ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

エクスプレス セットアップ

デバイスを簡単な構成で手早くセットアップするには、基本操作に必要な設定をすべてこのページで入力します。基本設定の変更や更新が必要なときは、[エクスプレス セットアップ] ページで必要な項目を簡単に見つけることができます。

無線の設定

無線ネットワークでの役割

ネットワークでのデバイスの役割を選択します。

[アクセス ポイント ルート] によって、クライアントはルータに直接関連付けることができます。

無線ネットワークを最適化する

ここでは、無線の事前設定またはカスタム設定を選択できます。[スループット] を選択すると、デバイスが扱うデータ量が最大化されますが、範囲が狭くなる可能性があります。データ レートはすべて基本に設定されています。[範囲] を選択すると、デバイスの範囲が最大化されますが、スループットが低下する可能性があります。最低のデータ レートは [Required] に、その他のデータ レートは [有効] に設定されています。802.11a 無線では、[デフォルト] オプションを選択することによって、データ レートをデフォルト値に設定することもできます。

[カスタム] リンクをクリックすると、[Network Interfaces-Radio 802.11a/b/g Setting] ページが表示され、各種のパラメータを設定できます。

注: 802.11g アクセス ポイント無線を、最適なスループットが得られるように構成すると、802.11g のすべてのデータ レートが基本レート (必須) に設定されます。この設定では 802.11b クライアント デバイスからの関連付けがブロックされます。

Aironet 拡張機能

Cisco Aironet 802.11 拡張機能を使用するには [有効にする] を選択します。負荷分散、MIC (Message Integrity Check)、TKIP (Temporal Key Integrity Protocol) などの機能を使用するには、これを [有効にする] に設定する必要があります。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

エクスプレス セキュリティ セットアップ:

[エクスプレス セキュリティ] ページではセキュリティの基本設定を構成します。これらのページでは一意の SSID を作成し、3 つのセキュリティ タイプのいずれかを割り当てます。詳細なセキュリティ設定は、Web ブラウザ インターフェイスのメインの [セキュリティ] ページで構成します。[エクスプレス セキュリティ] ページは基本構成を簡単に行うためのページであるため、設定できるオプションはアクセス ポイントのセキュリティ機能の一部のみです。[エクスプレス セキュリティ] ページで扱う設定の範囲は『Cisco IOS Software Configuration Guide』に説明されています。

ブリッジング接続またはルーティング接続を構成できます。

[ブリッジング]。ブリッジング接続の基本セキュリティ設定を構成するページです。ブリッジング接続は BVI (Bridge-Group Virtual Interface) を使用して、すべての無線インターフェイスからのトラフィックを 1 つのサブネットワークに統合します。この種類の接続には、SDM または IOS CLI を使用してブリッジ グループを作成し、BVI インターフェイスに IP アドレスを指定する必要があります。

[ルーティング]。ルーティング接続の基本セキュリティを構成するページです。このページではルーティング接続の基本セキュリティを設定します。ルーティング接続では、個々の無線インターフェイスに別々のネットワークを作成し、トラフィックを各ネットワークにルーティングできます。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

エクスプレス セキュリティ セットアップ: ブリッジング

このページではブリッジング接続の基本セキュリティを設定します。ブリッジング接続は BVI (Bridge-Group Virtual Interface) を使用して、すべての無線インターフェイスからのトラフィックを 1 つのサブネットワークに統合します。[エクスプレス セキュリティ] ページは簡単な基本設定を行うために用意されたものなので、設定できるオプションはアクセス ポイントのセキュリティ機能の一部のみです。[エクスプレス セキュリティ] ページで扱う設定の範囲は『Cisco IOS Software Configuration Guide』に説明されています。

この接続には、SDM または IOS CLI を使用して BVI インターフェイスと IP アドレスを作成する必要があります。

SSID

アクセス ポイントの設定が出荷時のデフォルト値になっている場合は、[エクスプレス セキュリティ] ページで最初に作成した SSID によって、デフォルトの SSID (アクセス ポイントでは tsunami) が上書きされます。デフォルトの SSID にはセキュリティ設定はありません。作成した SSID はページの下部の SSID テーブルに表示されます。アクセス ポイントには最大 16 の SSID を作成できます。

