越えてスケールできるようになります。

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 -80dBm 以上の信号強度で受信すると、コントローラによって自動モードの RF 領域が動的に生成されます。 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、どちらもコントローラのクラスタ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 グループはスケー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 グループはスケー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 リーダーとしてコントローラ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、パワーおよびチャネルの割り当てを算出し、RF グループの各コントローラに送信します。 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 より前のコントローラのソフトウェア リリースでは、動的チャネル割り当て（DCA）の検索アルゴリズムによって、RF グループのコントローラにアソシエートされた無線について適切なチャ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ネル オプションがないため、チャ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ネル計画が次善のものになり、チャ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ことがあります。 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、新しいチャネル計画を検索する方法と、起こる可能性のあるチャ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。 コントローラ 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ネルを変更できます。 アク

セス ポイントによるチャ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、すべてのチャネル計画変更に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

コントローラには RF グループ名が設定されます。この RF グループ名は、そのコントローラに 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コントローラに同じ RF グループ名を設定します。

コントローラに join しているアクセス ポイントが別のコントローラ上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらのコントローラに同じ 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コントローラは、同じ国で構成された一連の国々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 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。
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]、このコントローラの [RF Group role]、[Update Interval]、およびこのコントローラの [Group Leader] のコントローラ名と 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：一度コントローラがスタティック 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。メンバのコントローラ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 （オプション）選択しなかったネットワーク タイプ（802.11a または 802.11b/g）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）

1

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 リーダーであるコントローラを確認します。
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、コントローラ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、このコントローラの 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、そのコントローラは現在、グループ リーダーです。

（注） * は、コントローラがスタティック メンバとして 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 リーダーであるコントローラを表示します。

show advanced 802.11b group

RRM の無効化

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。

チャネルおよびパワーの動的割り当てをコントローラでグローバルに無効にすることも、チャ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ネルおよびパワーを静的に設定することもできます。コントローラ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、動的チャネル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。

注意事項および制約事項

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。

相互に隣接するすべてのアクセス ポイントを最大電力レベルに割り当てないでください。

アクセスポイント無線へのチャネルおよび送信電力設定の静的割り当て

チャ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] または [802.11b/g/n] の順に選択して、[802.11a/n（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 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 チャネルおよび拡張チャネルを表示し、それらのチャ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（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。 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。
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、コントローラによって、実際の環境の等方性放射電力（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。 768 ビットは、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 は常に各国番号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 インストレーション 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] をクリックして、変更を確定します。

ステップ 9 次のように、アクセス ポイント無線の管理状態をコントローラから WCS へ即座に送信するように設定します。

1. [Wireless] > [802.11a/n] 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。
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。

ステップ 11 静的なチャネルおよびパワー 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 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 ポイントのチャネル幅を設定します。
config {**802.11a** | **802.11b**} **chan_width** *Cisco_AP* {**20** | **40**}

値は次のとおりです。

- **20**：20 MHz チャネルだけを使用して無線は通信できます。 20 MHz チャ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。 768 ビットは、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 ステップ *5* で選択するプライマリ チャネルおよび拡張チャネルを使用します。 各チャネルには、1 つの拡張チャネルがあります（36 と 40 のペア、44 と 48 のペアなど）。たとえば、プライマリ チャネルとして 44 を選択すると、コントローラでは拡張チャネルとしてチャネル 48 が使用されます。 プライマリ チャネルとして 48 を選択すると、コントローラでは拡張チャネルとしてチャネル 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 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 チャネル幅の設定（**config advanced 802.11a channel dca chan-width-11n** {**20** | **40**} 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。

（注） 米国およびカナダでは、チャネル 116、120、124、および 128 は、 40 MHz チャネル 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

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、コントローラによって、実際の環境の等方性放射電力（EIRP）が低減されます。

ステップ 5 次のコマンドを入力して、特定のアクセス ポイントで使用するチャネルを指定します。
config {**802.11a** | **802.11b**} **channel ap** *Cisco_AP channe*l

たとえば、802.11a チャネル 36 を AP1 のデフォルト チャ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ネルはプライマリ チャネル（たとえば、チャネル 36）です。このチャネルは、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、ステップ *2* でチャネル幅として 40 を選択した場合、このチャネルをプライマリ チャ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ネルも使用します。

（注） 動作チャネルを変更すると、アクセス ポイント無線はリセットされます。

ステップ 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 は常に各国番号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 インストレーション 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 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 静的なチャネルおよびパワー 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 9 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 10 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コントローラから 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 11 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 12 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
```

コントローラにおけるチャネルおよびパワーの動的割り当てのグローバルな無効化

チャ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] または [802.11b/g/n] > [RRM] > [Auto RF] の順に選択して、[802.11a（または 802.11b/g）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、コントローラに join している各アクセス ポイント無線にチャ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 （オプション）選択しなかったネットワーク タイプ（802.11a または 802.11b/g）について、この手順を繰り返します。

チャ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、**config802.11b 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

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

コントローラの RF グループを作成したら、コントローラに接続されているアクセス ポイントで不正なアクセス ポイントを検出するように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が確認されます。 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、このテーブルはコントローラに送信されます。

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 グループ内の各コントローラに同じ 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。 各コントローラ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 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。
このコントローラが属する 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コントローラについて、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コントローラが RF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイント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 グループ内の各コントローラに同じ 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。 各コントローラ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 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コントローラについて、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コントローラが RF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイントとして報告されます。

CCX 無線管理機能の設定

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 モードの場合は、アクセス ポイントをコントローラ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ネルを指定する必要はありません。 コントローラ、アクセス ポイント、およびクライアントによって、使用するチャネルが自動的に特定されます。

無線測定機能は、（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コントローラで取得できます。 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コントローラに返します。 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コントローラ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、各コントローラ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、コントローラ CLI で確認できます。

コントローラ ソフトウェアでは、モビリティ サービス エンジン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。 コントローラは、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、クライアントはコントローラ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コントローラを設定できます。 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] 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。

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、このコントローラ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 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。

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、コントローラの 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 または 802.11b/g）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 つのコントローラにつき最大 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す。

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 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）

- 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するには、次のコマンドを入力します。

  debug airewave-director message {**enable** | **disable**}

- クライアントロケーション調整アクティビティをデバッグするには、次のコマンドを入力します。

  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}

- 転送されたプローブとそれに含まれている両アンテナの RSSI の出力をデバッグするには、次のコマンドを入力します。

  debug dot11 load-balancing

第 13 章

Cisco CleanAir の設定

この項では、コントローラとアクセス ポイントに Cisco CleanAir を設定する方法について説明します。 ここで説明する内容は、次のとおりです。

- CleanAir について，873 ページ
- 注意事項および制約事項，876 ページ
- Cisco CleanAir の設定，878 ページ
- 干渉デバイスのモニタリング，887 ページ
- Spectrum Expert の接続の設定，897 ページ
- 関連資料，900 ページ
- CleanAir の機能履歴，900 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。

Cisco CleanAir システムは、CleanAir 対応のアクセス ポイント、コントローラ、および Cisco Prime インフラストラクチャで構成されます。 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、コントローラに転送します。 コントローラは、アクセスポイントを制御し、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 インフラストラクチャまたはシスコ モビリティ サービス エンジン（MSE）に転送します。 コントローラにはローカルなユーザ インターフェイスがあり、CleanAir の基本的な機能を設定することや、基本的なスペクトラム情報を表示することができます。 Prime インフラストラクチャには高度なユーザ インターフェイスがあり、Cisco CleanAir の機能の設定、情報の表示、記録の保持などが行えます。 MSE は基本

的な機能セットに対するオプションですが、非 Wi-Fi 干渉デバイスの位置の追跡など、高度な機能を使用するためには必須です。

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。

Cisco CleanAir システムにおけるコントローラの役割

Cisco CleanAir システムにおいて、コントローラは次のような処理を実行します。

- 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 回に付き 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を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、あるチャネル、またはある範囲内のチャ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がストリーム化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てい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。 CleanAir を使用すると、RRM DCA 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コントローラに保存し、チャ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、この情報をコントローラに保存します。 ローカル/ブリッジ モードの AP は、稼働チャ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、同じコントローラ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、チャネル選択の品質が向上します。

注意事項および制約事項

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：すべてのチャネル
  - DCA：DCA リストによって管理されるチャネル選択
  - Country：規制ドメイン内で合法なすべてのチャネル

  （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。 これに加えてスペクトラム インテリジェンスを実行すると、アクセス ポイントから他にデータが提供されるようになります。

- Cisco 5500 シリーズのコントローラでは、最大 2,500 のデバイス クラスタと、最大 10,000 のデバイス レコードをサポートしています。

- スペクトラム データの処理に必要な電力量によって、Cisco CleanAir のモニタリングに使用できる監視モードのアクセス ポイントの数が制限されます。 サポートされるモニタ モードのアクセス ポイントの数は、Cisco 5500 および Cisco Flex 7500 シリーズ コントローラでサポートされるアクセス ポイントの最大数と同じです。 この制限は、Cisco CleanAir の機能だけに影響します。

- 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がありません。
- コントローラでは、サポートできる監視モードの AP の数に制限があります。 これは、監視モードの AP によってすべてのチャネルのデータが保存されるためです。
- SE Connect モードでは、Cisco 2500 シリーズ コントローラ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。

Cisco CleanAir の設定

この項では、コントローラとアクセス ポイントに Cisco CleanAir を設定する方法について説明します。 ここで説明する内容は、次のとおりです。

コントローラでの Cisco CleanAir の設定

ここでは、次の内容について説明します。

- コントローラでの Cisco CleanAir の設定（GUI），（879 ページ）
- コントローラでの Cisco CleanAir の設定（CLI），（881 ページ）

コントローラでの Cisco CleanAir の設定（GUI）

ステップ 1 [Wireless] > [802.11a/n] 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選択して、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。コントローラがスペクトラム干渉を検出しないようにするには、これを選択解除します。 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選択して、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。コントローラが干渉源をレポートしないようにするには、これを選択解除します。 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、同じコントローラ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播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 のみ）
- [WiMAX Mobile]：WiMAX モバイル デバイス（802.11a/n のみ）
- [XBox]：Microsoft Xbox（802.11b/g/n のみ）

（注） 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、コントローラや Prime インフラストラクチャ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。この機能を無効にするには、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選択して、指定したデバイス タイプがコントローラ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、このボックスを選択解除します。 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のある干渉源が [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、コントローラ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選択して、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、Event Driven Radio Resource Management（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を表すのに対して、[High] は、感度を上げることを表します
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。

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、802.11a/n または 802.11b/g/n ネットワークで Cisco CleanAir の機能を設定します。
config {802.11a | 802.11b} cleanair {enable | disable} *all*

この機能を無効にすると、コントローラはスペクトラム 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 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） コントローラにアソシエートされているアクセス ポイントは、このコマンドで指定された干渉の種類に対し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ッディングを発生させたり、コントローラや Prim インフラストラクチャ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 3 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 4 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 5 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 6 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 7 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 8 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 9 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、Event Driven Radio Resource Management（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**}：Event Driven RRM（EDRRM）を有効または無効にします。 デフォルト値は [disabled] 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*：感度のしきい値を custom に設定した場合は、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 10 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 11 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 12 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 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 Event Driven RRM（EDRRM）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] または [802.11b/g/n] の順に選択して、[802.11a/n（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（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す。

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 [Back] をクリックして、[802.11a/n（または 802.11b/g/n）Radios] ページに戻ります。

ステップ 7 [802.11a/n（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 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 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 または 802.11b/g/n ネットワークにあるアクセス 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），（885 ページ）のステップ 7 を参照してください。

干渉デバイスのモニタリング

この項では、コントローラ GUI または CLI を使用して、802.11a/n および 802.11b/g/n 無線帯域の干渉デバイスをモニタする方法について説明します。

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] > [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。

  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。

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。
- [AP Name]：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] をクリックして、変更を適用します。
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 または 802.11b/g/n 無線帯域について、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について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*

以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No  ClusterID          DevID  Type             AP Name             ISI  RSSI   DC   Channel
--- ------------------ ------ ---------- ---------------- ---- ----- ---- -------------
1   c2:f7:40:00:00:03  0x8001 DECT phone  CISCO_AP3500  1    -43     3       149,153,157,161
3   c2:f7:40:00:00:03  0x8005 Canopy          CISCO_AP3500  2    -62      2
153,157,161,165
```

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 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*

以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
  * indicates cluster center device

No  ClusterID          DevID  Type                  AP Name       ISI  RSSI  DC   Channel
--- ------------------ ------ --------------------- ------------- ---- ----- --- --------------
1  b4:f7:40:00:00:03 0x4185 DECT-like (26) CISCO_AP3500 1    -58      3   153,157,161,165
```

永続的干渉源の検出

802.11a/n 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*

以下に類似した情報が表示されます。

```
Number Of Slots.................................. 2
AP Name.......................................... AP1-L
MAC Address...................................... c4:7d:4f:3a:07:1e
  Slot ID........................................ 1
  Radio Type..................................... RADIO_TYPE_80211a
  Sub-band Type.................................. All
  Noise Information
    Noise Profile................................ PASSED
    Channel 34..................................  -97 dBm
    Channel 36..................................  -90 dBm
    Channel 38..................................  -97 dBm
Interference Information
    Interference Profile......................... PASSED
    Channel 34................................... -128 dBm @  0 % busy
    Channel 36................................... -128 dBm @  0 % busy
```

```
    Channel 38..................................... -128 dBm @  0 % busy
    Channel 40..................................... -128 dBm @  0 % busy
Load Information
    Load Profile................................... PASSED
    Receive Utilization............................ 0 %
    Transmit Utilization........................... 0 %
    Channel Utilization............................ 0 %
    Attached Clients............................... 0 clients
  Coverage Information
    Coverage Profile............................... PASSED
    Failed Clients................................. 0 clients
  Client Signal Strengths
    RSSI -100 dbm.................................. 0 clients
    RSSI  -92 dbm.................................. 0 clients
    RSSI  -84 dbm.................................. 0 clients
Client Signal To Noise Ratios
    SNR    0 dB.................................... 0 clients
    SNR    5 dB.................................... 0 clients
    SNR   10 dB.................................... 0 clients
    SNR   15 dB.................................... 0 clients
Nearby APs
    AP c4:7d:4f:52:cf:a0 slot 1.................  -36 dBm on 149 (10.10.10.27)
    AP c4:7d:4f:53:1b:50 slot 1.................  -10 dBm on 149 (10.10.10.27)
Radar Information
  Channel Assignment Information
    Current Channel Average Energy................ unknown
    Previous Channel Average Energy............... unknown
    Channel Change Count.......................... 0
Last Channel Change Time..................... Mon May 17 11:56:32 2010
    Recommended Best Channel...................... 149
  RF Parameter Recommendations
    Power Level.................................... 7
    RTS/CTS Threshold.............................. 2347
    Fragmentation Tnreshold........................ 2346
    Antenna Pattern................................ 0

  Persistent Interference Devices
  Classtype Channel DC (%) RSSI (dBM) Last Update Time
---------------  -------  ------  ----------  ------------------------
  Canopy       149      4   -63        Tue May 18 03:21:16 2010
  All third party trademarks are the property of their respective owners.
```

永続的デバイスのモニタリング（GUI）

コントローラのGUIを使用して特定のアクセスポイントに対する永続的デバイスをモニタリングするには、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（または 802.11b/g/n）Radios] ページを開きます。 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（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、コントローラ GUI と CLI の両方を使用して、802.11a/n 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] または [802.11b/g] > [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 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 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ネル。
- [Minimum AQ]：この無線チャネルの最低電波品質。
- [Average AQ]：この無線チャネルの平均電波品質。
- [Interferer]：802.11a/n 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 または 802.11b/g/n の無線帯域の電波品質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。

電波品質のサマリーの表示

802.11a/n 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

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel   Avg AQ     Min AQ    Interferers  DFS
--------------  --------- -------  ------- ------------ ----
CISCO_AP3500     36      95    70    0
CISCO_AP3500     40           93  75     0
CISCO_AP3500     44           95   80     0
CISCO_AP3500     48           97   75     0
CISCO_AP3500     52           98   80     0
...
```

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 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

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel   Avg AQ     Min AQ   Interferers   DFS
--------------- --------- -------- --------- ------------ ------
CISCO_AP3500     1    83     57       3      5
```

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 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*

以下に類似した情報が表示されます。

```
Slot Channel  Avg AQ   Min AQ    Total Power (dBm)  Total Duty Cycle (%)
---- ------- -------  ------    -----------------  --------------------
1  140    100  100   -89      0

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS
---------------------- ------------------------- ----------- ---
-128       0                          0
```

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] > [802.11b/g] > [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 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 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。
- [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]：802.11a/n 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。

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] または [802.11b/g/n] の順に選択して、[802.11a/n（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（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、802.11a/n または 802.11b/g/n の無線帯域の電波品質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。

電波品質のサマリーの表示（CLI）

802.11a/n 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

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel   Avg AQ     Min AQ    Interferers  DFS
--------------  --------- -------  ------- ------------ ----
CISCO_AP3500     36           95     70       0
CISCO_AP3500     40           93     75       0
CISCO_AP3500     44           95     80       0
CISCO_AP3500     48           97     75       0
CISCO_AP3500     52           98     80       0
...
```

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 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

以下に類似した情報が表示されます。

```
AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name         Channel   Avg AQ     Min AQ   Interferers   DFS
--------------- --------- -------- --------- ------------ ------
CISCO_AP3500     1    83     57       3      5
```

ある無線帯域のアクセス ポイントの電波品質の表示（CLI）

802.11a/n 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*

以下に類似した情報が表示されます。

```
Slot Channel  Avg AQ   Min AQ    Total Power (dBm)  Total Duty Cycle (%)
```

```
---- ------- -------  ------    -----------------  --------------------
1  140    100  100   -89      0

Interferer Power (dBm) Interferer Duty Cycle (%) Interferers DFS
---------------------- ------------------------- ----------- ---
-128       0                         0
```

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 または 802.11b/g/n 無線帯域について、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について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*

  以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No  ClusterID          DevID  Type             AP Name             ISI  RSSI   DC
Channel
--- ------------------ ------ ---------- --------------- ---- ----- ---- -------------
1   c2:f7:40:00:00:03  0x8001 DECT phone  CISCO_AP3500  1    -43     3
149,153,157,161
3   c2:f7:40:00:00:03  0x8005 Canopy          CISCO_AP3500  2    -62      2
153,157,161,165
```

- 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）

以下に類似した情報が表示されます。

```
DC = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
  * indicates cluster center device

No  ClusterID          DevID  Type                  AP Name       ISI  RSSI  DC
 Channel
--- ----------------- ------ -------------- ------------ ---- ----- ---
--------------
1  b4:f7:40:00:00:03 0x4185 DECT-like (26) CISCO_AP3500 1    -58      3
153,157,161,165
```

永続的干渉源の検出（CLI）

802.11a/n 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*

以下に類似した情報が表示されます。