ビーコンで **SSID** をブロードキャストする

この設定はデバイスがルート AP モードのときにのみアクティブになります。SSID をブロードキャストすると、SSID が指定されていないデバイスをアクセス ポイントに関連付けることができます。このオプションは、ゲストや公共の場所のクライアント デバイスが SSID を使用する場合に便利です。SSID をブロードキャストしないと、クライアント デバイスは、自分の SSID とこの SSID が一致しない限り、アクセス ポイントへの関連付けができません。ビーコンには SSID を 1 つだけ含めることができます。

VLAN

ワイヤレス LAN で VLAN を使用し、VLAN に SSID を割り当てる場合、4 種類のセキュリティ設定のいずれかを使用して、[エクスプレス セキュリティ] ページで複数の SSID を作成できます。ただし、ワイヤレス LAN で VLAN を使用しない場合、SSID に割り当て可能なセキュリティ オプションは制限されます。これは、[エクスプレス セキュリティ] ページでは暗号化の設定と認証タイプがリンクされているためです。VLAN を使用しないと、暗号化の設定 (WEP および Cipher) は 2.4-GHz 無線などのインターフェイスに適用され、1 つのインターフェイスに複数の暗号化設定を使用できなくなります。

ネイティブ VLAN のブリッジ グループ番号を入力する場合、ブリッジ グループ番号は SDM で設定されているものと一致している必要があります。

セキュリティ

SSID に割り当て可能なセキュリティの種類は 4 つあります。

- **[セキュリティなし]** - これは最も低いセキュリティのオプションです。これは公共の場所で使用する SSID にのみ使用すべきオプションで、その場合はネットワークへのアクセスを制限する VLAN に SSID を割り当てます。
- **[スタティック WEP キー]** - これは [セキュリティなし] より高いセキュリティのオプションです。ただし、スタティック WEP キーは攻撃を受けやすいキーです。このオプションを構成する場合、アクセス ポイントへの関連付けを MAC アドレスに基づいて制限することを考慮する必要があります。また、RADIUS サーバを使用しないネットワークでは、アクセス ポイントをローカル認証サーバとして使用することを考慮してください。このセキュリティ機能では強制 WEP が有効になります。アクセス ポイントのキーに一致する WEP キーがないと、クライアント デバイスはこの SSID を使用して関連付けすることができません。
- **[EAP 認証]** - このオプションでは 802.1x 認証 (LEAP、PEAP、EAP-TLS、EAP-GTC、EAP-SIM など) が有効になり、ネットワーク上の認証サーバ (サーバ認証ポート 1645) について IP アドレスと共有シークレット キーを入力する必要があります。802.1x 認証によってダイナミック暗号化キーが提供されるので、WEP キーを入力する必要はありません。このセキュリティ機能では強制 802.1x 認証が有効になります。この SSID を使用して関連付けを行うクライアント デバイスは、802.1 認証を実行する必要があります。
- **[WPA]** - WPA (Wi-Fi Protected Access) は認証サーバのサービスによってデータベースを照会して認証されたユーザへのワイヤレス アクセスを許可し、次に IP トラフィックが WEP で使用されるものより強力なアルゴリズムによって暗号化されます。EAP 認証と同様に、ネットワーク上の認証サーバ (サーバ認証ポート 1645) について、IP アドレスと共有シークレット キーを入力する必要があります。このセキュリティ機能では強制 WPA 認証が有効になります。この SSID を使用して関連付けを行うクライアント デバイスは、WPA に対応している必要があります。

SSID テーブル

この表には、SSID とそれに関連付けられている VLAN、暗号化、認証、およびキー管理のオプションが表示されます。

関連トピック: [エクスプレス セキュリティ] ページの使用

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

エクスプレス セキュリティ セットアップ: ルーティング

このページではルーティング接続の基本セキュリティを設定します。ルーティング接続では、個々の無線インターフェイスに別々のネットワークを作成し、トラフィックを各ネットワークにルーティングできます。[エクスプレス セキュリティ] ページは簡単な基本構成を行うために用意されたものなので、設定できるオプションはアクセス ポイントのセキュリティ機能の一部のみです。[エクスプレス セキュリティ] ページで扱う設定の範囲は『Cisco IOS Software Configuration Guide』に説明されています。