```
Number Of Slots.................................. 2
AP Name.......................................... CISCO_AP3500
...
Persistent Interferers
  Classtype                 Channel  DC (%)  RSSI (dBm)  Last Update Time
  ------------------------  -------  ------  ----------  -------------------------
 802.11FH                      149  3  -58   Thu Jan 1 00:20:34 2009
 Radar                         153  2  -81   Thu Jan 1 00:20:35 2009
 Continuous Transmitter        157  2  -62   Thu Jan 1 00:20:36 2009
 ...
    All third party trademarks are the property of their respective owners.
```

Spectrum Expert の接続の設定

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 インフラストラクチャから半自動的に開始することも、コントローラ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 コントローラの 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す。 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。

コントローラの 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 機能にを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 つ以上あることが必要です。
d) [Apply] をクリックして、変更を確定します。
e) アクセス ポイントをリブ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 ポイントをリブ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） コントローラ（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。 コントローラ 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 ポイントがコントローラに 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、これにコントローラは 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コントローラで作成されたものです。 コントローラはアクセス 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。コントローラの GUI の [802.11a/n（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。

関連資料

関連項目	参照先
• CleanAir に関する Cisco Prime インフラストラクチャ レポート • Cisco Prime インフラストラクチャを使用して Spectrum Expert の接続を開始する方法	『Cisco Location Application Configuration Guide』 URLhttp://www.cisco.com/en/US/products/ps12239/products_installation_and_configuration_guides_list.html
Spectrum Expert の使用方法	Cisco Spectrum Expert Users Guide, Release 4.0 URLhttp://www.cisco.com/en/US/products/ps9393/products_user_guide_list.html

CleanAir の機能履歴

次の表に、この機能のリリースの履歴を示します。

表 *43*：*CleanAir* の機能履歴

機能名	リリース	機能情報
Cluster ID	7.0.116.0	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。
CleanAir	7.0.98.0	CleanAir を使用すると、Wi-Fi 以外の干渉源を識別および追跡し、最適なパフォーマンスが得られるようネットワーク設定を調整し、悪意のあるデバイスからの脅威を識別し、WLAN と他のワイヤレスデバイスを共存させられるようになります。

第 14 章

FlexConnect の設定

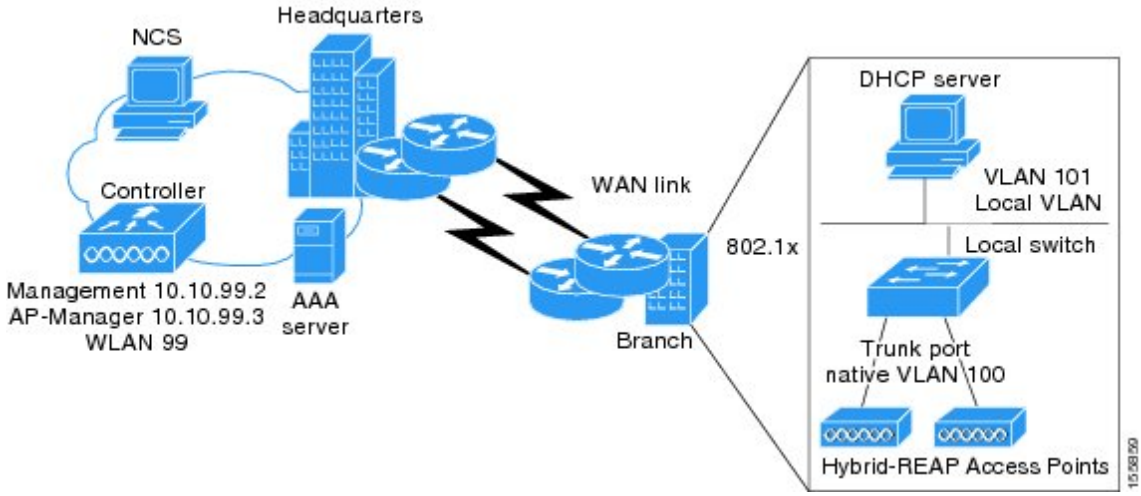
- FlexConnect について，901 ページ
- 注意事項および制約事項，906 ページ
- FlexConnect の設定，909 ページ
- FlexConnect ACL の設定，922 ページ
- FlexConnect グループの設定，926 ページ

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 *108*：*FlexConnect* の導入



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ると、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とき（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。 この状態はスタンドアロン 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 ポイントがスタンドアロン 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 Radio Resource Management（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、ネイバー 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、スタンドアロン モードで動的周波数選択をサポートします。

（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 ポイントがスタンドアロン 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 ポイントはスタティック IP に戻ってリブートします（アクセス ポイントがスタティック 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ト解除して、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。

注意事項および制約事項

- 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 アドレスを提供できる必要があります。
- 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。
- FlexConnect は、1040、1130、1140、1550、3500、3600、2600、1250、1260、1240、OEAP 600、ISR 891、および ISR 881 の各アクセス ポイントでのみサポートされています。
- アクセス ポイントとコントローラの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。

- 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。
- クライアント接続は、アクセス ポイントがスタンドアロン 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 ポイントがスタンドアロン モードから接続モードに移行した後で、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 ポイントがスタンドアロン 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- QoS プロファイルのユーザ別の帯域幅コントラクトは、FlexConnect によりローカルでスイッチされた WLAN においてサポートされます。 QoS ユーザ別の帯域幅コントラクトは、中央でスイッチされた WLAN およびローカル モードの AP でのみサポートされます。
- ゲスト ユーザ設定は、FlexConnect ローカル スイッチングではサポートされていません。
- 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。
- FlexConnect アクセス ポイントでは、クライアント ロード バランシングはサポートされていません。
- 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。
- 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、50 台までのアクセス 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。
- 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 スイッチングを使用する 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 スイッチングを有効にすると、AP はローカル スイッチングを実行します。 ただし、ローカル モードの AP に対しては、中央スイッチングが実行されます。

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
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
```

```
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 209.165.200.228 255.255.255.224
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
 ip helper-address 209.165.200.225
!
interface Vlan101
 ip address 209.165.200.225 255.255.255.224
 ip helper-address 209.165.200.225
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。 この表に、3 つの WLAN の例を示します。

表 *44*：*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）

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）
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）

（注） ゲスト ユーザ設定は、FlexConnect ローカル スイッチングではサポートされていません。

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 アカウントの作成の詳細については、「ユーザ アカウントの管理」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、（表 44：WLAN の例にある表の例に従って）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] をクリックして、変更を確定します。 [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。

a) [Layer 3 Security] ドロップダウン リストから [None] を選択します。

b) [Web Policy] チェックボックスをオンにします。

c) [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。

（注） WLAN へのローカル ユーザの追加の詳細については、またゲスト ユーザが WLAN にアクセスしたときに表示されるログイン ページのコンテンツと外観のカスタマイズの詳細については、「セキュリティ ソリューションの設定」の手順に従ってください。

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] をクリックして、変更を確定します。 [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。

a) [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。
b) 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。
c) [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [WPA+WA2] 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。

a) [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。
b) 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。
c) [Security > Layer 2] タブで、[Layer 2 Security] ドロップダウン リストから [WPA+WA2] を選択し、必要に応じて [WPA+WPA2] パラメータを設定します。
d) [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） これらは、この機能の注意事項および制限事項です。

  - 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。

- [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 をイネーブルにするには、[Central DHCP Processing] を有効に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 [Save Configuration] をクリックして、変更を保存します。

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。

- **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。

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**}：FlexConnect CCKM 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 [AP サブ 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。

- [PPPOE]：アクセス ポイント上での Point-to-Point Protocol over Ethernet（PPPoE）サブモードを設定します。
- [PPPOE+WIPS]：アクセス ポイント上での Point-to-Point Protocol over Ethernet（PPPoE）サブモードと wIPS サブモードの両方を設定します。

（注） FlexConnect モードで PPPoE を有効にする場合は、20 台を超えるクライアントを AP に関連付けないことを推奨します。 20 台を超えるクライアントを AP に関連付けた場合は、AP のメモリ不足の問題を引き起こす場合があります。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

ステップ 6 [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 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] をクリックして、変更を確定します。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] をクリックして、変更を確定します。

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。

（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 タギングは有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。

- 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するには、次のコマンドを入力します。

  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。

- FlexConnect モードの AP 上で Web ポリシー ACL を設定するには、次のコマンドを入力します。

  config ap flexconnect web-policy acl {**enable** | **disable**} *acl_name cisco_ap*

（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。

- 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*

- WLAN ごとに AP 上での中央 DHCP を設定するには、次のコマンドを入力します。

  config ap flexconnect central-dhcp *wlan-id ap-name* {**enable override dns** | **disable** | **delete**}

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 44：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、オープンの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 ACL の設定

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中央処理装置（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、ローカルで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。

注意事項および制約事項

- FlexConnect ACL は FlexConnect アクセス ポイントにのみ適用できます。 設定は、AP ごと、VLAN ごとに適用されます。
- 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。
- AP ごとに最大 32 の ACL を使用して、コントローラ上で最大 512 の ACL を設定できます。
- 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。 インターフェイスを作成し、FlexConnect アクセス ポイント上での WLAN-VLAN マッピングを設定できます。
- 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。

- コントローラで設定されている FlexConnect 以外の ACL は、FlexConnect AP に適用できません。
- 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 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。
- CAPWAP が LWAPP と異なるポートを使用しているので、ネットワーク内の ACL を変更する必要がある場合があります。
- 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、アクセス ポイントによってドロップされます。

FlexConnect ACL の設定

FlexConnect ACL の設定（GUI）

ステップ 1 [Security] > [Access Control Lists] > [FlexConnect Access Control Lists] を選択して、[FlexConnect ACL] ページを開きます。
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、このコンとローラ上で作成した FlexConnect ACL が表示されます。 ACL 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 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。
[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 [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。

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]：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]：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]：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。

[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、ネットワーキング 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 編集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。

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] をクリックして、変更を保存します。

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 }**：このルール 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「any」を入力します。 デフォルトは 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 flexconnectacl 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**：アクセス コントロール リストの概要を表示します。
- **show flexconnect acl detailed acl-name**：アクセス コントロール リストの詳細な ACL 情報を表示します。
- **debug flexconnect acl {enable | disable}**：FlexConnect ACL を有効または無効にします。 トラブルシューティングするには、このコマンドを使用します。
- **debug capwap reap**：CAPWAP のデバッグを有効にします。

FlexConnect グループの設定

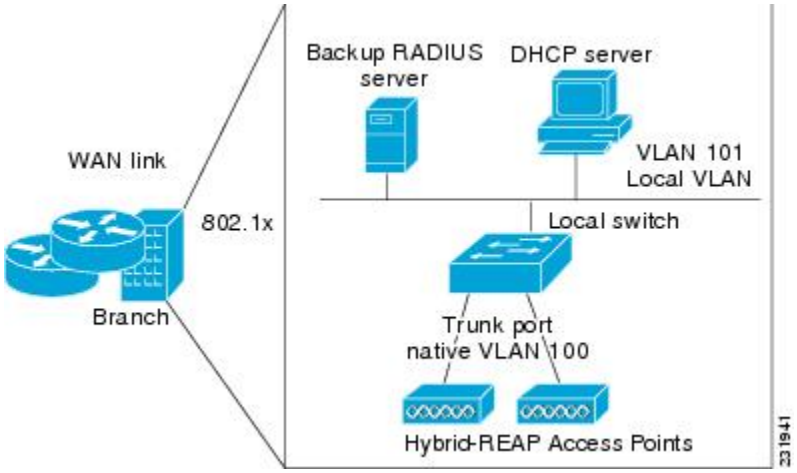
FlexConnect グループについて

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。

ブランチ オフィスにバックアップ RADIUS サーバを持つ、一般的な FlexConnect の導入。

図 *109*：*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 高速ローミングで必要となります。 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 または EAP-FAST 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） 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 50 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（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 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 9 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、不一致が起こらないように、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 10 [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 11 [Apply] をクリックして、変更を確定します。

ステップ 12 この FlexConnect グループにアクセス ポイントをさらに追加するには、ステップ *9* ～ステップ *11* を繰り返します。

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。

a) [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。

b) [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。

c) [Apply] をクリックして、変更を確定します。
d) [Local Authentication] タブを選択して、[FlexConnect > Edit (Local Authentication > Local Users)] ページを開きます。
e) LEAP または EAP-FAST 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。
f) [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。
g) 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す。
h) [Apply] をクリックして、変更を確定します。
i) [Protocols] タブを選択して、[FlexConnect > Edit (Local Authentication > Protocols)] ページを開きます。
j) 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てステップ *n* に進みます。
k) FlexConnect アクセス ポイントが EAP-FAST 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 EAP-FAST Authentication] チェックボックスをオンにして次の手順に進みます。 デフォルト値はオフです。
l) 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。

m) [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。
n) [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。
o) 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。
p) [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。

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_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_name* **radius server** {**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 4 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_name* **radius ap** {**enable** | **disable**}

c) LEAP または EAP-FAST を使用して認証できるクライアントのユーザ名とパスワードを入力するには、次のコマンドを入力します。
config flexconnect *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) 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かどうかを指定するには、次のコマンドを入力します。
config flexconnect *group_name* **radius ap leap** {**enable** | **disable**}

e) FlexConnect アクセス ポイントが EAP-FAST を使用してクライアントを認証できるかどうかを指定するには、次のコマンドを入力します。
config flexconnect group_name radius ap eap-fast {**enable** | **disable**}

f) 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_name* **radius ap server-key** *key*：PAC の暗号化と復号化に使用するサーバ 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_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。

g) 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_name* **radius ap authority id** *id*
id は 32 桁の 16 進数文字です。

h) 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_name* **radius ap authority info** *info*
info は 32 桁までの 16 進数文字です。

i) 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_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 5 WLAN ごとに中央 DHCP を設定するには、次のコマンドを入力します。
config flexconnect group *group-name* **central-dhcp** *wlan-id* {**enable override dns** | **disable** | **delete**}

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、FlexConnect グループの最新のリストを表示します。
show flexconnect summary

以下に類似した情報が表示されます。

```
flexconnect Summary: Count 2

Group Name    # Aps
Group 1    1
Group 2    1
```

ステップ 8 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*

以下に類似した情報が表示されます。

```
Number of Ap's in Group: 3

00:1d:45:12:f2:24    AP1240.EW3.f224    Joined
00:1d:45:12:f7:12    AP1240.10.f712     Joined
00:1d:a1:ed:9f:84    AP1131.23.9f84     Joined

Group Radius Servers Settings:
 Primary Server Index.......................... Disabled
 Secondary Server Index........................ Disabled

Group Radius AP Settings:
AP RADIUS server............. Enabled
EAP-FAST Auth................ Enabled
LEAP Auth.................... Enabled
Server Key Auto Generated... No
Server Key..................     <hidden>
Authority ID................. 436973636f00000000000000000000000
Authority Info............... Cisco A_ID
PAC Timeout.................. 0
Number of User's in Group: 20

                  1cisco                   2cisco
                  3cisco                   4cisco
                   cisco                    test1
                  test10                   test11
                  test12                   test13
                  test14                   test15
                   test2                    test3
                   test4                    test5
                   test6                    test7
```

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、入力 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）

はじめる前に

- **config flexconnect group** *group-name* **vlan add** *vlan-id* acl *ingress-acl egress-acl*：FlexConnect グループに VLAN を追加して、入力 ACL および出力 ACL をマッピングします。

VLAN-ACL マッピングの表示（CLI）

はじめる前に

- **show flexconnect group detail** *group-name*：FlexConnect グループの詳細を表示します。
- **show ap config general** *ap-name*：アクセス ポイントの VLAN-ACL マッピングを表示します。

FlexConnect の AAA Override の設定

AAA Override について

WLAN の Allow AAA Override オプションを使用すると、WLAN で認証を設定できます。 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、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。 FlexConnect に対する AAA Override は、オーバーライドされたクライアントの高速ローミング（OKC/CCKM）もサポートしています。

注意事項および制約事項

- 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。

- 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、既存の WLAN-VLAN マッピングを使用してアクセス ポイント上に作成することができます。
- VLAN は、FlexConnect グループで設定することができます。
- 常に、AP には最大 16 の VLAN があります。 まず、VLAN は AP の設定（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 メッセージが記録されます。
- WLAN-VLAN を使用して AP で VLAN を設定する場合、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 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。
- ローカルにスイッチされたクライアントに対する AAA は、VLAN Override のみをサポートします。

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] 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 Override を設定するアクセス ポイントの [AP name] リンクをクリックします。

ステップ 3 [FlexConnect] タブをクリックします。

ステップ 4 ネイティブ VLAN ID 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。 このページには、次の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 Mappings]：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 に対する VLAN ID の列を編集して、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]：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 マッピングと出力 ACL マッピングを変更します。 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。
- [Group Level VLAN ACL Mappings]：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*

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関する情報

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。

注意事項および制約事項

- 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] および [Backup] 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}**：プリイメージ 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 15 章

モビリティ グループの設定

- モビリティについて，941 ページ
- モビリティ グループについて，945 ページ
- モビリティ グループの設定，949 ページ
- モビリティ グループの統計の表示，955 ページ
- 自動アンカー モビリティの設定，958 ページ
- WLAN モビリティ セキュリティの値の検証，963 ページ
- シンメトリック モビリティ トンネリングの使用，964 ページ
- シンメトリック モビリティ トンネリングの確認，965 ページ
- モビリティ ping テストの実行，966 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，967 ページ
- 外部マッピングの設定，970 ページ

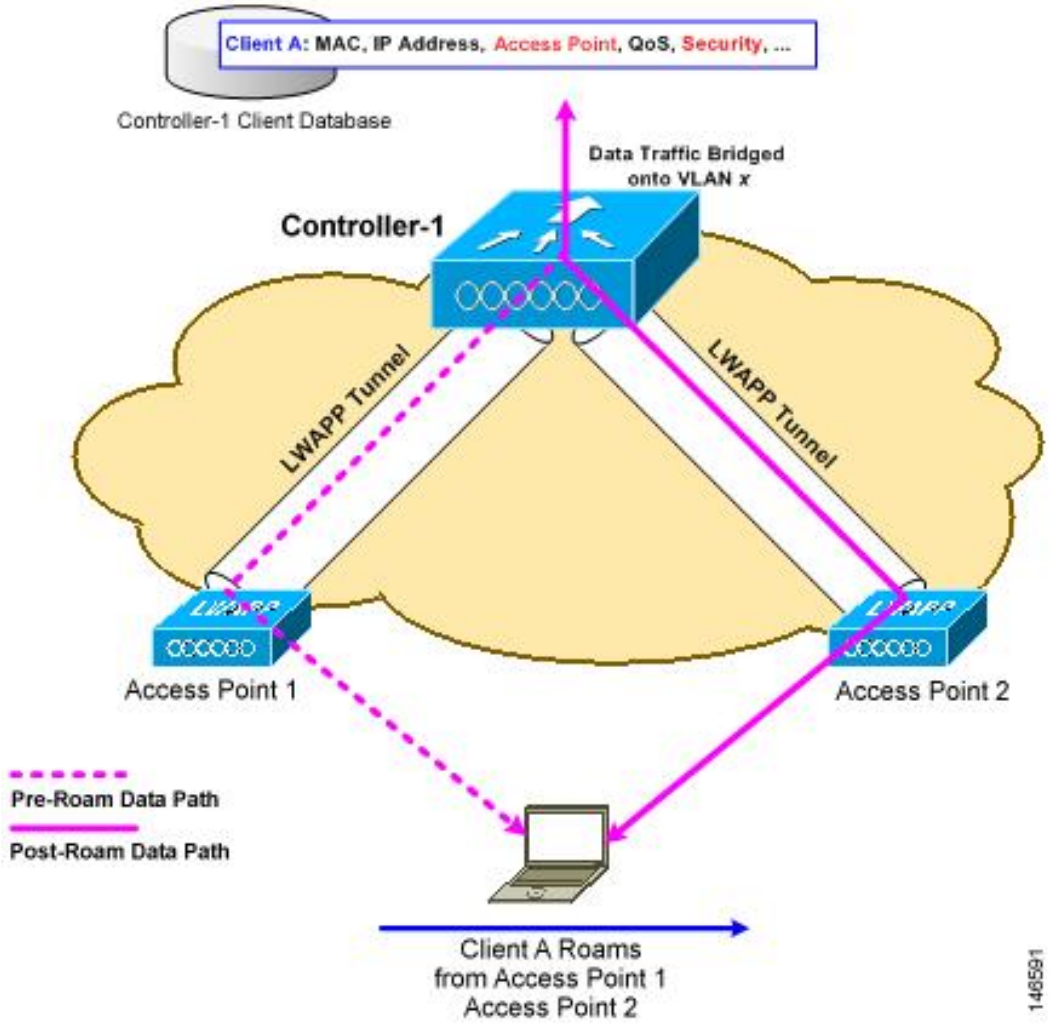
モビリティについて

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 *110*：コントローラ内ローミング

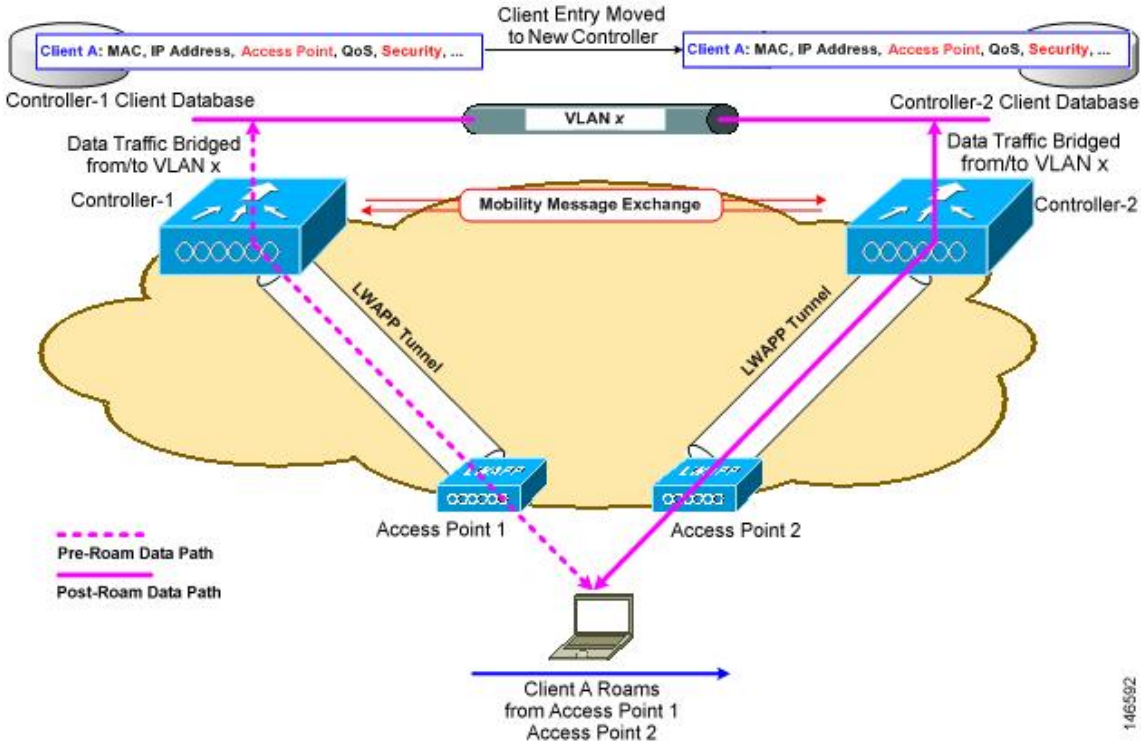


ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントへ移動する場合、コントローラはクライアントのデータベースを新たにアソシエートするアクセス ポイントでアップデートするだけです。 必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

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 *111*：コントローラ間ローミング

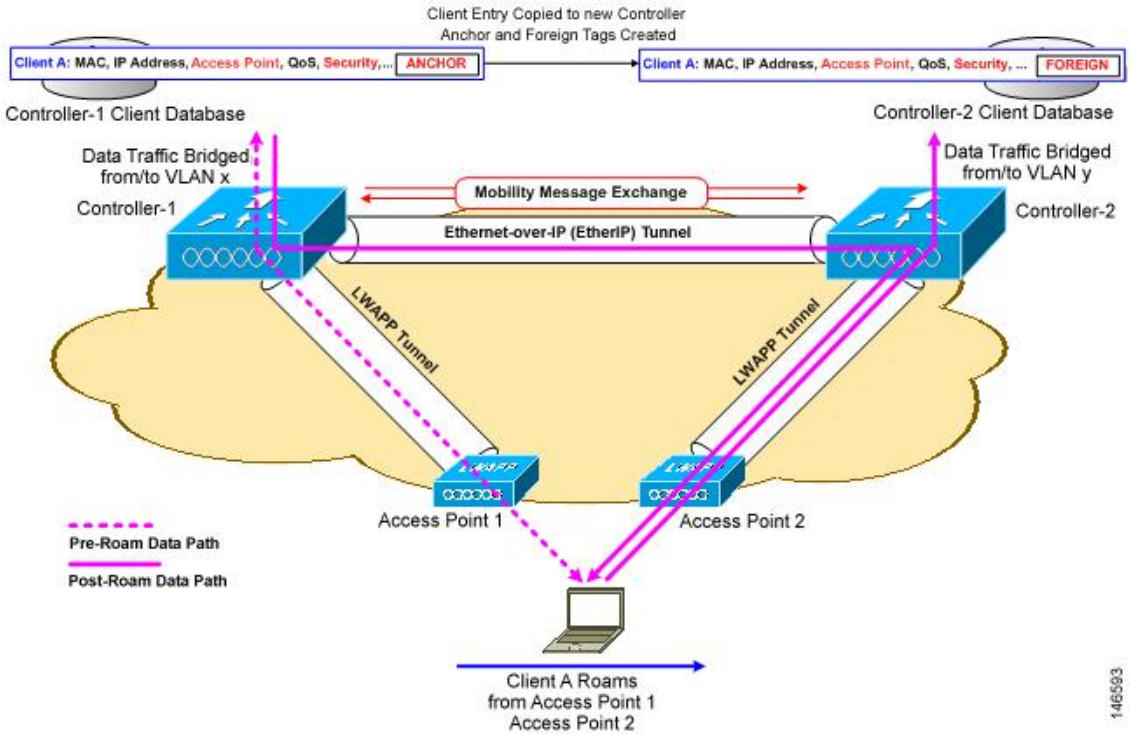


クライアントが新たなコントローラに join されたアクセス ポイントへアソシエートする場合、新たなコントローラはモビリティ メッセージを元のコントローラと交換し、クライアントのデータベース エントリは新たなコントローラに移動されます。 新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセスポイントに対してアップデートされます。 このプロセスは、ユーザには透過的に行われます。

（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 *112* : 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、ソースベースのルーティングやソースベ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。

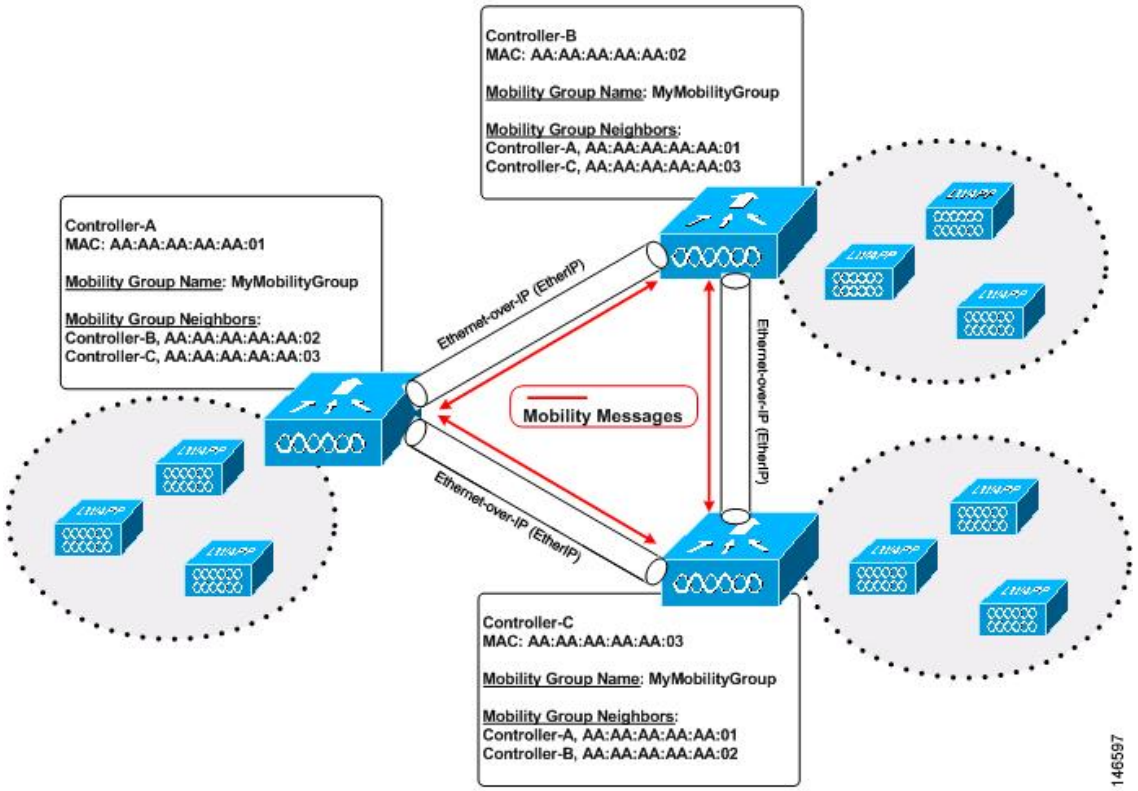
（注） クライアントが Web 認証状態でローミングする場合、クライアントはモバイル クライアントして見なされるのではなく、別のコントローラ上の新しいクライアントとして見なされます。

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 *113*：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

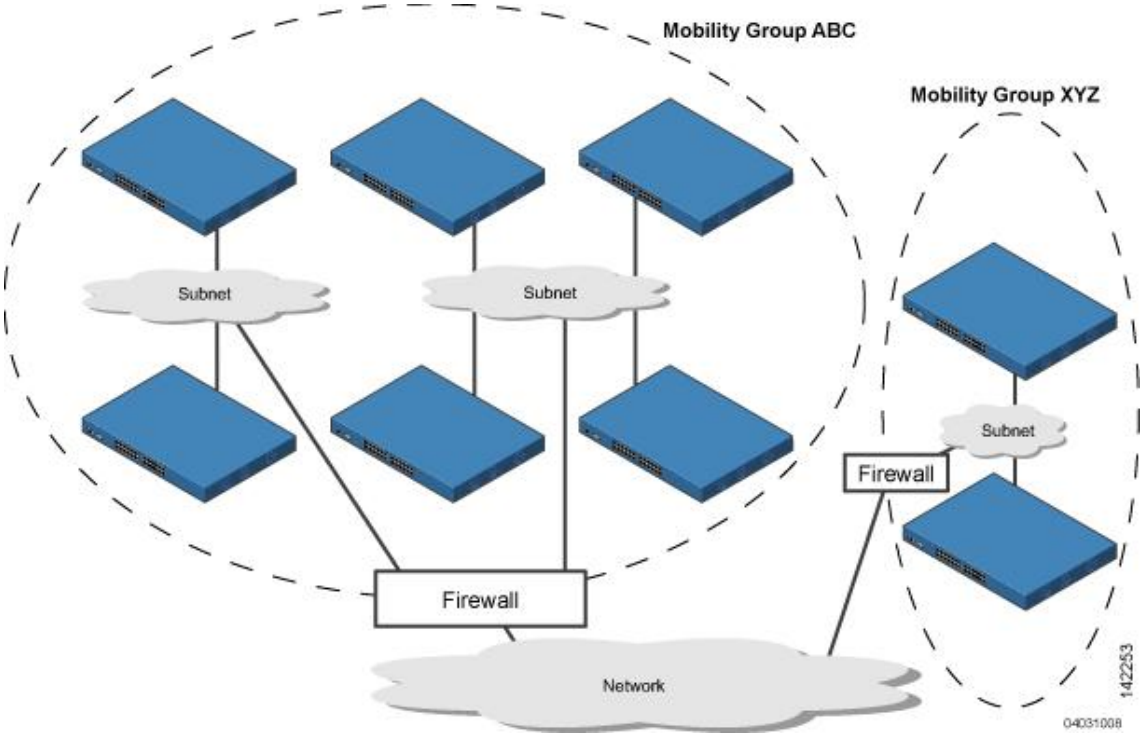
メッセージ（または、モビリティ マルチキャストが設定されている場合はマルチキャスト メッセージ）をそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。

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 *114* : *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。

例：

```
Controller 1                  Controller 2                  Controller 3
Mobility group: A             Mobility group: A             Mobility group: C
Mobility list:                Mobility list:                Mobility list:
 Controller 1 (group A)       Controller 1 (group A)        Controller 1 (group A)
 Controller 2 (group A)       Controller 2 (group A)        Controller 3 (group C)
 Controller 3 (group C) ?
```

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、クライアントは異なるモビリティ グループでも同じ IP アドレスを維持します。ただし、Cisco Centralized Key Management（CCKM）および Public Key Cryptography（PKC）は、モビリティ グループ間ローミングの場合だけ、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。

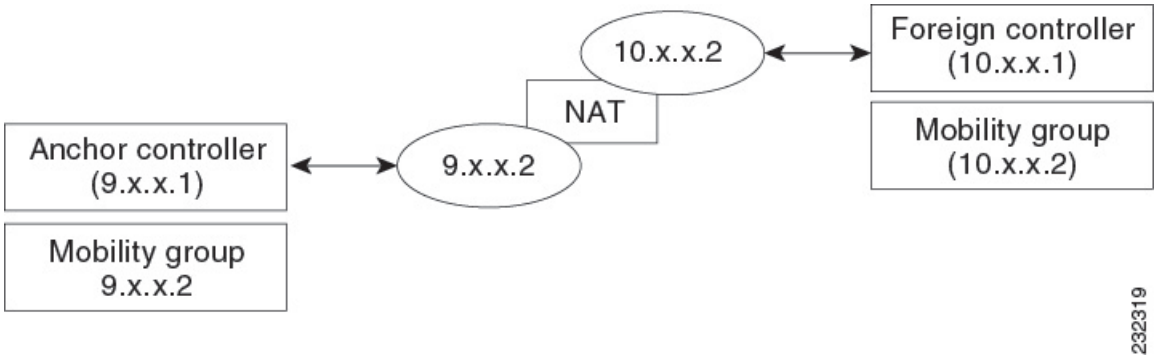
NAT が有効になっているネットワークのモビリティ グループを設定する際に、コントローラの管理インターフェイス IP アドレスではなく、NAT デバイスからコントローラに送信される IP アドレスを入力します。 さらに、PIX などのファイアウォールを使用している場合には、ファイアウォールで次のポートが開いていることを確認します。

- 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にのみ機能します。 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。

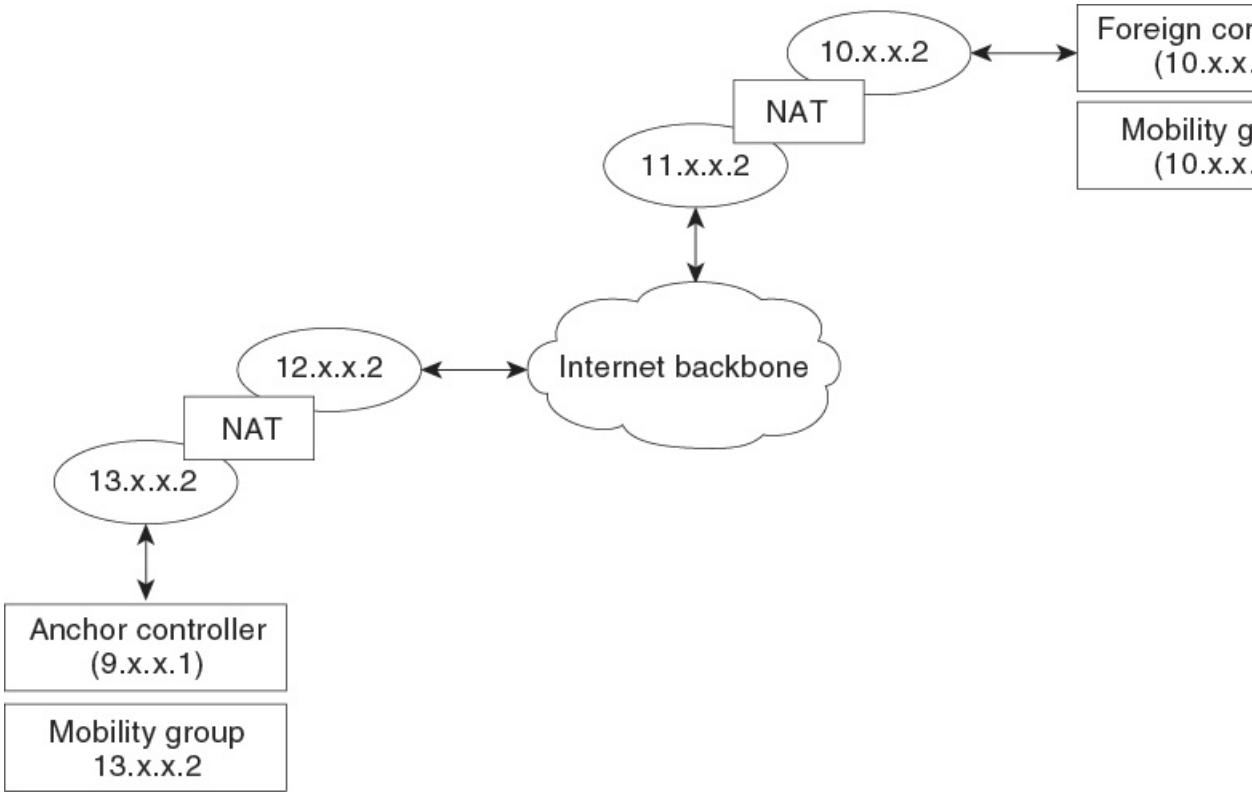
次の図は、1 台の NAT デバイスを使用したモビリティ グループの設定例を示しています。 この例では、すべてのパケットが NAT デバイスを通過します（つまり、送信元から宛先、およびその逆方向に送信されるパケット）。

図 *115*：*1* 台の *NAT* デバイスを使用したモビリティ グループの設定



次の図は、2 台の NAT デバイスを使用したモビリティ グループの設定例を示しています。 この例では、送信元とゲートウェイとの間に 1 台の NAT デバイスを使用し、宛先とゲートウェイとの間にもう 1 台の NAT デバイスを使用しています。

図 *116* : *2* 台の *NAT* デバイスを使用したモビリティ グループの設定



モビリティ グループの設定

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 *45*：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
NTP	UDP ポート 123
SNMP[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） 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す。

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す。
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

以下に類似した情報が表示されます。

```
Symmetric Mobility Tunneling (current) .......... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port........................... 16666
Mobility Security Mode........................... Disabled
Default Mobility Domain.......................... snmp_gui
Multicast Mode .................................. Disabled
Mobility Domain ID for 802.11r................... 0x66bd
Mobility Keepalive Interval...................... 10
Mobility Keepalive Count......................... 3
Mobility Group Members Configured................ 3
Mobility Control Message DSCP Value.............. 0

Controllers configured in the Mobility Group
 MAC Address        IP Address       Group Name  Multicast IP  Status
 00:0b:85:32:42:c0  1.100.163.24     snmp_gui         0.0.0.0          Up
 00:cc:11:ee:1b:10  10.100.100.1        VoWLAN           0.0.0.0       Control and Data Path Down

 11:22:11:33:11:44  1.2.3.4                test       0.0.0.0       Control and Data Path Down
```

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す。 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 [disabled] です。

ステップ 6 （オプション）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**}

モビリティ グループの統計の表示

コントローラの GUI から次の 3 種類のモビリティ グループの統計を表示できます。

- Global Mobility Statistics：すべてのモビリティ トランザクションに影響します。
- Mobility Initiator Statistics：モビリティ イベントを開始するコントローラによって生成されます。
- Mobility Responder Statistics：モビリティ イベントに応答するコントローラによって生成されます。

コントローラの GUI または CLI を使用して、モビリティ グループの統計を表示できます。

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]：ポリシー施行モジュール（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。

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

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い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て使用する場合は、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

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。

以下に類似した情報が表示されます。

```
Mobility Anchor Export List
WLAN ID   IP Address    Status
 1  10.50.234.2    UP
 1  10.50.234.6    UP
 2  10.50.234.2    UP
 2  10.50.234.3    CNTRL_DATA_PATH_DOWN

GLAN ID   IP Address    Status
 1  10.20.100.2    UP
 2  10.20.100.3    UP
```

[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

  以下に類似した情報が表示されます。

```
Mobility Keepalive interval..................... 10
Mobility Keepalive count........................ 3
```

```
Mobility Group members configured..... 3

Controllers configured in the mobility group
MAC Address     IP Address    Group Name    Status
00:0b:85:32:b1:80      10.10.1.1     local    Up
00:0b:85:33:a1:70     10.1.1.2    local    Data Path Down
00:0b:85:23:b2:30     10.20.1.2    local    Up
```

- 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。

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

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およびそれらに対応するセキュリティポリシーのリストを示します。

表 *46*：*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

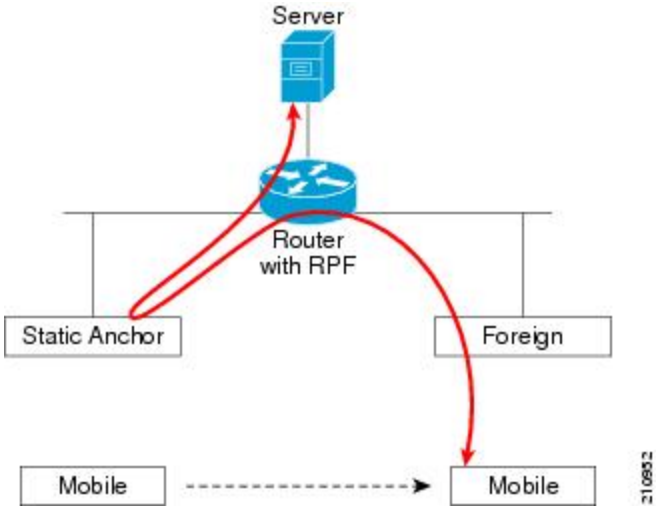
セキュリティの 16 進数値	セキュリティ ポリシー
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed （注） ソフトウェア リリース 6.0 以降を実行しているコントローラは、このセキュリティ ポリシーをサポートしていません。
0x00001000	Security_Web_Passthrough

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

シンメトリックモビリティトンネリングがイネーブルになっている場合、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 *117*：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

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）

コントローラ CLI を使用して、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検証するには、次のコマンドを入力します。

show mobility summary

以下に類似した情報が表示されます。