SSID

アクセス ポイントの設定が出荷時のデフォルト値になっている場合は、[エクスプレス セキュリティ] ページで最初に作成した SSID によって、デフォルトの SSID (アクセス ポイントでは tsunami) が上書きされます。デフォルトの SSID にはセキュリティ設定はありません。作成した SSID はページの下部の SSID テーブルに表示されます。アクセス ポイントには最大 16 の SSID を作成できます。

ビーコンで **SSID** をブロードキャストする

この設定はデバイスがルート AP モードのときにのみアクティブになります。SSID をブロードキャストすると、SSID が指定されていないデバイスをルート アクセス ポイントに関連付けることができます。このオプションは、ゲストや公共の場所のクライアント デバイスが SSID を使用する場合に便利です。SSID をブロードキャストしないと、クライアント デバイスは、自分の SSID とこの SSID が一致しない限り、アクセス ポイントへの関連付けができません。ビーコンに含めることができる SSID は、1 つだけです。

VLAN

ワイヤレス LAN で VLAN を使用し、VLAN に SSID を割り当てる場合、4 種類のセキュリティ設定のいずれかを使用して、[エクスプレス セキュリティ] ページで複数の SSID を作成できます。ただし、ワイヤレス LAN で VLAN を使用しない場合、SSID に割り当て可能なセキュリティ オプションは制限されます。これは、[エクスプレス セキュリティ] ページでは暗号化の設定と認証タイプがリンクされているためです。VLAN を使用しないと、暗号化の設定 (WEP および Cipher) は 2.4-GHz 無線などのインターフェイスに適用され、1 つのインターフェイスに複数の暗号化設定を使用できなくなります。

IP プロトコル

ルーティングを行う無線インターフェイスに IP アドレスを割り当てる必要があります。

セキュリティ

SSID に割り当て可能なセキュリティの種類は 4 つあります。

- **[セキュリティなし]** - これは最も低いセキュリティのオプションです。これは公共の場所で使用する SSID にのみ使用すべきオプションで、その場合はネットワークへのアクセスを制限する VLAN に SSID を割り当てます。
- **[スタティック WEP キー]** - これは [セキュリティなし] より高いセキュリティのオプションです。ただし、スタティック WEP キーは攻撃を受けやすいキーです。このオプションを構成する場合、アクセス ポイントへの関連付けを MAC アドレスに基づいて制限することを考慮する必要があります。また、RADIUS サーバを使用しないネットワークでは、アクセス ポイントをローカル認証サーバとして使用することを考慮してください。このセキュリティ機能では強制 WEP が有効になります。アクセス ポイントのキーに一致する WEP キーがないと、クライアント デバイスはこの SSID を使用して関連付けすることができません。
- **[EAP 認証]** - このオプションでは 802.1x 認証 (LEAP、PEAP、EAP-TLS、EAP-GTC、EAP-SIM など) が有効になり、ネットワーク上の認証サーバ (サーバ認証ポート 1645) について IP アドレスと共有シークレット キーを入力する必要があります。802.1x 認証によってダイナミック暗号化キーが提供されるので、WEP キーを入力する必要はありません。このセキュリティ機能では強制 802.1x 認証が有効になります。この SSID を使用して関連付けを行うクライアント デバイスは、802.1 認証を実行する必要があります。
- **[WPA]** - WPA (Wi-Fi Protected Access) は認証サーバのサービスによってデータベースを照会して認証されたユーザへのワイヤレス アクセスを許可し、次に IP トラフィックが WEP で使用されるものより強力なアルゴリズムによって暗号化されます。EAP 認証と同様に、ネットワーク上の認証サーバ (サーバ認証ポート 1645) について、IP アドレスと共有シークレット キーを入力する必要があります。このセキュリティ機能では強制 WPA 認証が有効になります。この SSID を使用して関連付けを行うクライアント デバイスは、WPA に対応している必要があります。

SSID テーブル

この表には、SSID とそれに関連付けられている VLAN、暗号化、認証、およびキー管理のオプションが表示されます。

関連トピック: [エクスプレス セキュリティ] ページの使用

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

ネットワーク マップ:ネットワーク マップ

[ネットワーク マップ] ウィンドウを使用して、ワイヤレス ネットワークに存在するすべてのデバイスの情報を表示します。[アソシエーション] ウィンドウと異なり、LAN 上のワイヤード デバイスは [ネットワーク マップ] ウィンドウに表示されません。