```
Symmetric Mobility Tunneling (current) ..... Enabled
Symmetric Mobility Tunneling (after reboot) ..... Enabled
Mobility Protocol Port..... 16666
Mobility Security Mode..... Disabled
Default Mobility Domain..... User1
Mobility Keepalive interval..... 10
Mobility Keepalive count..... 3
Mobility Group members configured..... 7

Controllers configured in the Mobility Group
MAC Address           IP Address       Group Name             Status
00:0b:85:32:b0:80    10.28.8.30       User1                    Up
00:0b:85:47:f6:00    10.28.16.10      User1           Up
00:16:9d:ca:d8:e0    10.28.32.10      User1               Up
00:18:73:34:a9:60    10.28.24.10      <local>            Up
00:18:73:36:55:00    10.28.8.10       User1               Up
```

```
00:1a:a1:c1:7c:e0    10.28.32.30      User1                Up
00:d0:2b:fc:90:20       10.28.32.61          User1         Control and Data Path Down
```

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

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。

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

スタティック 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ートを試みることができました。 クライアントが、スタティック 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ートしようとすると、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スタティック 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ー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てもネットワークが処理されるように WLAN を設定できます。

スタティック 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ー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 にアソシエートすると、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 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応答した場合、クライアントのトラフィックはそのコントローラ 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-2 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スタティック 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（スタティック 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（スタティック 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

- スタティック 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 でスタティック 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、スタティック 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。

スタティック 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、スタティック 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。

スタティック 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 上でスタティック 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。

スタティック 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*：スタティック 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

外部マッピングの設定

外部マッピングについて

自動アンカー モビリティ（外部マッピングとも呼ばれる）によって、異なる外部コントローラに存在するユーザがサブネットまたはサブネットのグループから IP アドレスを取得するように設定できます。

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 16 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，971 ページ
- 802.11u Mobility Services Advertisement Protocol の設定，974 ページ
- 802.11u HotSpot の設定，975 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。

a) [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。
b) [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。
c) [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。
d) [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。
e) 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。
f) [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。

a) [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。
b) [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。
c) [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。
d) [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。

a) [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。
b) [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。
c) [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 文字のモバイル国番号を入力します。
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 hotpspot 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。

a) [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。

b) [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。

c) 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。

a) [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。

b) [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。
c) [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。
d) [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。

a) [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。
b) [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。
c) [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。
d) [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。
e) [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 hotpsot 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 hotpsot 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 47：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	• 0：未指定のアセンブリ • 1：アリーナ • 2：スタジアム • 3：乗客ターミナル（たとえば、空港、バス、フェリー、電車の駅） • 4：円形劇場 • 5：アミューズメント パーク • 6：礼拝所 • 7：会議場 • 8：図書館 • 9：博物館 • 10：レストラン • 11：シアター • 12：バー • 13：喫茶店 • 14：動物園または水族館 • 15：緊急対応センター
ビジネス	2	• 0：未指定のビジネス • 1：医師または歯科医師のオフィス • 2：銀行 • 3：消防署 • 4：警察署 • 6：郵便局 • 7：専門家のオフィス • 8：研究および開発施設 • 9：弁護士のオフィス

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	• 0：未指定の教育機関 • 1：小学校 • 2：中学校 • 3：大学
工場および産業	4	• 0：未指定の工場および産業 • 1：工場
機関	5	• 0：未指定の公共機関 • 1：病院 • 2：長期看護施設（療養所、ホスピスなど） • 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 • 4：グループ ホーム • 5：刑務所または拘置所
商業	6	• 0：未指定の商業施設 • 1：小売店 • 2：食料品店 • 3：自動車サービス ステーション • 4：ショッピング モール • 5：ガソリン スタンド
住居	7	• 0：未指定の居住施設 • 1：私邸 • 2：ホテルまたはモーテル • 3：寄宿舎 • 4：宿泊施設
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	• 0：未指定の乗り物 • 1：自動車またはトラック • 2：飛行機 • 3：バス • 4：フェリー • 5：船またはボート • 6：電車 • 7：モーター バイク
アウトドア	11	• 0：未指定のアウトドア • 1：自治体メッシュ ネットワーク • 2：都市公園 • 3：休憩施設 • 4：交通管制施設 • 5：バス停留所 • 6：売店

付 録 A

トラブルシューティング

この付録の内容は、次のとおりです。

- LED の解釈，984 ページ
- システム メッセージ，984 ページ
- システム リソースの表示，988 ページ
- CLI を使用したトラブルシューティング，990 ページ
- システム ロギングとメッセージ ロギングの設定，991 ページ
- アクセス ポイント イベント ログの表示，1000 ページ
- ログとクラッシュ ファイルのアップロード，1001 ページ
- コントローラからのコア ダンプのアップロード，1004 ページ
- パケット キャプチャ ファイルのアップロード，1007 ページ
- メモリ リークの監視，1010 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，1012 ページ
- デバッグ ファシリティの使用方法，1027 ページ
- 無線スニファの設定，1033 ページ
- 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，1037 ページ
- アクセス ポイント監視サービスのデバッグ，1040 ページ
- OfficeExtend アクセス ポイントのトラブルシューティング，1040 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 インストレーション 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 *48*：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。

エラー メッセージ	説明
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。
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。

エラー メッセージ	説明
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。
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。

エラー メッセージ	説明
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。
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 の最大数を超えました。 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。

エラー メッセージ	説明
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。
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。
RADIUS_SERVERS_FAILED	RADIUS とコントローラ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。

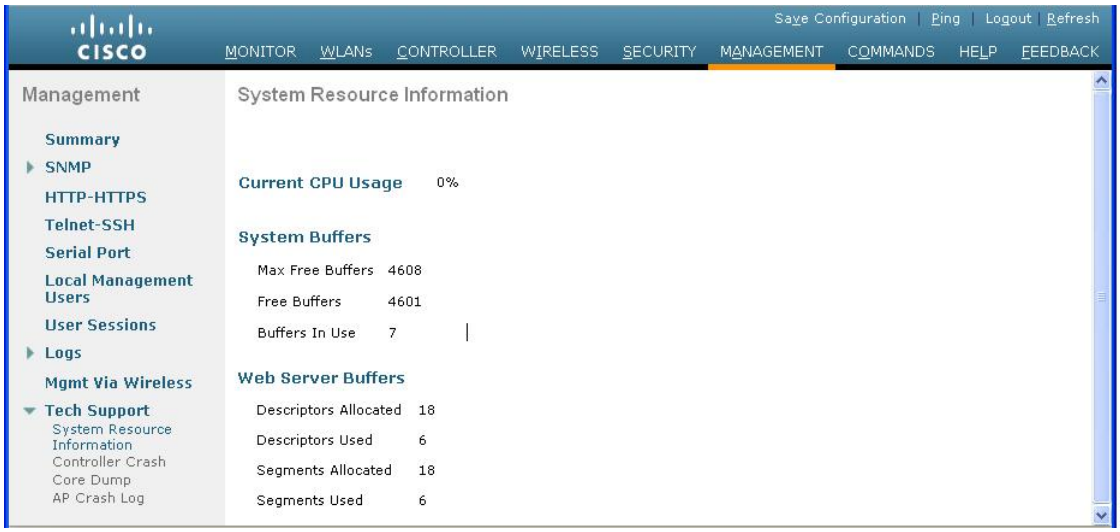
注意事項および制約事項

Cisco 5500 シリーズ コントローラでは、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 *118*：*[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**

  以下に類似した情報が表示されます。

```
Current CPU(s) load: 0%
ndividual CPU load: 0%/0%, 0%/0%, 0%/1%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%, 0%/0%,
0%/0%
```

  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**

  以下に類似した情報が表示されます。

```
System Information
Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 6.0.165.0
...
---------------Show cpu---------------
Current CPU(s) Load.............................. 0%
Individual CPU Load.............................. 0%/3%, 0%/1%, 0%/1%, 0%/1%, 0%/0%,
0%/1%

---------------Show system buffers---------------
```

```
System Buffers
   Max Free Buffers.............................. 4608
   Free Buffers.................................. 4596
   Buffers In Use................................ 12

Web Server Resources
   Descriptors Allocated......................... 259
   Descriptors Used.............................. 4
   Segments Allocated............................ 259
   Segments Used................................. 4

System Resources
   Uptime........................................ 595748 Secs
   Total Ram..................................... 907872 Kbytes
...
```

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。

ステップ 1 **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。以下に類似した情報が表示されます。

```
Name                 Priority         CPU Use            Reaper
 reaperWatcher       ( 3/124)          0 %               (0/0)%   I
 osapiReaper         (10/121)          0 %               (0/0)%   I
 TempStatus          (255/1)           0 %               (0/0)%   I
 emWeb               (255/1)           0 %               (0/0)%   T 300
 cliWebTask          (255/1)           0 %               (0/0)%   I
 UtilTask            (255/1)           0 %               (0/0)%   T 300
```

上の例のフィールドの説明は、次のとおりです。

[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。

ステップ 2 **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。

以下に類似した情報が表示されます。

```
Name                Priority       BytesInUse   BlocksInUse     Reaper
 reaperWatcher      ( 3/124)       0               0           ( 0/0)%   I
 osapiReaper        (10/121)       0               0           ( 0/0)%   I
 TempStatus         (255/1)        308             1           ( 0/0)%   I
 emWeb              (255/1)        294440         4910         ( 0/0)%   T 300
 cliWebTask         (255/1)        738               2         ( 0/0)%   I
 UtilTask           (255/1)        308               1         ( 0/0)%   T 300
```

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。

ステップ 3 **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。

ステップ 4 **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。

ステップ 5 **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

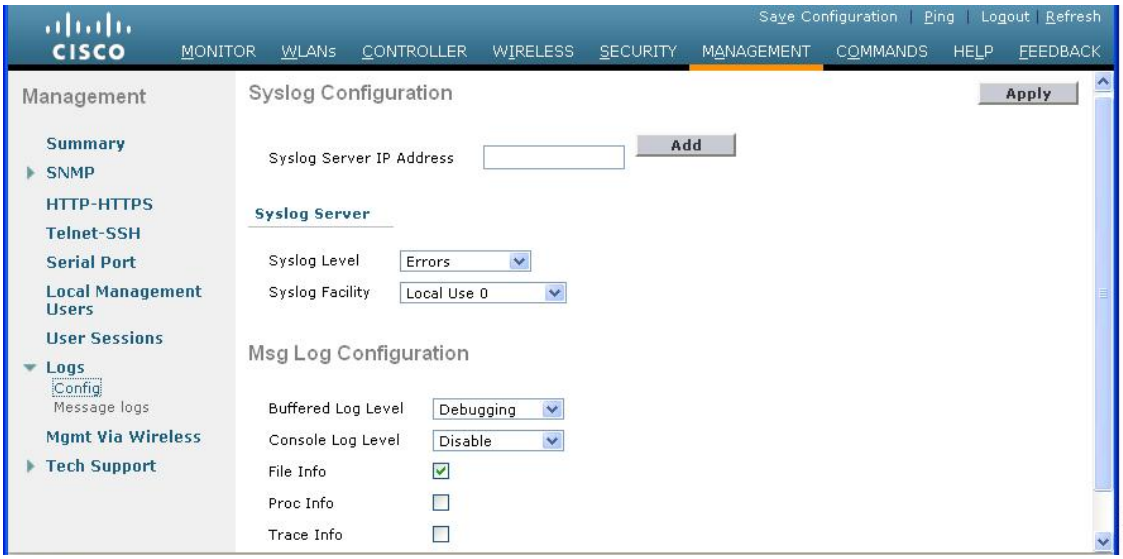
システム ロギングを使用すると、コントローラのシステム イベントを最大 3 台のリモート syslog サーバにログできるようになります。 syslog メッセージはコントローラに設定されている syslog

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がありません。 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 *119*：*[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] をクリックして、変更を確定します。

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ギング 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 ロギングが無効になります。

ロギング 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、ロギング 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。デフォルトではディセーブルになっています。

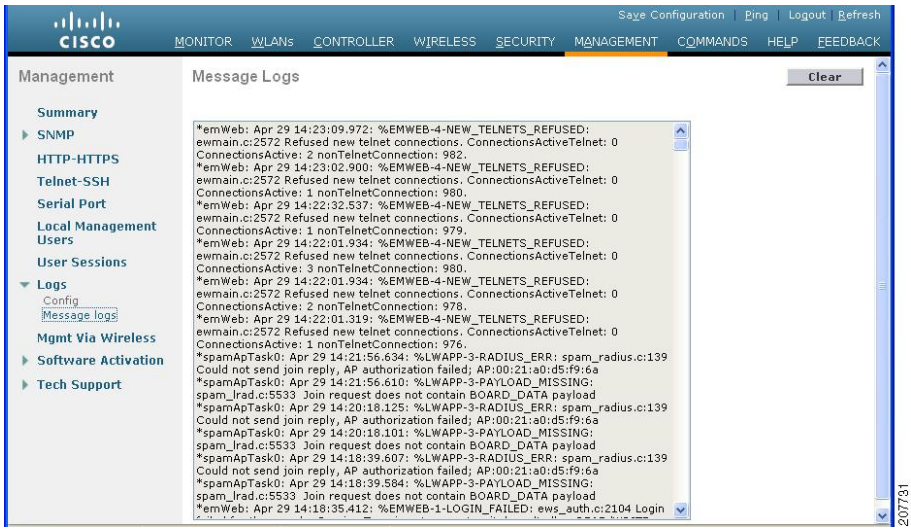
ステップ 9 [Apply] をクリックして、変更を確定します。

ステップ 10 [Save Configuration] をクリックして、変更を保存します。

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 *120*：*[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 ロギングとメッセージ ロギングの設定（CLI）

コントローラ CLI を使用してシステム ロギングとメッセージ ロギングを設定するには、次の手順を実行します。

ステップ 1 システム ロギングを有効化し、syslog メッセージの宛先 syslog サーバの 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 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） コントローラから syslog サーバを削除するには、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 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、次のコマンドを入力します。
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 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するには、次のコマンドを入力します。
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 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するには、次のコマンドを入力します。
config logging syslog facility *facility_code*

facility_code は、次のいずれかです。

- authorization = 認可システム。 ファシリティ レベル = 4。

- auth-private = 認可システム（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） ロギング 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、ロギング 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 デバッグ メッセージをコントローラ バッファ、コントローラ コンソール、または syslog サーバに保存するには、次のコマンドを入力します。

- **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 コントローラがメッセージログ内にプロセス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 procinfo {**enable** | **disable**}

デフォルト値は [disabled] です。

ステップ 9 コントローラがメッセージログ内にトレースバック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 traceinfo {enable | disable}

デフォルト値は [disabled] です。

ステップ 10 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するには、次のコマンドを入力します。

- **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。 768 ビットは、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 変更を保存するには、次のコマンドを入力します。
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

以下に類似した情報が表示されます。

```
Logging to buffer :
- Logging of system messages to buffer :
 - Logging filter level..................... errors
 - Number of system messages logged..... 8716
 - Number of system messages dropped..... 2906
- Logging of debug messages to buffer ..... Disabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
Logging to console :
- Logging of system messages to console :
 - Logging filter level..................... errors
 - Number of system messages logged..... 0
 - Number of system messages dropped..... 11622
- Logging of debug messages to console ..... Enabled
 - Number of debug messages logged..... 0
 - Number of debug messages dropped..... 0
Logging to syslog :
- Syslog facility..... local0
- Logging of system messages to syslog :
 - Logging filter level..... errors
 - Number of system messages logged..... 8716
- Number of debug messages dropped..... 0
- Number of remote syslog hosts..... 0
  - Host 0..... Not Configured
  - Host 1..... Not Configured
  - Host 2..... Not Configured
Logging of traceback..... Disabled
Logging of process information..... Disabled
Logging of source file informational..... Enabled
Timestamping of messages.....
- Timestamping of system messages..... Enabled
 - Timestamp format..... Date and Time
- Timestamping of debug messages..... Enabled
 - Timestamp format..... Date and Time

Logging buffer (8722 logged, 2910 dropped)

*Mar 26 09:23:13.574: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid packet
 from 1.100.163.144. Source member:0.0.0.0. source member unknown.
*Mar 26 09:23:13.574: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid packet
 from 1.100.163.144. Source member:0.0.0.0. source member unknown.
```

```
Previous message occurred 2 times.
*Mar 26 09:22:44.925: %MM-3-INVALID_PKT_RECVD: mm_listen.c:5508 Received an invalid packet
 from 1.100.163.144. Source member:0.0.0.0. source member unknown.
...
```

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

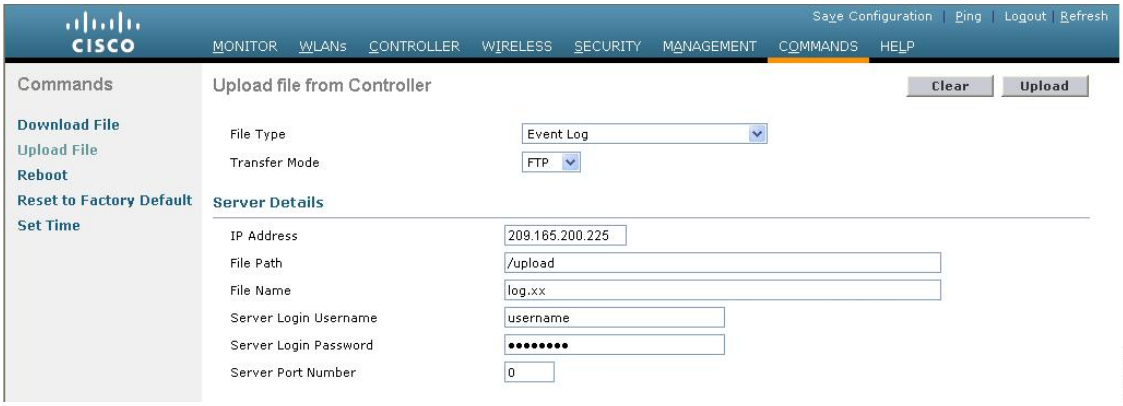
ログとクラッシュ ファイルをアップロードするための前提条件

- 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。
  - サードパーティの TFTP または FTP サーバと WCS 内蔵 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 WCS 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。

図 *121*：*[Upload File from Controller]* ページ



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 リストから、[TFTP] または [FTP] を選択します。

ステップ 4 [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 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 TFTP/FTP 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**}

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ブ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

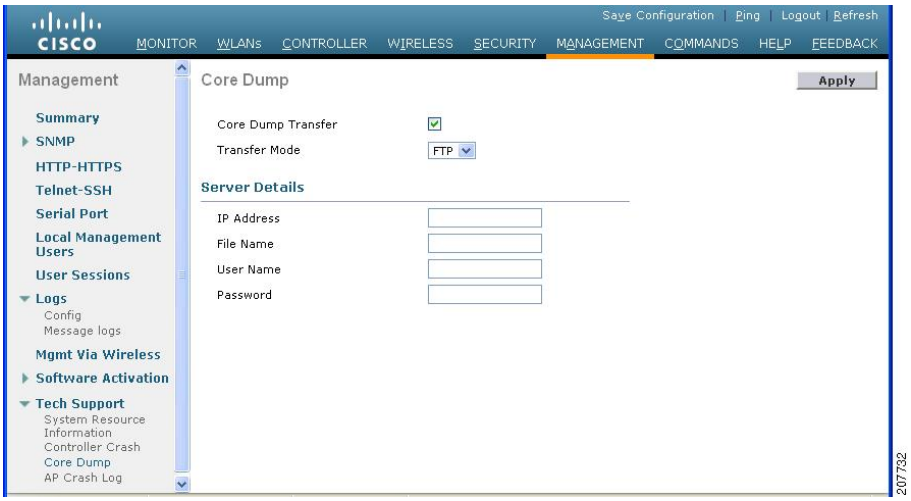
コントローラからのコア ダンプのアップロードについて

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 *122* : *[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TFTPまたはFTP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 TFTP または FTP 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**}
- **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。

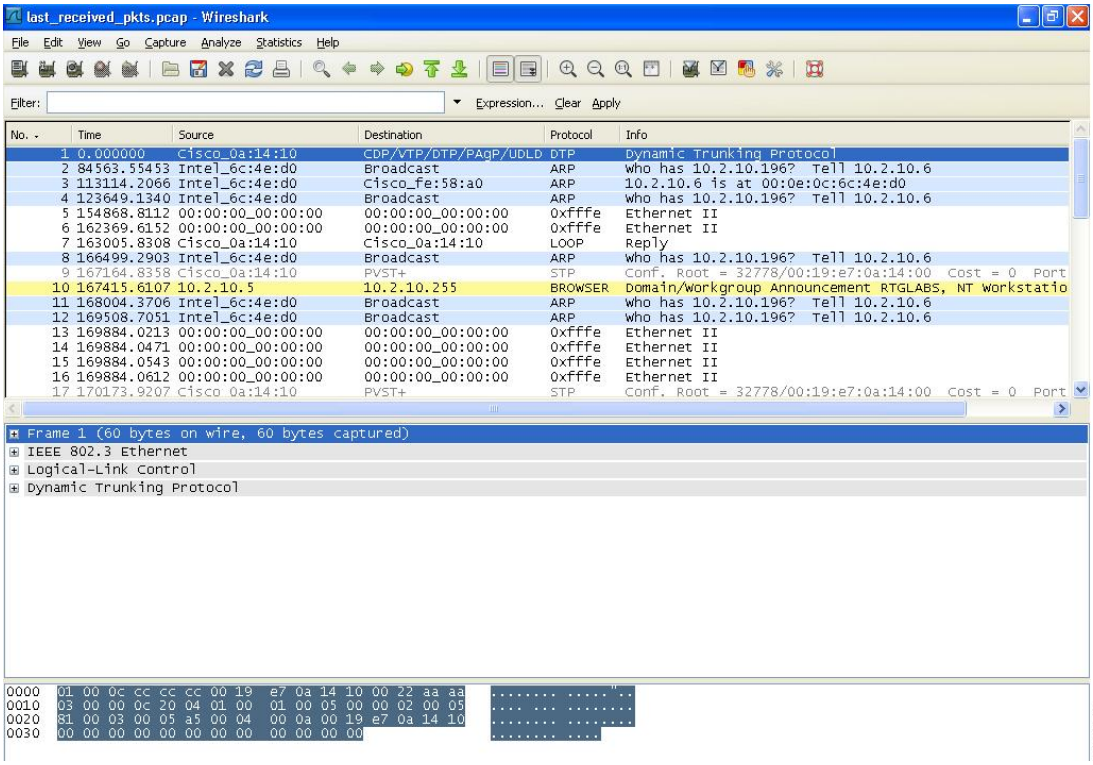
クラッシュが発生すると、新しいパケット キャプチャ ファイル（*.pcap ファイル）が作成され、次のようなメッセージがコントローラ クラッシュ ファイルに出力されます。

```
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。

Wireshark でのパケット キャプチャのサンプル出力

図 *123*：*Wireshark* でのパケット キャプチャ ファイルのサンプル出力



注意事項および制約事項

- 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。
  - サードパーティの TFTP または FTP サーバと WCS 内蔵 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 WCS 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。

図 *124*：*[Upload File from Controller]* ページ

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 リストから、[TFTP] または [FTP] を選択します。

ステップ 4 [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 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**} 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。

```
Mode..................................... TFTP
TFTP Server IP........................... 209.165.200.224
TFTP Path................................ /tftp/user/
TFTP Filename............................ last_received_pkts.pcap
Data Type................................ Packet capture

Are you sure you want to start? (y/N) y

TFTP Packet Capture Dump starting.

File transfer operation completed successfully.
```

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ので、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 [disabled] 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 ceeff00d 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 a1b7cee6 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。

注意事項および制約事項

これらの機能は、CCXv5 クライアントでのみサポートされています。 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。

診断チャネルの設定

診断チャネル機能により、WLAN とのクライアント通信に関する問題のトラブルシューティングが可能になります。 クライアントに発生している通信の問題の原因を特定するために、定義済みのテストのセットを使用してクライアントとアクセス ポイントをテストし、その後、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行うことができます。 診断チャ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 や WCS を使用します。

（注） 診断チャネル機能は、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。

診断チャネルの設定（GUI）

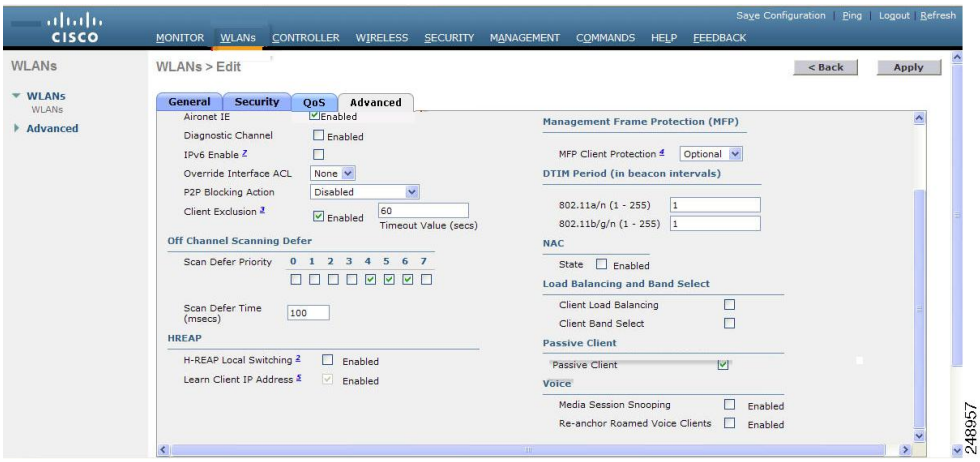
ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

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 *125*：*[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 b0  ............D...
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 30  ............D..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。

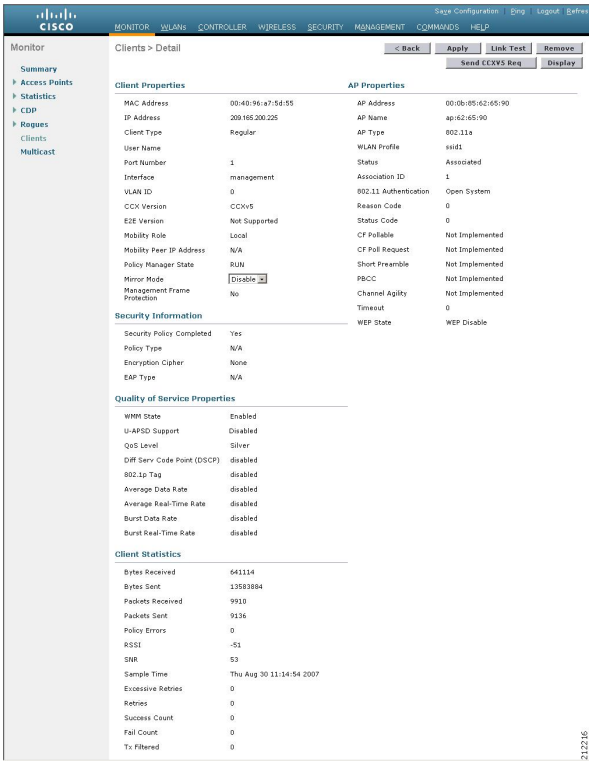
- **クライアント プロファイル**：クライアントの設定に関する情報を示します。
- **動作パラメータ**：クライアントの現在の動作モードの詳細を示します。
- **製造元情報**：使用されている無線 LAN クライアント アダプタに関するデータを示します。
- **クライアント機能**：クライアントの機能に関する情報を示します。

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。

図 *126*：*[Clients > Detail]* ページ

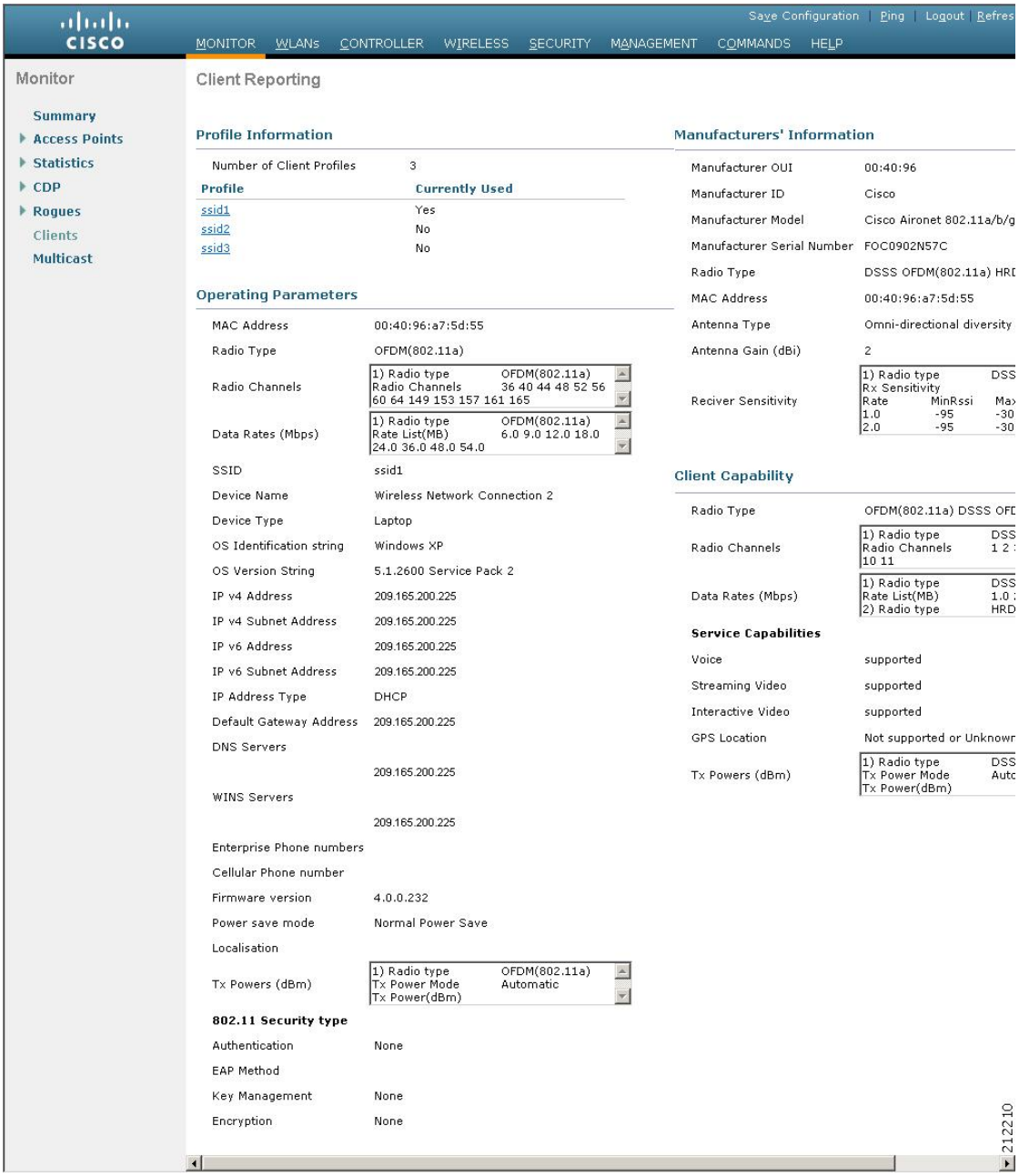


ステップ 3　レポート要求をクライアントに送信するには、[Send CCXV5 Req] をクリックします。

（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。

図 *127*：*[Client Reporting]* ページ



このページには、クライアント プロファイルおよび現在使用中かどうかが表示されます。 クライアントの動作パラメータ、製造元、および機能に関する情報も表示されます。

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*

以下に類似した情報が表示されます。

```
Number of Profiles.............................. 1
Current Profile................................. 1

Profile ID...................................... 1
Profile Name.................................... wifiEAP
SSID............................................ wifiEAP
Security Parameters[EAP Method,Credential]..... EAP-TLS,Host OS Login Credentials
Auth Method..................................... EAP
Key Management................................. WPA2+CCKM
Encryption...................................... AES-CCMP
Power Save Mode................................. Constantly Awake
Radio Configuration:
Radio Type...................................... DSSS
  Preamble Type................................. Long preamble
  CCA Method.................................... Energy Detect + Carrier Detect/Correlation
  Data Retries.................................. 6
  Fragment Threshold............................ 2342
  Radio Channels................................ 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................. Automatic
  Rate List(MB)................................. 1.0 2.0
```

```
Radio Type..................................... HRDSSS(802.11b)
  Preamble Type................................ Long preamble
  CCA Method................................... Energy Detect + Carrier Detect/Correlation
  Data Retries................................. 6
  Fragment Threshold........................... 2342
  Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................ Automatic
  Rate List(MB)................................ 5.5 11.0

Radio Type..................................... ERP(802.11g)
  Preamble Type................................ Long preamble
  CCA Method................................... Energy Detect + Carrier Detect/Correlation
  Data Retries................................. 6
  Fragment Threshold........................... 2342
  Radio Channels............................... 1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................ Automatic
  Rate List(MB)................................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Radio Type..................................... OFDM(802.11a)
  Preamble Type................................ Long preamble
  CCA Method................................... Energy Detect + Carrier Detect/Correlation
  Data Retries................................. 6
  Fragment Threshold........................... 2342
Radio Channels............................... 36 40 44 48 52 56 60 64 149 153 157 161 165
  Tx Power Mode................................ Automatic
  Rate List(MB)................................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

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*

以下に類似した情報が表示されます。

```
Client Mac..................................... 00:40:96:b2:8d:5e
Radio Type..................................... OFDM(802.11a)

Radio Type..................................... OFDM(802.11a)
  Radio Channels............................... 36 40 44 48 52 56 60 64 100 104 108 112 116 120
 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode................................ Automatic
  Rate List(MB)................................ 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Power Save Mode................................ Normal Power Save
SSID........................................... wifi
Security Parameters[EAP Method,Credential]..... None
Auth Method.................................... None
Key Management................................ None
Encryption..................................... None
Device Name.................................... Wireless Network Connection 15
Device Type.................................... 0
OS Id.......................................... Windows XP
OS Version..................................... 5.1.2600 Service Pack 2
IP Type........................................ DHCP address
IPv4 Address................................... Available
IP Address..................................... 70.0.4.66
```

```
Subnet Mask..................................... 255.0.0.0
Default Gateway................................. 70.1.0.1
IPv6 Address.................................... Not Available
IPv6 Address.................................... 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
IPv6 Subnet Mask................................ 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0: 0:
DNS Servers..................................... 103.0.48.0
WINS Servers.....................................
System Name..................................... URAVAL3777
Firmware Version................................ 4.0.0.187
Driver Version.................................. 4.0.0.187
```

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*

以下に類似した情報が表示されます。

```
Manufacturer OUI................................ 00:40:96
Manufacturer ID................................. Cisco
Manufacturer Model.............................. Cisco Aironet 802.11a/b/g Wireless Adapter
Manufacturer Serial............................. FOC1046N3SX
Mac Address..................................... 00:40:96:b2:8d:5e
Radio Type...................................... DSSS OFDM(802.11a) HRDSSS(802.11b) ERP(802.11g)
Antenna Type.................................... Omni-directional diversity
Antenna Gain.................................... 2 dBi

Rx Sensitivity:
Radio Type...................................... DSSS
Rx Sensitivity ................................. Rate:1.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:2.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type...................................... HRDSSS(802.11b)
Rx Sensitivity ................................. Rate:5.5 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:11.0 Mbps, MinRssi:-95, MaxRssi:-30
Radio Type...................................... ERP(802.11g)
Rx Sensitivity ................................. Rate:6.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:9.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:12.0 Mbps, MinRssi:-95, MaxRssi:-30
Rx Sensitivity ................................. Rate:18.0 Mbps, MinRssi:-95, MaxRssi:-30
```

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。

以下に類似した情報が表示されます。

```
Service Capability..............................  Voice, Streaming(uni-directional) Video,
 Interactive(bi-directional) Video
Radio Type.....................................  DSSS OFDM(802.11a) HRDSSS(802.11b)
ERP(802.11g)

Radio Type.....................................  DSSS
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  1.0 2.0

Radio Type.....................................  HRDSSS(802.11b)
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  5.5 11.0

Radio Type.....................................  ERP(802.11g)
  Radio Channels...............................  1 2 3 4 5 6 7 8 9 10 11
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0

Radio Type.....................................  OFDM(802.11a)
  Radio Channels...............................  36 40 44 48 52 56 60 64 100 104 108 112
 116 120 124 128 132 136 140 149 153 157 161 165
  Tx Power Mode................................  Automatic
  Rate List(MB)................................  6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
```

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 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方法

デバッグ ファシリティの使用方法について

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
  - Port
- 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
  - Protocol
  - 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
  - Protocol
  - 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
- Protocol
- 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、eoip-ping、iapp、ip、lwapp、multicast、orphan-from-sta、orphan-to-sta、rbcp、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、rlp、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、qmtp、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 *128*：*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 *129*：*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 ..1n.....@.@..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 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
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
```

232343

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。

注意事項および制約事項

- 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 Airopeek
  - 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

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。

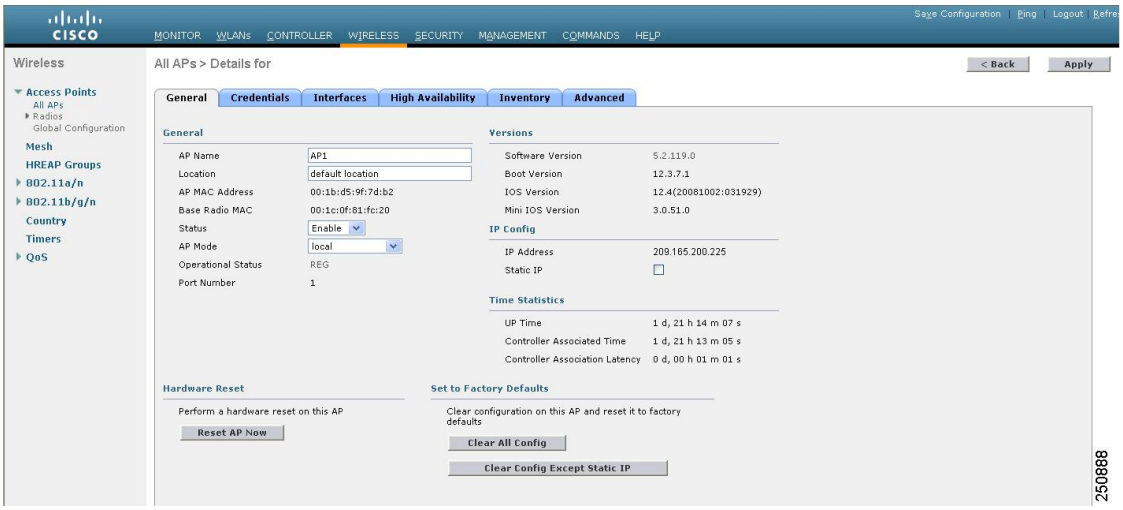
- 専用アクセス ポイント：スニファとして設定されたアクセス ポイントは、そのネットワーク上で無線アクセス サービスを同時に提供できません。 カバレッジの中断を回避するには、既存のワイヤレス ネットワークの一部ではないアクセス ポイントを使用します。
- リモート監視デバイス：アナライザ ソフトウェアを実行できるコンピュータ。
- Windows XP または Linux オペレーティング システム：コントローラは、Windows XP と Linux のいずれのマシンでもスニファをサポートしています。
- ソフトウェアおよび関連ファイル、プラグイン、またはアダプタ：アナライザ ソフトウェアによっては、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