ネットワーク マップ

ネットワーク マップ機能の [有効にする] または [無効にする] を選択します。[有効にする] を選択した場合は、ネットワーク検出時間によるシステムの負荷が増えるため、ページを終了する前にデフォルトの [無効にする] に戻すことをお勧めします。

ネットワーク マップ テーブル

MAC アドレス

メーカーによってデバイスに割り当てられた一意の識別子。

IP アドレス

ポートの IP アドレス。

デバイス

デバイスのタイプ (クライアント、アクセス ポイント、ブリッジなど)。

名前

デバイスに与えられた名前。

ソフトウェア バージョン

現在デバイス上で実行されているソフトウェアのバージョン。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

アソシエーション:

SSID <SSID 名>

表示: クライアント、リピータ

関連付けを表示するデバイスのタイプを選択します。

名前

ワイヤードまたはワイヤレスのポート接続の名前を表示します。

IP アドレス

クライアントの IP アドレス。IP アドレスのリンクをクリックすると、そのクライアントのホーム ページが表示されます。

MAC アドレス

MAC (Media Access Control) アドレスはメーカーによって割り当てられたネットワーク インターフェイスの一意の識別子です。表示される MAC アドレスは [SSID Manager] の画面で有効にされたものです。

状態

クライアントの状態は [Associated] または [Association Processing] で表示されます。

VLAN

このクライアントに VLAN が関連付けられているかどうかを示します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

アソシエーション: アクティビティ タイムアウト

アクセス ポイントがアクティブでないデバイスを追跡する秒数を構成します。秒数はデバイスのクラスに依存します。アクセス ポイントは Cisco Aironet 以外のデバイスを不明なデバイス クラスとして扱います。

デバイス クラス

各デバイス クラスは最初の列にリストされます。デフォルトと最大値をブリッジ、クライアント ステーション、リピータ、ワークグループ ブリッジ、不明な Cisco 製以外のデバイスに対して指定できます。

デフォルト (オプション)

デバイスが関連付けを行ったときにゼロ リフレッシュ レートを提示した場合や、リフレッシュ レートを提示しない場合に、アクセス ポイントで使用するアクティビティ タイムアウトの値を指定します。

最大 (オプション)

デバイスが関連付けを行ったときに提示するリフレッシュ レートに関係なく、デバイスに適用されるアクティビティ タイムアウトの最大許容値を指定します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

アソシエーション： ステーション ビュークライアント

ステーション情報およびステータス

[MAC アドレス] - 製造元によって割り当てられる、一意の識別子。
[名前] - ブリッジに割り当てられる名前。
[IP アドレス] - ブリッジの IP アドレス。
[クラス] - ステーションの種類。
[デバイス] - ブリッジの種類およびモデル番号。
[ソフトウェア バージョン] - ブリッジにインストールされているソフトウェアのバージョン。
[状態] - ステーションの動作状態。[関連付け] または [関連付けプロセス] のいずれかの動作状態が示されます。
親 - あるブリッジの親ブリッジ。
[SSID] - クライアント デバイスがアクセス ポイントとの関連付けに使用する一意の識別子。
[VLAN] - クライアント デバイスが属している VLAN。
[インフラストラクチャへのホップ] - ステーションとネットワーク インフラストラクチャの間のブリッジ数。
[最後のアクティビティ] - ブリッジが最後にアクティブだったときから経過した秒数。
[現在のレート] - 現在のデータ伝送レート。
[暗号化] - 使用された暗号化方式。
[サポートされるレート] - アクセス ポイントとステーションの両方でサポートされている伝送レート。
[インターフェイスを介した通信] - アクセス ポイントが通信に使用しているネットワーク ポート。
[信号の強度] - 現在の無線信号の品質。
[接続速度] - クライアント デバイスがアクセス ポイントに接続されていた秒数。
[信号品質] - 信号の品質が良好である割合。この割合が低い場合、ステーションがカバレッジ エリアの境界部分に存在する可能性があるので、アクセス ポイントにより近い位置に移動する必要があります。
[アクティビティ タイムアウト] - データを最後に受信してから、クライアント デバイスがオフになっていることをブリッジが認識するまでの合計時間。