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。

図 *130*：*[All APs > Details for]* ページ



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。

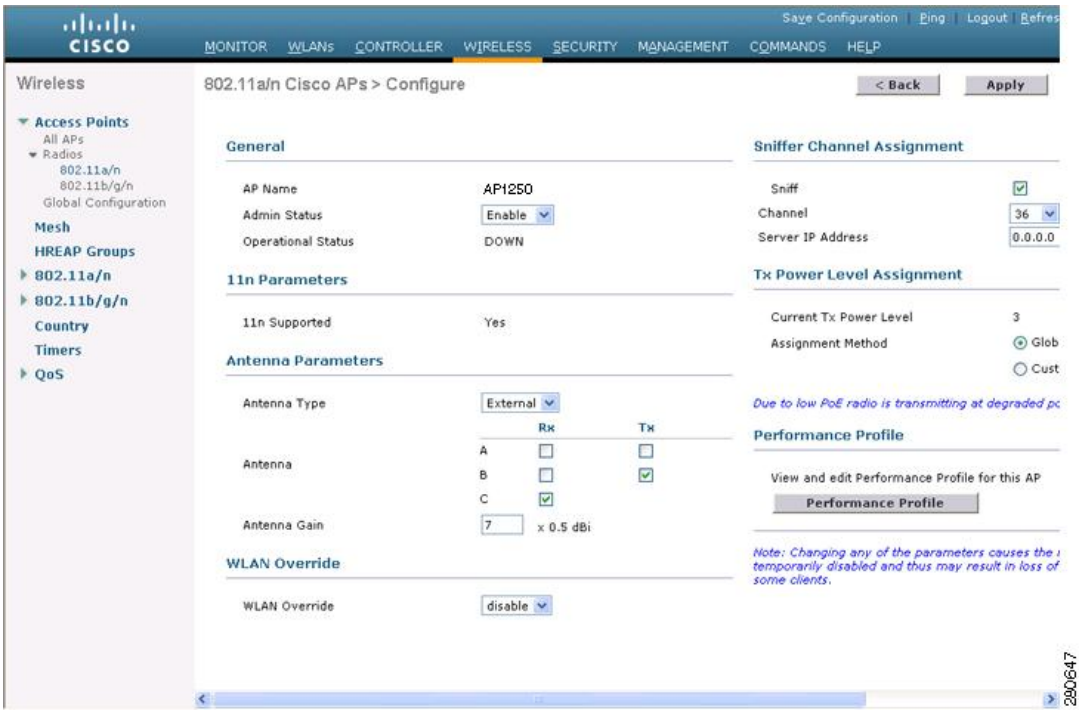
ステップ 4 [Apply] をクリックして、変更を確定します。

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 [Wireless] > [Access Points] > [Radios] > [802.11a/n]（または [802.11b/g/n]）の順に選択して、[802.11a/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（または 802.11b/g/n）Cisco APs > Configure] ページが表示されます。

図 *131*：*[802.11a/n Cisco APs > Configure]* ページ



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。

アクセス ポイントのスニファの設定（CLI）

ステップ 1 アクセス ポイントをスニファとして設定するには、次のコマンドを入力します。
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 アクセス ポイントでスニファを有効にするには、次のコマンドを入力します。
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）と 1（802.11b/g/n）です。
- *server_IP_address* は 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 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 アクセス ポイントのスニファ設定を表示するには、次のコマンドを入力します。
show ap config {**802.11a | 802.11b**} *Cisco_AP*

以下に類似した情報が表示されます。

```
Cisco AP Identifier.............................. 17
Cisco AP Name.................................... AP1131:46f2.98ac
...
AP Mode ......................................... Sniffer
Public Safety ................................... Global: Disabled, Local: Disabled
Sniffing ........................................ No
...
```

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

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」を参照してください。

注意事項および制約事項

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。

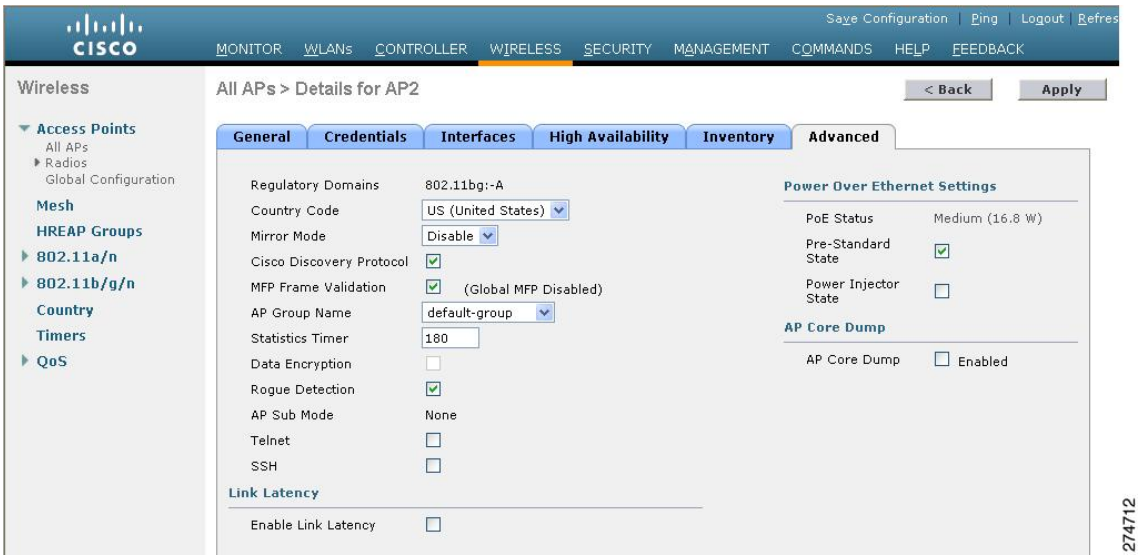
Telnet または SSH を使用したアクセス ポイントのトラブルシューティング（GUI）

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。

図 *132*：*[All APs > Details for]*（*[Advanced]*）ページ



ステップ 4 このアクセス ポイント上での Telnet 接続を有効にするには、[Telnet] チェックボックスをオンにします。デフォルトではオフになっています。

ステップ 5 このアクセス ポイント上での SSH 接続を有効にするには、[SSH] チェックボックスをオンにします。 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。

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 アクセス ポイントで Telnet または SSH の接続を有効にするには、次のコマンドを入力します。
config ap {**telnet | ssh**} **enable** *Cisco_AP*

デフォルト値は [disabled] です。

（注） アクセス ポイントで Telnet または SSH の接続を無効にするには、次のコマンドを入力します。
config ap {**telnet | ssh**} **disable** *Cisco_AP*

ステップ 2 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 3 アクセス ポイントで Telnet または SSH が有効になってい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 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 | nmsp | 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。
- **nmsp**：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

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 WCS 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で、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。

索 引

記号

-J 規制ドメインから -U 規制ドメインへのアクセス ポイントの移動に関する日本の規制 571

数字

11n Mode パラメータ 131
1250 シリーズ アクセス ポイント 588, 589, 591
  PoE を使用する場合の送信電力設定 589
  PoE を使用する場合の動作モード 588
  および [PoE Status] フィールド 591
7920 AP CAC パラメータ 421
7920 Client CAC パラメータ 421
7920 サポート モード 418
  設定 418
  説明 418
7921 サポート モード 419
802.11a/n（4.9 GHz）> Configure ページ 742
802.11a/n Radios ページ（Monitor メニューから） 492
802.11a/n（または 802.11b/g/n）Radios ページ 182, 859
[802.11a > RRM > Dynamic Channel Assignment (DCA)] ページ 837
[802.11a > RRM > General] ページ 843
802.11a（または 802.11b/g）> EDCA Parameters ページ 191
802.11a（または 802.11b/g）Global Parameters ページ 127, 868
802.11a（または 802.11b/g）Network Status パラメータ 127, 134, 135
802.11a（または 802.11b）> Client Roaming ページ 162
802.11a（または 802.11b）> Voice Parameters ページ 177, 180, 188
802.11b/g/n Cisco APs > Configure ページ 1035
802.11g Support パラメータ 127
802.11h Global Parameters ページ 134
802.11h、説明 134
802.11n 130, 595
  クライアント 595
  デバイス 130
802.1Q VLAN トランク ポート 67
802.1X 391, 397
  設定 391
  説明 397
  動的キー設定 391
802.1x Authentication パラメータ 498
802.3 Bridging パラメータ 151
802.3X フロー制御、有効化 150
802.3 ブリッジ 151, 152
  CLI を使用した設定 152
  GUI を使用した設定 151
802.3 フレーム 151

A

Access Control List Name パラメータ 288
Access Control Lists > Edit ページ 290, 925
Access Control Lists > New ページ 288
Access Control Lists ページ 287
Access Mode パラメータ 141, 143
Accounting Server パラメータ 458
ACL。「アクセス コントロール リスト（ACL）」を参照 286, 922
ACL Name パラメータ 290, 291
ACL の設定（GUI） 287
Action パラメータ 290, 925
Add AAA Client ページ（CiscoSecure ACS で） 232, 248
Add AP ボタン 930
Add New Rule ボタン 288
Admin Status パラメータ 85, 86
Admission Control（ACM）パラメータ 177
AES-CCMP 397
Aggregated MAC Service Data Unit（A-MSDU） 133
AirMagnet Enterprise Analyzer 1033

Aironet IE パラメータ 438
Airopeek 1033
All APs > Details for page 1041
[All APs > Access Point Name > Link Details > Neighbor Name] ページ 735
[All APs > Access Point Name > Mesh Neighbor Stats] ページ 735
[All APs > Access Point Name > Neighbor Info] ページ 733
[All APs > Access Point Name > Statistics] ページ 727
All APs > Access Point Name > VLAN Mappings ページ 917
[All APs > Details for]（[Advanced]）ページ 61, 481, 522, 585, 1038
  リンク遅延の設定 585
All APs > Details for（Credentials）ページ 496, 499
[All APs > Details for]（FlexConnect）ページ 916
All APs > Details for（General）ページ 916
[All APs > Details for]（[High Availability]）ページ 557, 561
[All APs > Details for] ページ 1034
All APs > Details ページ 625, 680
[All APs] ページ 487, 726, 733, 865
AnchorTime パラメータ 664, 838
Anonymous Provision パラメータ 271
Antenna Gain パラメータ 859
Antenna Type パラメータ 859
Antenna パラメータ 859
ap-count 評価ライセンス、アクティブ化 117, 118
  CLI の使用 117, 118
  GUI の使用 117
AP > Clients > Traffic Stream Metrics ページ 182
AP801 アクセス ポイント 501, 502
  コントローラで使用 502
  説明 501
AP Authentication Policy ページ 297
AP Core Dump パラメータ 522
AP Ethernet MAC Addresses パラメータ 508
AP Failover Priority パラメータ 561
AP Group Name パラメータ 445
AP Groups > Edit（APs）ページ 445
AP Groups ページ 444, 463
AP Mode パラメータ 540, 865, 916, 1035
AP Name パラメータ 446
AP Primary Discovery Timeout パラメータ 557, 629
AP Sub Mode パラメータ 916
AP マネージャ インターフェイス 73, 83
  および動的インターフェイス 83
  説明 73
AP ローカル認証 921
  GUI の使用 921
Assignment Method パラメータ 860
Authority ID Information パラメータ 271, 931, 933
Authority ID パラメータ 271, 931
Authorize LSC APs against auth-list パラメータ 511
Authorize MIC APs against auth-list or AAA パラメータ 511
AutoInstall 47, 48, 49, 50
  described 50
  取得 48
    TFTP サーバ情報 48
    インターフェイス用の DHCP アドレス 48
  使用 47
  設定ファイルの選択 49
  説明 47
  操作例 50
Average Data Rate パラメータ 167, 170, 416
Average Real-Time Rate パラメータ 167, 171, 417
Avoid Cisco AP Load パラメータ 664, 838
Avoid Foreign AP Interference パラメータ 664, 838, 956
Avoid Non-802.11a（802.11b）Noise パラメータ 665, 838

B

Back-up Primary Controller Name フィールド 557, 629
Back-up Secondary Controller Name パラメータ 557, 630
Backhaul Client Access パラメータ 639, 742
Beacon Period パラメータ 127
Bind Username パラメータ 262
Burst Data Rate パラメータ 167, 170, 416
Burst Real-Time Rate パラメータ 167, 171, 417

C

CAC 180, 181, 183, 418, 698, 708, 710
  7920 電話に対する設定 418
  CLI を使用した表示 183
  イネーブル化 180, 181
    CLI の使用 181
    GUI の使用 180
  メッシュ ネットワーク内の 698
  メッシュ ネットワーク内の表示 708, 710
CA Server URL パラメータ 508
CCKM 399, 927
  FlexConnect グループ 927
  設定 399

CCX 437, 438, 582
Aironet IE の設定 438
CLI の使用 438
クライアントのバージョンの表示 438
GUI の使用 438
説明 437
リンク テスト 582
CCXv5 Req ボタン 1019
CCXv5 クライアント 212
有効化、位置プレゼンスの 212
CCX Version パラメータ 438
CCX 無線管理 867
flexconnect の考慮事項 867
機能 867
CCX レイヤ 2 クライアント ローミング 161, 162, 163, 164
CLI を使用した情報の取得 163
CLI を使用したデバッグ 164
設定 163
CLI の使用 163
説明 161, 162
CDP > AP Neighbors > Detail ページ 199
CDP > Interface Neighbors > Detail ページ 198
CDP > Traffic Metrics ページ 199
CDP Advertisement Version パラメータ 196
CDP AP Neighbors ページ 199
CDP Protocol Status パラメータ 195
CDP State パラメータ 196
Certificate Authority（CA）証明書 268, 272, 771, 772, 774
概要 771
ダウンロード 772, 774
CLI の使用 772, 774
GUI の使用 772
ローカル EAP での使用 268, 272
Certificate File Name パラメータ 792
Certificate File Path パラメータ 792
Certificate Issuer パラメータ 270
Certificate Password パラメータ 769, 792
Certificate Type パラメータ 511
Change Rules Priority パラメータ 321
Channel Announcement パラメータ 134
Channel Assignment Leader パラメータ 839
Channel Assignment Method パラメータ 664, 837
Channel Quiet Mode パラメータ 134
Channel Scan Duration パラメータ 844
Channel Width パラメータ 665, 839
Channel パラメータ 859, 1035
Check Against CA Certificates パラメータ 270
Check Certificate Date Validity パラメータ 270
CIDS Sensor Add ページ 338
CIDS Shun List ページ 339
Cisco 2500 シリーズ コントローラ 8
Cisco 3200 シリーズ モバイル アクセス ルータ
（MAR） 740, 742, 743
説明 740
メッシュ アクセス ポイントで動作 742, 743
CLI を使用した設定 743
GUI を使用した設定 742
Cisco 3200 シリーズ モバイル アクセス ルータで動作 740
説明 740
Cisco 3300 シリーズ Mobility Services Engine（MSE）、wIPS での使用 353
Cisco 5500 シリーズ Wireless LAN Controller 9, 66, 67, 96, 98
説明 9
複数の AP マネージャ インターフェイス 96, 98
ポート 66, 67
Cisco 7921 Wireless IP Phone 419
Cisco Adaptive Wireless Path Protocol（AWPP） 611
Cisco AV ペア 455, 456
Cisco Centralized Key Management（CCKM）。 CCKM を参照 397
Cisco Clean Access（CCA） 460
Cisco CleanAir の設定 879, 881
CLI の使用 881
GUI の使用 879
Cisco Discovery Protocol（CDP） 193, 194, 195, 196, 197, 198, 200
GUI を使用した有効化 196
サポートされるデバイス 194
設定 195, 197, 198
CLI の使用 197, 198
GUI の使用 195, 197
説明 193
トラフィック情報の表示 200
CLI の使用 200
ネイバーの表示 198, 200
CLI の使用 200
GUI の使用 198, 200
Cisco Discovery Protocol パラメータ 196
Cisco License Manager（CLM） 123
およびコントローラ ライセンス エージェント 123
Cisco Licensing Web サイト 119
Cisco Logo パラメータ 797
Cisco Prime Network Control System（NCS） 2
CiscoSecure Access Control Server（ACS） 231

Cisco Unified Wireless Network（UWN）ソリューション 1, 4
説明 1, 4
CleanAir のガイドライン 878
CleanAir の概要 873
Clear Filter リンク 372, 489, 517
Clear Stats on All APs ボタン 517
Clear Stats ボタン 957
CLI 43, 46, 47, 62, 991
使用 43, 47
トラブルシューティング コマンド 991
ナビゲーション 46
ログアウト 46
ログイン 43
ワイヤレス接続の有効化 62
Client Certificate Required パラメータ 270
ClientLink の設定（CLI） 618
Client Protection パラメータ 298
[Client Reporting] ページ 1020
Clients > AP > Traffic Stream Metrics ページ 182
[Clients > Detail] ページ 551, 552, 1019
クライアントの詳細情報の表示 552
クライアント レポートの設定 1019
ワークグループ ブリッジのステータスの表示 551
Client Type パラメータ 551
CLI を使用した FlexConnect AP の設定 920
CLI を使用した電波品質のモニタリング 893
Commands > Reset to Factory Defaults ページ 217
Community Name パラメータ 141
Conditional Web Redirect パラメータ 457
Configuration File Encryption パラメータ 780
Configuration Wizard - 802.11 Configuration ページ 30
Configuration Wizard - Management Interface Configuration ページ 25
Configuration Wizard - Miscellaneous Configuration ページ 26
Configuration Wizard - Service Interface Configuration ページ 23
Configuration Wizard - Set Time ページ 31
Configuration Wizard - SNMP Summary ページ 22, 24
Configuration Wizard - System Information ページ 21
Configuration Wizard - Virtual Interface Configuration ページ 27
Configuration Wizard Completed ページ 32
Configure オプション、RRM の無効化用 859
Control and Provisioning of Wireless Access Points プロトコル（CAPWAP） 478, 479, 483
MTU 情報の表示 483
説明 478
注意事項 479
Control and Provisioning of Wireless Access Points プロトコル（CAPWAP） *(続き)*
デバッグ 483
Controller Time Source Valid パラメータ 297
[Core Dump] ページ 1004
Country Code パラメータ 567
Country ページ 567
Coverage Exception Level per AP パラメータ 841
Coverage Hole Detection Enabled パラメータ 459
CPU、5500 シリーズ コントローラ 988
Custom Signatures ページ 346

D

Data Encryption パラメータ 481, 540
Data Path パラメータ 960
Data Rates パラメータ 127
DCA Channel Sensitivity パラメータ 665, 838
DCA Channels パラメータ 666, 840
Default Mobility Group パラメータ 951
Default Routers パラメータ 380
Description パラメータ 258, 623
Destination Port パラメータ 289, 924
Destination パラメータ 288, 924
Detect and Report Ad-Hoc Networks パラメータ 311
DHCP Addr. Assignment Required パラメータ 377
DHCP proxy 137
configuring 137
using the CLI 137
DHCP Option 82 Remote ID Field Format パラメータ 285
DHCP Parameters ページ 136, 137
DHCP Scopes ページ 379
DHCP Server IP Addr パラメータ 377
DHCP オプション 43、コントローラ ディスカバリ プロセス 485
DHCP オプション 82 284, 285
設定 285
GUI の使用 285
説明 284
例 284
DHCP サーバ 375
内部 375
DHCP スコープ 379
説明 379
DHCP タイムアウト 137
GUI を使用した設定 137

DHCP プロキシ 136
説明 136
Diagnostic Channel パラメータ 1013
Direction パラメータ 289
Diversity パラメータ 860
DNS Domain Name パラメータ 380
DNS IP Address パラメータ 525
DNS Servers パラメータ 380
Domain Name パラメータ 525
Download File to Controller ページ 765, 772, 780, 807
CA 証明書のダウンロード 772
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 807
設定ファイルのダウンロード 780
ログイン バナー ファイルのダウンロード 765
Download SSL Certificate パラメータ 792
[Download] ボタン 769, 772, 808
CA 証明書のダウンロード 772
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 808
デバイスの証明書のダウンロード 769
DSCP パラメータ 289, 925
DTIM 384
DTLS 106
DTLS データ暗号化。 「データ暗号化」を参照 479
DTPC Support パラメータ 127
Dynamic AP Management パラメータ 71, 81
管理インターフェイス 71
動的インターフェイス 81
Dynamic WEP Key Index パラメータ 269

E

EAPOL-Key Max Retries パラメータ 269
EAPOL-Key Timeout パラメータ 269
EAP Profile Name パラメータ 271
EDCA Profile パラメータ 191
Edit QoS Profile ページ 167
Edit QoS Role Data Rates ページ 170
Egress Interface パラメータ 816
Email Input パラメータ 817
Enable AP Local Authentication パラメータ 930
Enable Authentication for Listener パラメータ 124
Enable Check for All Standard and Custom Signatures パラメータ 346
Enable Counters パラメータ 287
Enable Coverage Hole Detection パラメータ 841
Enable CPU ACL パラメータ 291
Enable Default Authentication パラメータ 124
Enable DHCP Proxy パラメータ 136
Enable Dynamic AP Management パラメータ 95
Enable EAP-FAST Authentication パラメータ 931
Enable LEAP Authentication パラメータ 931
Enable Least Latency Controller Join パラメータ 541
Enable Link Latency パラメータ 541, 585
Enable Listener パラメータ 124
Enable Low Latency MAC パラメータ 192
Enable LSC on Controller パラメータ 508
Enable NAT Address パラメータ 71
Enable Notification パラメータ 124
Enable OfficeExtend AP パラメータ 540
Enable Password パラメータ 495
Enable Server Status パラメータ 262
Enable Tracking Optimization パラメータ 577
Encryption Key パラメータ 405
Enhanced Distributed Channel Access（EDCA）パラメータ 192, 193
CLI を使用した設定 192, 193
Enter Saved Permission Ticket File Name パラメータ 120
EoIP ポート 966
epings 967
Expedited Bandwidth パラメータ 177
Expiration Timeout for Rogue AP and Rogue Client Entries パラメータ 311
Extensible Authentication Protocol（EAP; 拡張認証プロトコル） 272, 273, 276
タイムアウトおよび失敗の回数 276
アクセス ポイントごと 276
クライアントごと 276
ローカル タイマーの設定 272, 273

F

Fallback Mode パラメータ 237
File Compression パラメータ 522
File Name to Save Credentials パラメータ 119
File Type パラメータ 751, 758, 760, 765, 769, 772, 775, 778, 780, 807, 1009
CA 証明書のダウンロード 772
PAC のアップロード 775
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 807
コントローラ ソフトウェアのアップグレード 751, 758, 760

File Type パラメータ *(続き)*
設定ファイルのアップロード **778**
設定ファイルのダウンロード **780**
デバイスの証明書のダウンロード **769**
パケット キャプチャ ファイルのアップロード **1009**
ログイン バナー **765**
Fingerprint パラメータ **338**
FlexConnect **902, 904, 906, 915, 920**
帯域幅の制限 **904**
デバッグ **915, 920**
認証プロセス **902, 906**
FlexConnect Mode AP Fast Heartbeat Timeout パラメータ **556**
FlexConnect グループ **926, 927, 928**
CCKM **927**
説明 **926**
バックアップ RADIUS サーバ **927**
ローカル認証 **928**
FlexConnect グループ サポート **929**
Fragmentation Threshold パラメータ **127**
FTP サーバ ガイドライン **747**

G

General（controller）ページ **93, 856**
RF グループの設定 **856**
リンク集約の有効化 **93**
General（security）ページ **256**
General ページ **268**
Generate Rehost Ticket ボタン **120**
Global AP Failover Priority パラメータ **561**
[Global Configuration] ページ **556, 561, 629**
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 **561**
バックアップ コントローラの設定 **556, 629**
Group Mode パラメータ **857, 956**
Group Name パラメータ **930, 952**
Guest LAN パラメータ **816**
Guest User Role パラメータ **257**
Guest User パラメータ **257**
GUI **36, 37**
使用 **36**
注意事項 **36**
ログアウト **37**
ログイン **37**
GUI の使用 **290**
GUI を使用した電波品質のモニタリング **892**

H

Headline パラメータ **797**
hex2pcap 出力例 **1031**
Holdtime パラメータ **196**
HTTP Access パラメータ **38**
[HTTP Configuration] ページ **38**
HTTPS Access パラメータ **38**
Hysteresis パラメータ **162**

I

Identity Request Max Retries パラメータ **269**
Identity Request Timeout パラメータ **269**
IDS シグニチャ **341, 347, 349, 350**
frequency **347**
MAC frequency **347, 349**
Quiet time **347, 350**
説明 **341**
測定間隔 **347**
追跡方法 **347**
パターン **347**
IDS センサー **337**
説明 **337**
IGMP Timeout パラメータ **156**
IGMP スヌーピング **468**
IKE Diffie Hellman Group パラメータ **236**
IKE Phase 1 パラメータ **236**
Index パラメータ、IDS 用 **338**
Infrastructure Protection パラメータ **298**
Ingress Interface パラメータ **816**
Injector Switch MAC Address パラメータ **591**
Install License ボタン **110**
Interface Name パラメータ **445, 462, 463, 623**
[Interfaces > Edit] ページ **95**
複数の AP マネージャ インターフェイスの作成 **95**
Interface パラメータ **377**
Interference threshold パラメータ **843**
Interval パラメータ **664, 838**
Inventory ページ **581**
Invoke Channel Update Now ボタン **664, 837**
Invoke Power Update Now ボタン **833**
IP Mask パラメータ **141**
IPSec パラメータ **236**
IP アドレスと MAC アドレス間のバインディング **164**
設定 **164**
説明 **164**

K

Keep Alive Count パラメータ 960
Keep Alive Interval パラメータ 960
Key Encryption Key（KEK）パラメータ 235
Key Index パラメータ 405
Key Size パラメータ 405
Key Wrap Format パラメータ 235
Key Wrap パラメータ 235

L

LAG Mode on Next Reboot パラメータ 93
Last Auto Channel Assignment パラメータ 839
Layer 2 Security パラメータ 399, 405, 457
Layer 3 Security パラメータ 408, 410, 413, 457, 816
  VPN パススルー 408, 413
  Web 認証 410
  Web リダイレクト 457
  有線ゲスト アクセスの場合 816
LDAP 261, 263
  サーバの優先順位の選択 263
  設定 261, 263
    GUI の使用 261, 263
LDAP Servers パラメータ 271
LDAP Servers ページ 261
LDAP サーバ 263
  WLAN への割り当て 263
Lease Time パラメータ 380
の LED 594, 984
  解釈 984
  設定 594
License Commands ページ 110
License Detail ページ 112, 116
Licenses ページ 111, 116
Lifetime パラメータ 257, 790
lightweight モード、自律モードへの復帰 504
Link Status パラメータ 86
Link Trap パラメータ 86
Listener Message Processing URL パラメータ 124
Lobby Ambassador Guest Management > Guest Users List ページ 790
Local Auth Active Timeout パラメータ 269
Local EAP Authentication パラメータ 271
Local Management Users > New ページ 788
Local Management Users ページ 788
Local Mode AP Fast Heartbeat Timer パラメータ 556
Local Net Users > New ページ 257
Local Significant Certificates（LSC）- AP Provisioning ページ 508
Local Significant Certificates（LSC）- General ページ 508
LWAPP-enabled アクセス ポイント 504, 505, 519, 520, 521, 522, 524
  アップロード 521, 522
    アクセス ポイントのコア ダンプ 522
    無線コア ダンプ 521, 522
  クラッシュ情報のコントローラへの送信 519
  自律モードへの復帰 504, 505
  デバッグ コマンド 519
  無線コア ダンプの取得 520
  リセット ボタンの無効化 524

M

[MAC Filtering] ページ 622
MAC Filters > New ページ 623
MAC Address パラメータ 623
MAC フィルタリング 382, 384
  WLAN の設定 382, 384
Management Frame Protection パラメータ 297
Management IP Address パラメータ 540
Master Controller Configuration ページ 485
Master Controller Mode パラメータ 485
Max-Login Ignore Identity Response パラメータ 269
Max HTTP Message Size パラメータ 124
Maximum Local Database Entries パラメータ 256
Maximum Number of Sessions パラメータ 124
Max RF Bandwidth パラメータ 177, 180
MCS データ レート 131
Member MAC Address パラメータ 952
[Mesh > LinkTest Results] ページ 734
Message Authentication Code Key（MACK）パラメータ 235
[Message Logs] ページ 995
Message パラメータ、Web 認証用 797
Metrics Collection パラメータ 178
MFP Client Protection パラメータ 297
MIC 403
Min Failed Client Count per AP パラメータ 841
Minimum RSSI パラメータ 162
MMH MIC 405, 406
  設定 405, 406
Mobility Anchor Create ボタン 960
Mobility Anchors オプション 960

Mobility Services Engine 207
コントローラとの同期化 207
MODE access point ボタン 524
Mode パラメータ 162, 868
mpings 967
Multicast Groups ページ 158
Multicast ページ 156

N

NAC State パラメータ 445, 463
NAC アウトオブバンド統合 460, 462
図 460
注意事項 462
NAC アウトオブバンドのサポート 463, 464
特定のアクセス ポイント グループに対する設定 463, 464
CLI の使用 464
GUI の使用 463
NAC インバンド モード 462
Native VLAN ID パラメータ 916
NAT アドレス 71, 73, 81, 82
管理インターフェイス 71, 73
動的インターフェイス 81, 82
Neighbor Information オプション 733
Neighbor Packet Frequency パラメータ 844
Netbios Name Servers パラメータ 380
Netmask パラメータ 380
Network Mobility Services Protocol（NMSP） 204, 212, 213, 215, 216
クライアント、RFID タグ、および不正デバイスの通知間隔の変更 212
設定の表示 213, 215
デバッグ 216
Network パラメータ 380
NTP サーバ 51
日時を取得するための設定 51
Number of Attempts to LSC パラメータ 508
Number of Hits パラメータ 290

O

OEAP のトラブルシューティング 1040
OfficeExtend AP パラメータ 541
OfficeExtend アクセス ポイント 527, 528, 538, 539, 541, 546, 547, 1041
の LED 1041
一般的なセットアップ 528
および NAT 528
サポートされるアクセス ポイント モデル 528
設定 539, 541, 546
GUI の使用 539, 541
個人 SSID 546
説明 527
統計情報の表示 547
配置 1041
ファイアウォールの要件 538
OfficeExtend アクセス ポイントの [Home] ページ 545
Order Used for Authentication パラメータ 237, 251
Over-ride Global Credentials パラメータ 496, 499, 541
Override Global Config パラメータ 810, 817
Override Interface ACL パラメータ 291

P

P2P Blocking パラメータ 389
Params パラメータ 508
Password パラメータ 257, 495, 498, 775
PAC 775
アクセス ポイント認証の 498
アクセス ポイントの 495
ローカル ネット ユーザ 257
path loss measurement（S60）、CLI コマンド 208
PEAP パラメータ 270
Personal SSID パラメータ 546
Physical Mode パラメータ 85
Physical Status パラメータ 86
ping テスト 966
ping リンク テスト 582
PMKID キャッシュ 401
PMK キャッシュ ライフタイム タイマー 401
PoE Status パラメータ 590
Pool End Address パラメータ 379
Pool Start Address パラメータ 379
Port Number パラメータ 85, 235, 251, 262, 816
LDAP サーバ 262
RADIUS サーバ 235
TACACS+ サーバ 251
コントローラ 85
有線ゲスト アクセスの場合 816
Ports ページ 85

Port パラメータ、IDS 用 338
Power Injector Selection パラメータ 591
Power Injector State パラメータ 591
Power Neighbor Count パラメータ 834
Power Over Ethernet（PoE）パラメータ 86
Power over Ethernet（PoE） 15, 590, 592
　設定 590, 592
　　CLI の使用 592
　　GUI の使用 590, 592
　説明 15
Power Threshold パラメータ 834
Preauthentication ACL パラメータ 292, 457
Primary Controller のパラメータ 557, 630
Primary RADIUS Server パラメータ 930
Priority Order > Local-Auth ページ 268
Priority Order > Management User ページ 237, 251
Privacy Protocol パラメータ 143
Profile Name パラメータ 369, 440, 474, 623, 816
Protected Access Credential（PAC） 268, 774, 775, 776, 931
　アップロード 775, 776
　　CLI の使用 775, 776
　　GUI の使用 775
　概要 774
　ローカル EAP での使用 268, 931
Protection Type パラメータ 297, 865
Protocol Type パラメータ 168
Protocol パラメータ 288, 924
PSK 397
　説明 397
PSK Format パラメータ 399
Public Key Cryptography（PKC）、モビリティを使用 947

Q

QBSS 418
QoS 166, 415
　レベル 166, 415
QoS プロファイル 166, 168, 169
　設定 166, 168, 169
　　CLI の使用 168, 169
　　GUI の使用 166, 168
QoS ロール 169, 171
　設定 169, 171
　　CLI の使用 171
　　GUI の使用 169, 171
Quality of Service（QoS）パラメータ 416
Quarantine パラメータ 80, 462
　NAC アウトオブバンド統合 462
　動的インターフェイス 80
Query Interval パラメータ 338

R

Radio Resource Management（RRM） 663, 666, 829, 833, 836, 840, 841, 844, 851, 855, 858, 859, 864, 867
　CCX の機能。「CCX 無線管理」を参照 867
　RRM の無効化 858
　Wireless > 802.11a/n（または 802.11b/g/n）> RRM > TPC パラメータ 833
　カバレッジ ホールの検出 829, 841
　　GUI を使用したコントローラごとの設定 841
　　説明 829
　更新間隔 855, 858
　設定 844
　　GUI を使用した監視間隔 844
　チャネルおよび送信電力設定の静的割り当て 859
　　GUI の使用 859
　チャネルおよび電力の動的割り当ての無効化 864
　　CLI の使用 864
　チャネルの指定 663, 666, 836, 840
　デバッグ 851
Radio Resource Management（RRM）の設定 849
　CLI を使用した表示 849
RADIUS 231, 232, 238, 240, 927
　ACS での設定 231, 232
　FIPS 標準 238
　FlexConnect の使用方法 927
　KEK パラメータ 238
　MACK パラメータ 238
　サーバのフォール バック動作 240
RADIUS 認証属性 241, 244
Range（RootAP to MeshAP）パラメータ 638
Re-sync ボタン 339
Redirect URL After Login パラメータ 797
Refresh-time Interval パラメータ 196
Regenerate Certificate ボタン 792
Rehost Ticket File Name パラメータ 120
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 230
Request Max Retries パラメータ 269
Request Timeout パラメータ 269
Reserved Roaming Bandwidth パラメータ 177
Reset Link Latency ボタン 585

Reset Personal SSID パラメータ 540
RF-Network Name パラメータ 856
RF Channel Assignment パラメータ 864
RFID タグ 203, 207
　説明 203
　追跡 207
　　CLI を使用したデバッグ 207
RF グループ 853, 854, 855, 856, 857
　概要 853, 855
　カスケード 854
　固定 854
　ステータスの表示 857
　　CLI の使用 857
　　GUI の使用 857
　ステータスの表示 857
　　GUI の使用 857
　設定 856
　　GUI の使用 856
RF グループの設定 832
　CLI の使用 832
RF グループ名 855
　説明 855
RF グループ モードの設定 831
　GUI の使用 831
RF グループ リーダー 853, 854
　説明 853, 854
RLDP。「Rogue Location Discovery Protocol（RLDP）」を参照 309
Rogue Detection パラメータ 311, 540
Rogue Location Discovery Protocol パラメータ 311
Rogue Policies ページ 311
Role Name パラメータ 170
Role パラメータ 258
RRM。「Radio Resource Management（RRM）」を参照 825
RSNA ログ 1024, 1025
　設定 1025
　説明 1024

S

Save and Reboot ボタン 772
Save Licenses ボタン 110
Scan Threshold パラメータ 163
Scope Name パラメータ 379
SE-Connect 898
Search AP ウィンドウ 493, 517
Search WLANs ウィンドウ 372, 487
Secondary Controller のパラメータ 557, 630
Secondary RADIUS Server パラメータ 930
Security Mode パラメータ 640
Select APs from Current Controller パラメータ 930
Sequence パラメータ 288, 923
Server Address パラメータ 338
Server Index（Priority）パラメータ 235, 251, 262
Server IP Address パラメータ 235, 251, 262, 1035
　LDAP サーバ 262
　RADIUS サーバ 235
　TACACS+ サーバ 251
　無線スニファ用 1035
Server Key パラメータ 271, 931
Server Status パラメータ 235, 251
Server Timeout パラメータ 235, 251, 263
Set Priority ボタン 116
Set to Factory Default ボタン 844
Severity Level Filtering パラメータ 992
Shared Secret Format パラメータ 235, 251
Shared Secret パラメータ 235, 251
Short Preamble Enabled パラメータ 277
Signature Events Summary ページ 348
Sniff パラメータ 1035
SNMP v1 / v2c Community ページ 141
SNMP V3 Users ページ 143
SNMP v3 ユーザ 142, 143
　GUI を使用したデフォルト値の変更 142, 143
SNMP エンジン ID 140
SNMP、設定 140
Source パラメータ、ACL 288, 924
SpectraLink NetLink 電話 277
　概要 277
Spectrum Expert 898
Spectrum Expert の設定 897
Splash Page Web Redirect パラメータ 457
SSH 58, 60, 540, 542, 1037
　アクセス ポイントのトラブルシューティング 60, 1037
　　GUI の使用 60, 1037
　および OfficeExtend アクセス ポイント 540, 542
　設定 58, 60
　　CLI の使用 58, 60
SSH パラメータ 61, 1038
SSID 366, 369, 370
　設定 369, 370
　　CLI の使用 370
　　GUI の使用 369
　説明 366

SSLv2、Web 管理の設定 39
SSL 認証 40, 41, 42
ロード 40, 41, 42
CLI の使用 42
GUI の使用 40, 41
SSL プロトコル 37
State パラメータ 338, 347
Static IP パラメータ 525
Statistics オプション 727
Status パラメータ 141, 370, 380, 440, 474, 816
DHCP スコープ 380
SNMP コミュニティの 141
WLAN 370, 440, 474
ゲスト LAN の場合 816
[Summary] ページ 58
Switch IP Address（Anchor）パラメータ 960
SX/LC/T Small Form-Factor Plug-in（SFP）モジュール 67
Symmetric Mobility Tunneling Mode パラメータ 965
syslog 1025, 1026
説明 1025
ログ 1025, 1026
[Syslog Configuration] ページ 992
Syslog Facility パラメータ 993
Syslog Server IP Address パラメータ 992
Syslog サーバ 992
コントローラからの削除 992
重大度レベルのフィルタリング 992
[System Resource Information] ページ 989

T

TACACS+ 245, 246, 249, 252
アカウンティング 246
許可 246
設定 252
GUI の使用 252
説明 245
認証 246
ロール 249
TACACS+（Authentication, Authorization, or Accounting）Servers > New ページ 251
TACACS+（Authentication, Authorization, or Accounting）Servers ページ 250
TACACS+ Administration .csv ページ（CiscoSecure ACS で） 254, 255
TCP MSS 587
説明 587
Telnet 60, 61, 1037, 1038, 1039
アクセス ポイントのトラブルシューティング 60, 61, 1037, 1038, 1039
CLI の使用 61, 1039
GUI の使用 60, 61, 1037, 1038
[Telnet-SSH Configuration] ページ 57
Telnet セッション 56, 58
設定 56, 58
GUI の使用 56, 58
Telnet パラメータ 61, 1038
Tertiary Controller のパラメータ 557, 630
text2pcap 出力例 1032
Time Length Value（TLV）、CDP のサポート 193, 194
Time to Live for the PAC パラメータ 271, 931
Traffic Specifications（TSPEC）要求 174
例 174
Traffic Stream Metrics（TSM） 176, 182, 183, 184, 185
説明 176
統計情報の表示 182, 183, 184, 185
CLI の使用 184, 185
GUI の使用 182, 183
Transfer Mode パラメータ 751, 758, 760, 769, 772, 775, 778, 780, 807, 1009
CA 証明書のダウンロード 772
PAC のアップロード 775
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 807
コントローラ ソフトウェアのアップグレード 751, 758, 760
設定ファイルのアップロード 778
設定ファイルのダウンロード 780
デバイスの証明書のダウンロード 769
パケット キャプチャ ファイルのアップロード 1009
Transition Time パラメータ 163
Trap Logs ページ 423
Tx Power Level Assignment パラメータ 864
Type パラメータ 369, 440, 474, 816

U

U-APSD 175, 182, 183
ステータスの表示 182, 183
CLI の使用 183
GUI の使用 182
説明 175
UDP、RADIUS での使用 230
UDP ポート 966

Unique Device Identifier（UDI） 580, 581
取得 581
CLI の使用 581
GUI の使用 581
説明 580
Upload CSV File パラメータ 931
[Upload File from Controller] ページ 521, 775, 778, 1002, 1009
Upload ボタン 346, 775, 1002, 1009
URL to Send the Notifications パラメータ 124
USB コンソール ポート、5500 シリーズ コントローラ 88, 89
Use AES Key Wrap パラメータ 234
user accounts, managing 809
User Access Mode パラメータ 789
User Attribute パラメータ 263
User Base DN パラメータ 262
User Credentials パラメータ 263
Username パラメータ 495, 498, 499
User Name パラメータ 257
User Object Type パラメータ 263
User Profile Name パラメータ 143
User パラメータ 775

V

Validate Rogue Clients Against AAA パラメータ 311
Validity パラメータ 775
VCI 文字列 513
Verify Certificate CN Identity パラメータ 270
VLANs 79, 85
説明 79
注意事項 85
VLAN Identifier パラメータ 74, 80, 81
AP マネージャ インターフェイス 74
動的インターフェイス 80, 81
VLAN ID パラメータ 462, 917
VLAN Select 98
voice-over-IP（VoIP）による通話ローミング 160
Voice RSSI パラメータ 841
VoIP Snooping and Reporting パラメータ 423
VoIP コール、エラー コード 427
VoIP スヌーピング 422
説明 422
VPN Gateway Address パラメータ 408
VPN パススルー 408, 414
GUI を使用した設定 414
説明 408