統計情報の受信/送信

[パケット入力合計] ： ステーションに送られてきた、正常なパケットの数。
[パケット出力合計] - ステーションから送られてきた、正常なパケットの数。
[バイト入力合計] - ステーションに送られてきた、正常なバイトの数。
[バイト出力合計] - ステーションから送られてきた、正常なバイトの数。
[受信した重複] - 重複して受信したパケットの数。
[最大データ試行回数] - データ パケット送信の最大試行数。
[解読エラー] - ステーションから送られてきた暗号化エラーの合計数。
[最大 RTS 試行回数] - RTS パケット送信の最大試行数。
[MIC が失敗しました] - Message Integrity Check (MIC) が失敗した回数。
[MIC がありません] - Message Integrity Checks (MICs) が実行されなかった回数。

パケット数およびエラー数をすべてクリアして、カウンタをゼロにリセットするには、**[クリア]** をクリックしてください。

クライアントに対するアクセス ポイントの認証を取り消すには、 **[Deauthenticate]** をクリックしてください。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ワイヤレス ネットワーク インターフェイス: 要約

このページにはファースト イーサネットと、アクセス ポイントにインストールされている無線 Radio-802.11b、Radio-802.11a、または Radio-802.11g の各インターフェイスの状態情報が含まれています。

インターフェイスの状態

ソフトウェアの状態

ファースト イーサネットと Radio-802.11b、Radio-802.11a、または Radio-802.11g の各インターフェイスがオペレータによって有効にされているかまたは無効にされているかが示されます。

ハードウェアの状態

ファースト イーサネットと Radio-802.11b、Radio-802.11a、または Radio-802.11g の各インターフェイスで回線プロトコルが稼動しているかまたは停止しているかが示されます。

インターフェイスのリセット

インターフェイスが完全にリセットされた回数。

受信

入力レートのタイムスパン

入力レートに使用されるタイムスパン。

入力レート (ビット/秒)

指定された入力レートのタイムスパン内に送信された平均ビット数/秒。

入力レート (パケット/秒)

指定された入力レートのタイムスパン内に送信された平均パケット数/秒。

最後に入力してからの時間

インターフェイスで最後にパケットが正常に受信されてからの時間 (時、分、秒)。この情報はインターフェイスの負荷やネットワーク問題の特定に役立ちます。

パケット入力合計

エラーなしで受信されたパケットの合計。

バイト入力合計

エラーなしで受信されたバイト数の合計。

ブロードキャスト パケット

インターフェイスで受信されたブロードキャスト パケット数の合計。

入力エラー合計

発生した入力関連のエラーの合計。ラント数、ジャイアント数、バッファなし、CRC、フレーム、オーバーラン、無視された数などがエラーに含まれます。

オーバーラン エラー

入力レートが受信側のデータ処理能力を超えたために、受信側ハードウェアが、受信したデータをハードウェア バッファに送ることができなかった回数。

無視されたパケット

インターフェイス ハードウェアの内部バッファに余裕がなくなったために、インターフェイスで無視された受信パケット数。ブロードキャスト ストームや大量のノイズにより、無視された数が増えることがあります。

スロットル

バッファやプロセッサに負荷がかかり過ぎて、そのポートの受信側が無効になった回数。

送信

出力レートのタイムスパン

出力レートに使用されるタイムスパン。

出力レート **(**ビット**/**秒**)**

指定された出力レートのタイムスパン内に送信された平均ビット数/秒。

出力レート **(**パケット**/**秒**)**

指定された出力レートのタイムスパン内に送信された平均パケット数/秒。

最後に出力してからの時間

インターフェイスで最後にパケットが正常に送信されてからの時間 (時、分、秒)。この情報はインターフェイスのトラフィック負荷やネットワーク問題の特定に役立ちます。

パケット出力合計

送信されたメッセージ数の合計。

バイト出力合計

データと MAC カプセル化を含む、送信されたバイト数の合計。

出力エラー合計

インターフェイスからのデータグラムの最終送信を検査できなかったすべてのエラーの合計。

最後の出力ハング

送信に時間がかかり過ぎたためにインターフェイスが最後にリセットされてからの時間 (時、分、秒)。リセットされていない場合は [無] となります。[最後に入力してからの時間]、[最後に出力してからの時間]、または [最後の出力ハング] フィールドで 24 時間を超えるものがあれば、経過時間は日数と時間で示されます。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

ワイヤレス ネットワーク インターフェイス: Radio0-802.11a/b/g Status

このウィンドウには無線インターフェイスの構成と統計が表示されます。

構成

ソフトウェアの状態

インターフェイスがオペレータによって有効にされたかまたは無効にされたかを示します。

ハードウェアの状態

インターフェイスの回線プロトコルが稼動しているかまたは停止しているかを示します。通常は、[ソフトウェアの状態] が有効になっていると、[ハードウェアの状態] が稼動状態になっています。[ソフトウェアの状態] が有効になっていて、[ハードウェアの状態] が停止状態の場合は、エラーが発生します。

稼働率

デバイスがデータ転送に使用するデータ レート (単位はメガビット/秒)。デバイスは常に選択された最高のレートでの送信を試みます。妨害や混信が発生すると、デバイスはデータ転送可能な最高のレートまで落とします。

基本レート

ユニキャストとマルチキャストの両方で、この基本レートでの転送がすべてのパケットで有効になります。1 つ以上のデータ レートが基本レートに設定されている必要があります。

Aironet 拡張機能

Cisco/Aironet 以外の製品との互換性が必要な場合は、[Aironet 拡張機能] の選択を解除します。このオプションを無効にすると、負荷分散、MIC (Message Integrity Check)、TKIP (Temporal Key Integrity Protocol) など、アクセス ポイントのいくつかの拡張機能が制限されます。

キャリア セット

アクセス ポイントが稼動する規制地域を示します。キャリア セットは使用可能な周波数や電力レベルを制限します。規制地域には、南北アメリカ、EMEA (欧州連合)、イスラエル、日本、中国などがあります。

現在の無線チャネル

802.11b、802.11a、802.11g 無線の現在のチャネルと周波数。

送信機の電力

無線送信の電力レベル。デフォルトの電力設定は、該当する規制地域で許可されている最高の送信電力になっています。

ネットワークでの役割

アクセス ポイントはアクセス ポイント (ルート) として動作できます。その場合、アクセス ポイントはワイヤレス トラフィックをワイヤード LAN にブリッジします。

インターフェイスの統計

インターフェイスのリセット

インターフェイスが完全にリセットされた回数。

受信/送信の統計

受信

過去 **5** 分以内の入力レート **(**ビット**/**秒**)**

過去 5 分間に受信した平均ビット数/秒。

過去 **5** 分以内の入力レート **(**パケット**/**秒**)**

過去 5 分間に受信した平均パケット数/秒。

最後に入力してからの時間

インターフェイスによって最後にパケットが正常に送信されてからの時間 (時、分、秒)。この情報はインターフェイスのトラフィック負荷やネットワーク問題の特定に役立ちます。

パケット入力合計

エラーなしで受信されたパケットの合計。

バイト入力合計

データと MAC カプセル化を含む、受信されたバイト数の合計。

送信

過去 **5** 分以内の出力レート **(**ビット**/**秒**)**

過去 5 分間に送信された平均ビット数/秒。

過去 **5** 分以内の出力レート **(**パケット**/**秒**)**

過去 5 分間に送信された平均パケット数/秒。

最後に出力してからの時間

インターフェイスで最後にパケットが正常に送信されてからの時間 (時、分、秒)。この情報はインターフェイスのトラフィック負荷やネットワーク問題の特定に役立ちます。

パケット出力合計

送信されたメッセージ数の合計。

バイト出力合計

データと MAC カプセル化を含む、送信されたバイト数の合計。

エラーの統計

受信

入力エラー合計

発生した入力関連のエラーの合計。ラント数、ジャイアント数、バッファなし、CRC、フレーム、オーバーラン、無視された数などがエラーに含まれます。

スロットル

バッファやプロセッサに負荷がかかり過ぎて、そのポートの受信側が無効になった回数。

送信

出力エラー合計

データグラムの最終送信を検査できなかったすべてのエラーの合計。

最後の出力ハング

送信に時間がかかり過ぎたためにインターフェイスが最後にリセットされてからの時間 (時、分、秒)。リセットされていない場合は [無] となります。[最後に入力してからの時間]、[最後に出力してからの時間]、または [最後の出力ハング] フィールドで 24 時間を超えるものがあれば、経過時間は日数と時間で示されます。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