W

webauth.tar ファイル 810
webauth bundle 806
Web Authentication Type パラメータ 797, 804, 808
Web Auth Type パラメータ 810, 817
Web Policy パラメータ 292, 457
Web Session Timeout パラメータ 38
Web 認証 409, 792, 794, 796
WLAN の設定 409
GUI の使用 409
certificate 792
GUI を使用して取得 792
処理 796
説明 794
ログイン成功ページ 796
SSLv2、Web 認証の、無効 797
Web 認証ログイン ページ 795, 797, 798, 800, 803, 804, 808
外部 Web サーバからのカスタマイズ 804
GUI の使用 804
デフォルト 795
デフォルトの選択 798, 800
CLI の使用 798, 800
プレビュー 797, 808
変更されたデフォルトの例 803
Web ブラウザ セキュリティ警告 794
Web モード 37
説明 37
Web リダイレクトの設定（GUI） 457
Web Login ページ 804
WEP キー、設定 390
WGB Wired Clients ページ 551
WGB パラメータ 551
WLAN 5, 369, 370, 371, 391, 406, 440, 475, 921
イネーブル化またはディセーブル化 370, 371
CLI の使用 371
GUI の使用 370
クライアントを接続 921
削除 369, 371
CLI の使用 371
GUI の使用 369
作成 440, 475
GUI の使用 440, 475
セキュリティ設定の確認 391
セッション タイムアウト 406
説明 406
有線セキュリティ ソリューション 5
WLAN ID パラメータ 369, 440, 474

WLAN Profile パラメータ 258
[WLANs > Edit]（[Advanced]）ページ 459, 1013
診断チャネルの設定 1013
[WLANs > Edit]（[Security] > [AAA Servers]）ページ 458, 811
WLAN のアカウンティング サーバの無効化 458
外部認証に対して RADIUS または LDAP サーバを選択 811
[WLANs > Edit]（[Security] > [Layer 3]）ページ 457
Web リダイレクトの設定 457
WLANs > Edit ページ 369, 440, 474, 816
WLAN SSID パラメータ 445, 463, 790
WLAN へのアクセス ポイント グループのマップ 445, 463
ゲスト ユーザの設定 790
WLANs ページ 369, 370, 373, 439, 474, 960
WLAN オーバーライド 746
WLAN 上の AP ローカル認証 921
CLI の使用 921
WLAN 上のローカル認証 920
GUI の使用 920
WLAN でのカバレッジ ホール検出の設定（GUI） 459
WLAN への ACL の適用 291
WLAN モビリティ セキュリティ値 963
WMM 173, 418, 420, 421
CAC を使用 173
設定 420, 421
説明 418
WMM パラメータ 191, 192
WPA2 Policy パラメータ 399
wplus ライセンス。 ライセンス 106
wplus ライセンス。 「ライセンス」を参照 107

あ

アクセス コントロール リスト（ACL） 287, 288, 292, 293, 294, 923, 1028
WLAN への適用 294
CLI の使用 294
カウンタ 288, 293
CLI を使用した設定 293
GUI を使用した設定 288
コントローラの CPU への適用 293
CLI の使用 293
設定 292, 293
CLI の使用 292, 293
デバッグ ファシリティでの使用 1028
アクセス コントロール リスト（ACL） *(続き)*
ルール 287, 293, 923
アクセス ポイント 161, 485, 501, 505, 506, 507, 511, 517, 518, 527, 594, 695, 984
join 情報の表示 517, 518
GUI の使用 517, 518
の LED 594, 984
解釈 984
設定 594
アクセス ポイントとコントローラの join の確認 485
許可リスト 511
組み込み 501
経由ローミング 161
経由ローミング、説明 695
サイズの大きなイメージのサポート 527
認可 505, 506, 507
LSC の使用 507
MIC の使用 506
SSC の使用 505
プライミング 485
アクセス ポイント グループ 445, 446, 447, 448
アクセス ポイントの割り当て 446, 447
CLI の使用 447
GUI の使用 446
削除 445, 446
CLI の使用 446
GUI の使用 445
作成 446, 447
CLI の使用 446, 447
表示 447, 448
アクセス ポイントでの RFID トラッキング、最適化 577, 578
GUI の使用 577, 578
アクセス ポイントの -J 規制ドメインから -U 規制ドメインへの移行 571, 574
アクセス ポイントの 802.1X 認証 497, 499, 500, 501
設定 499, 500, 501
CLI の使用 499, 500
スイッチ 501
説明 497
アクセス ポイントの MAC アドレス 524
コントローラ GUI に表示された 524
アクセス ポイントのイベント ログ、表示 1000
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 108

アクセス ポイントのグローバル クレデンシャル 494, 495, 496
説明 494
無効化 495, 496
CLI の使用 496
GUI の使用 495
アクセス ポイントのコア ダンプ、アップロード 522
GUI の使用 522
アクセス ポイントのスニファの設定 1034
GUI の使用 1034
アクセス ポイントのフェールオーバー プライオリティ 560, 561, 562
CLI を使用した表示 562
設定 561
CLI の使用 561
設定 561
GUI の使用 561
説明 560
アクセス ポイント無線、検索 492, 493
アクセス ポイント モニタ サービス、デバッグ 1040
暗号 398, 399, 400
設定 399, 400
説明 398

い

イーサネット VLAN タギングの設定（GUI） 680
イーサネット接続、リモートで使用 45
意図的な悪用 364
イベント報告、MFP に対する 296
イメージのプレダウンロード 755
インターネット グループ管理プロトコル（IGMP） 153, 156, 157
スヌーピング 153
設定 156, 157
CLI の使用 157
GUI の使用 156
インターフェイス 68, 79
概要 68, 79
インターフェイス グループ 99
インフラストラクチャ MFP 295
コンポーネント 295
インライン パワー 588

え

エンドユーザ ライセンス契約（EULA） 110, 111

お

屋内アクセス ポイント 736
メッシュ アクセス ポイントへの変換 736
オペレーティング システム 4, 5
セキュリティ 4, 5
ソフトウェア 4
音声情報、メッシュ ネットワークについて CLI を使用して表示 707
音声設定 178
設定 178
GUI の使用 178
オンライン ヘルプ、使用 36

か

回避クライアント 337
説明 337
拡張ネイバー リスト 161, 695
説明 161, 695
要求（E2E） 161
隔離 VLAN 71, 80, 463, 906, 912
FlexConnect を使用 906
NAC アウトオブバンド統合で 463
使用 912
設定 71, 80
virtual interface 76
説明 76
カバレッジ ホールの検出 459, 841, 842, 848
WLAN 上の無効化 459
説明 459
コントローラごとの設定 841, 842, 848
CLI の使用 848
GUI の使用 841, 842
カバレッジ ホールの検出と修正 829
監視間隔、GUI を使用した設定 844
干渉 828, 874
管理インターフェイス 70
説明 70
管理者アクセス権 137
管理フレーム検証 295

管理フレーム保護（MFP） 294
タイプ 294

き

キー置換 403, 405, 406
設定 405, 406
説明 403
キャパシティ Adder ライセンス。「ライセンス」を参照 106

く

国番号 565, 569
CLI を使用した表示 569
説明 565
国番号の設定（CLI） 568
国番号の設定（GUI） 566
クライアント 438, 439, 595, 597, 921
CCX バージョンの表示 438, 439
CLI の使用 439
GUI の使用 438
WLAN への接続 921
表示 595, 597
CLI の使用 597
GUI の使用 595, 597
クライアント MFP 295
クライアント除外ポリシーの設定（CLI） 300
クライアント除外ポリシーの設定（GUI） 299
クライアント レポート 1018
説明 1018
クライアント ローミング、設定 159, 164
クライアント ロケーション、Prime Infrastructure の使用 7
クラッシュ ファイル 1003
アップロード 1003
CLI の使用 1003

け

ゲスト WLAN、作成 791
ゲスト ユーザ アカウント 791
表示 791
CLI の使用 791
GUI の使用 791

こ

コア ダンプ ファイル 1004, 1007
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 1007
説明 1004
工場出荷時設定 217
GUI を使用したリセット 217
高速 SSID 変更 150
GUI を使用した設定 150
高速ハートビート タイマー 555, 556, 558
設定 556, 558
CLI の使用 558
GUI の使用 556
説明 555
コントローラ 2, 3, 6, 7, 484, 752, 754, 782
概要 6
シングルコントローラ展開 2
設定 782
保存 782
ソフトウェアのアップグレード 752, 754
CLI の使用 754
GUI の使用 752
ディスカバリ プロセス 484
プラットフォーム 7
マルチ コントローラ展開 3
コントローラ CPU への ACL の適用 291
コントローラ間ローミング 160, 942
説明 160
例 942
コントローラ内ローミング 159, 941
図示 941
説明 159
コントローラのシリアル番号、検索 119, 121
コントローラの設定（GUI） 21
コントローラの役割 874
コントローラのリセット 785
コンフィギュレーション ファイル 779, 780, 784
ダウンロード 779, 780
GUI の使用 779, 780
編集 784

さ

サービス ポート 68

サービス ポート インターフェイス 72, 77, 78
設定 72, 77
GUI の使用 72, 77
説明 78
最大ローカル データベース エントリ 255
GUI を使用した設定 255
サブネット間モビリティ 947
サブネット間ローミング 160, 944
図示 944
説明 160
サポートされたブラウザ 36

し

時刻、設定 51
NTP サーバの使用 51
自己署名証明書（SSC） 505
アクセス ポイントの認可に使用 505
システム メッセージ 984
システム リソース 988, 989
CLI を使用した表示 989
GUI を使用した表示 988
システム ロギング 991, 995
設定 991, 995
CLI の使用 995
GUI の使用 991
システム ログ、CLI を使用した表示 999
事前認証アクセス コントロール リスト（ACL） 294, 804, 912
WLAN への適用 294
CLI の使用 294
外部 Web サーバの 804, 912
失敗した Voice over IP（VoIP）コールのエラー コード 427
自動アンカー モビリティ 958, 960
概要 958
設定 960
GUI の使用 960
集約方法、指定 132
条件付き Web リダイレクト 455
説明 455
診断チャネル 1013, 1014
設定 1014
GUI の使用 1014
説明 1013
シンメトリック モビリティ トンネリング 964, 965
概要 964
シンメトリック モビリティ トンネリング (続き)
図示 964
ステータスの確認 965
CLI の使用 965

す

固定 IP アドレス 525
設定 525
GUI の使用 525
説明 525
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 967
設定 967
スタティック IP クライアントのダイナミック アンカーの設定 969
CLI の使用 969
GUI の使用 969
ステートフル DHCPv6 IP アドレス指定 433
スニファ。「無線スニファ」を参照 1033

せ

製品認証キー（PAK） 108, 109
登録 109
ライセンスのアップグレードの入手 108
セキュリティ 228
概要 228
セキュリティ設定 637
ローカルおよび外部認証 637
設定ウィザード 20, 33
CLI バージョン 33
説明 20
設定の保存 782

そ

送信電力 860, 861
CLI を使用した静的割り当て 861
GUI を使用した静的割り当て 860
送信電力のしきい値、減少 845
送信電力の動的制御、設定 127
送信電力レベル 860
ソフトウェア、アップグレード 745, 750, 752
CLI の使用 752

ソフトウェア、アップグレード *(続き)*
GUI の使用 **750**
注意事項 **745**

た

帯域幅ベースの CAC **173, 177, 179, 698**
イネーブル化 **177, 179**
CLI の使用 **179**
GUI の使用 **177**
説明 **173**
メッシュ ネットワーク用 **698**
耐障害性 **907**
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 **998**
タイムゾーン **53, 54**
CLI を使用した設定 **54**
GUI を使用した設定 **53**
ダイレクトされたローミング要求 **161**

ち

チョークポイント、RFID タグ追跡用 **204**

て

ディスカバリ要求タイマー、設定 **558, 631**
ディストリビューション システム ポート **67**
データの暗号化 **482, 542**
および OfficeExtend アクセス ポイント **542**
設定 **482**
CLI の使用 **482**
GUI の使用 **482**
デバイス証明書 **768, 769**
概要 **768**
ダウンロード **768, 769**
GUI の使用 **768, 769**
デバッグ コマンド、送信 **519**
デバッグ ファシリティ **1027, 1029**
説明 **1027, 1029**
デバッグ ファシリティの設定 **1030**
デフォルトグループ アクセス ポイント グループ **444**
デフォルトのイネーブル パスワード **494**

と

動的 AP 管理 **72, 82**
管理インターフェイス **72**
動的インターフェイス **82**
動的 AP マネージャ インターフェイス **83**
動的インターフェイスの例 **97**
動的周波数選択 **575, 576**
動的チャネル割り当て（DCA） **665, 827, 829, 839, 840, 846, 848**
20 MHz チャネライゼーション **829**
40 MHz チャネライゼーション **839**
感度のしきい値 **665**
設定 **840, 846, 848**
CLI の使用 **846, 848**
GUI の使用 **840**
説明 **827**
ドメイン ネーム サーバ（DNS）ディスカバリ **485**
トラップ ログ **539**
OfficeExtend アクセス ポイントの **539**
トラブルシューティング **514, 519, 990, 1012**
CCXv5 クライアント **1012**
アクセス ポイント join プロセス **514, 519**
問題 **990**
トンネル属性、Identity ネットワーキング **305**

に

日本の国番号 **571**
認証されたローカル認証バインド方式 **262, 264**

ね

ネイバー情報 **733, 735**
CLI を使用したアクセス ポイントの表示 **735**
GUI を使用したアクセス ポイントの表示 **733**
ネイバー ディスカバリ パケット **852**
ネイバー統計 **735**
CLI を使用したアクセス ポイントの表示 **735**
GUI を使用したアクセス ポイントの表示 **735**

は

パケット キャプチャ ファイル **1007, 1008, 1010**
Wireshark でのサンプル出力 **1008**

パケット キャプチャ ファイル *(続き)*
アップロード 1010
CLI の使用 1010
説明 1007
パスワード 991
クリア テキストでの表示 991
パスワードのガイドライン 499
バックアップ コントローラ 555, 627, 631
設定 631
GUI の使用 631
説明 555, 627
パッシブ クライアント 465

ひ

ピアツーピア ブロック 387
説明 387
日付 51
NTP サーバでの設定 51
ビデオ情報、メッシュ ネットワークについて CLI を使用して表示 707
評価ライセンス 107
5500 シリーズ コントローラにインストールされた 107

ふ

ファイル転送 15
フィルタ、クライアントの表示用 596
フェールオーバーの保護 16, 17
負荷ベース CAC 173, 174, 177
イネーブル化 177
GUI の使用 177
説明 173, 174
複数の AP マネージャ インターフェイスの作成（CLI） 96
複数の AP マネージャ インターフェイスの作成（GUI） 95
複数の国番号 567, 568
設定 567, 568
CLI の使用 568
GUI の使用 567
不正なアクセス ポイント 312, 314, 865
アラーム 865
自動的な阻止 312, 314
CLI の使用 314
GUI の使用 312
不正の検出 313, 542
および OfficeExtend アクセス ポイント 542
不正の状態 318
プレダウンロードのガイドラインおよび制限事項 756
プローブ要求、説明 579

ほ

ポート 85
設定 85
ポートのミラーリング、設定 86, 87

ま

マルチキャスト VLAN 102
GUI の使用 102
マルチキャスト クライアント テーブル、表示 159
マルチキャスト最適化 102
マルチキャスト モード 152, 154, 155
説明 152, 154
注意事項 155

み

ミラーモード。「ポートのミラーリング、設定」を参照 86

む

無効なクライアント、タイムアウトの設定 383
無線コア ダンプ 520, 521
アップロード 521
GUI の使用 521
説明 520
無線スニファ 1033, 1034, 1035
サポート対象のソフトウェア 1033
設定 1035
GUI の使用 1035
前提条件 1034
無線測定要求 867, 868, 869
CLI を使用した状態の表示 869
概要 867
設定 868, 869
CLI で 869
GUI で 868

無線による管理 282
説明 282
無線リソースの監視 826

め

メッシュ 637, 642, 657, 708, 725, 731, 732
統計情報 725, 731, 732
CLI を使用したアクセス ポイントの表示 731, 732
GUI を使用したアクセス ポイントの表示 725, 731
ネットワークの例 708
パラメータ 637, 642, 657
CLI を使用した設定 657
GUI を使用した設定 637, 642
メッシュ アクセス ポイント 602, 603, 604, 611, 739, 740
および CAPWAP 611
ネットワーク アクセス 604
非メッシュ アクセス ポイントへの変換 739
モデル 602
ロール 603
メッシュ ネイバー、親、および子 611
メッシュ ルーティング 611
メッセージのログ 991, 995, 999
設定 991
GUI の使用 991
表示 995, 999
CLI の使用 999
GUI の使用 995
メモリ 16
タイプ 16
メモリ リーク、モニタ 1010, 1011

も

モニタリング 892
モビリティ 941
概要 941
モビリティ ping テスト、実行 966
モビリティ アンカー。「自動アンカー モビリティ」を参照 958
モビリティ グループ 853, 945, 947, 948, 949
NAT デバイスでの使用 949
RF グループとの違い 853
図示 945
モビリティ グループ (続き)
設定 948
1 台の NAT デバイスの使用 948
内部でのメッセージング 947
モビリティ グループの NAT デバイス 947
モビリティ グループの統計 955
タイプ 955

ゆ

有線ゲスト アクセス 813, 814
設定の概要 814
説明 813, 814
1 つのコントローラの例 814
ユニキャスト モード 152

ら

ライセンス 108, 109, 110, 111, 112, 118, 119, 120, 122
RMA 後の交換コントローラへの転送 122
SKU 109
インストール 110, 111
CLI の使用 111
GUI の使用 110
再ホスト 118, 119, 120
GUI の使用 119, 120
説明 118
削除 111, 112
CLI の使用 111
GUI の使用 112
取得 108, 110
表示 112
CLI の使用 112
保存 110, 111
CLI の使用 111
GUI の使用 110
ライセンス エージェント 123
説明 123
ライセンスの再ホスト。「ライセンス」を参照 119

り

リリース間モビリティ 950
リンク集約（LAG） 90, 91
図示 91

リンク集約（LAG） *(続き)*
説明 **90, 91**
リンク遅延 **543, 584**
および OfficeExtend アクセス ポイント **543**
説明 **584**
リンク テスト **581, 583, 733, 734, 735**
ウィンドウ **734**
オプション **583, 734**
実施 **583, 733, 735**
CLI の使用 **583**
GUI の使用 **583, 733, 735**
パケットのタイプ **581**
ボタン **583**

れ

レイヤ 2 **5**
動作 **5**
レイヤ 3 **5, 229**
セキュリティ **229**
説明 **229**
動作 **5**

ろ

ローカル EAP **267, 275, 276**
CLI を使用した情報の表示 **275**
デバッグ **276**
例 **267**
ローカルで有効な証明書（LSC） **507, 508**
設定 **507, 508**
GUI の使用 **507, 508**
説明 **507**
ローカル認証、ローカル スイッチング **903**
ローカル ユーザ データベース、キャパシティ **788**
ローミング診断とリアルタイム診断 **1024, 1025**
説明 **1024**
ローミング診断とリアルタイム診断 *(続き)*
ログ **1024, 1025**
説明 **1024**
表示 **1025**
ローミング理由レポート **161**
ローミング理由レポート、説明 **695**
ログ **1002, 1003, 1025**
RSNA **1025**
アップロード **1002, 1003**
CLI の使用 **1003**
GUI の使用 **1002**
ログイン バナー ファイル **764, 765, 766, 767**
クリア **767**
説明 **764**
ダウンロード **765, 766**
CLI の使用 **766**
GUI の使用 **765, 766**
ロケーション **208, 210, 868**
CLI を使用した設定 **208, 210**
CLI を使用した設定の表示 **210**
調整 **868**

わ

ワークグループ ブリッジ（WGB） **528, 540, 545, 546, 547, 548, 551, 552**
図示 **528, 540, 545, 546, 548**
ステータスの表示 **551, 552**
CLI の使用 **552**
GUI の使用 **551, 552**
設定例 **551**
説明 **547**
デバッグ **552**
ワールド モード **127, 129**
ワイヤレス侵入防御システム（wIPS） **352**
説明 **352**