ワイヤレス ネットワーク インターフェイス: **Radio0-802.11a/b/g** の設定の詳細

無線

無線のタイプ

使用されている無線のブランド名。

無線のシリアル番号

使用されている無線のシリアル番号。

無線のファームウェアのバージョン

無線にインストールされているファームウェアのバージョン。

受信の統計

[受信済みホスト バイト] - 無線から受信してメイン アクセス ポイント プロセッサに渡されたバイト数。
[受信済みユニキャスト パケット] - ポイントツーポイント通信で受信したパケット数。
[ホストへのユニキャスト パケット] - メイン アクセス ポイント プロセッサに渡されたポイントツーポイントのパケット数。
[受信済みブロードキャスト パケット] - インターフェイスで受信されたブロードキャスト パケット数の合計。
[受信済みビーコン パケット] - 受信された 802.11 ビーコン パケット数。
[ホストへのブロードキャスト パケット] - 受信されたブロードキャスト パケットのうちメイン アクセス ポイント プロセッサに渡されたパケット数。
[受信済みマルチキャスト パケット] - 受信されたパケットのうち複数ノードに送信されたパケット数。
[ホストが受信したマルチキャスト パケット] - 受信されたマルチキャスト パケットのうちメイン アクセス ポイント プロセッサに渡されたパケット数。
[受信済み管理パケット] - 無線ファームウェアで受信された 802.11 管理パケット数。
[受信済み RTS] - 受信した 802.11 RTS パケット数。
[重複フレーム] - 同一パケットの受信が繰り返された回数。
[CRC エラー] - 受信の時点でそのデータが無効になっていたパケット数。
[WEP エラー] - 正しく解読できなかったパケット数。
[バッファ フル] - 無線装置で受信バッファがオーバーフローした回数。
[ホスト バッファ フル] - メイン アクセス ポイントがパケットの処理に追いつかず、パケットを捨てた回数。
[ヘッダ CRC エラー] - 802.11 無線ヘッダが壊れていたために捨てられたパケット数。
[無効なヘッダ] - 802.11 無線ヘッダが無効だったために捨てられたパケット数。
[無効な長さ] - 802.11 無線ヘッダの長さフィールドが無効だったために捨てられたパ

ケット数。
[不完全なフラグメント] - 1 つのフレームに属するすべてのフラグメントが受信されなかったために捨てられたパケット数。

Rate *X.X* Mbps Statistics

使用されたデータ レートごとに表示されるセクションです。統計欄がすべてゼロのデータ レートは表示されません。

[Rx Packets] (Rx パケット) - ステーションに入ってきたパケットの総数と過去 5 分間の合計。
[Rx Bytes] (Rx バイト) - ステーションに入ってきたバイトの総数と過去 5 分間の合計。
[RTS Retries] (RTS 再試行数) - RTS パケットが再試行された回数の総数と過去 5 分間の合計。
[Tx Packets] (Tx パケット) - ステーションから送信されたパケットの総数と過去 5 分間の合計。
[TX Bytes] (Tx バイト) - ステーションから送信されたバイトの総数と過去 5 分間の合計。
[Data Retries](データ再試行数) - データ パケットが再試行された回数の総数と過去 5 分間の合計。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

ワイヤレス ネットワーク インターフェイス: Radio0-802.11a/b/g の設定

無線を有効にする

有効の場合、アクセス ポイントは 802.11a/b/g 無線インターフェイスを介してパケットを送信し、他のデバイスが 802.11a/b/g 無線インターフェイスを使用してパケットを送信するのを監視します。無線の管理状態を稼動から停止に切り替えるには [無効にする] を選択します。無線の管理状態を停止から稼動に切り替えるには [有効にする] を選択します。

現在の状態 (ソフトウェア/ハードウェア)

- [ソフトウェア] - ユーザによってインターフェイスが有効にされたかまたは無効にされたかを示します。
- [ハードウェア] - インターフェイスの回線プロトコルが稼動しているかまたは停止しているかを示します。

無線ネットワークでの役割

アクセス ポイントはアクセス ポイント ルートとして動作できます。その場合、アクセス ポイントはワイヤレス トラフィックをワイヤード LAN にブリッジします。

データ レート

データ レートの設定はデータ転送速度の選択に使用します。速度はメガビット/秒単位で表示されます。デバイスは常に選択された最高のレートでの送信を試みます。妨害や混信が発生すると、デバイスは転送可能な最高のレートまで落とします。

アクセス ポイントの範囲を最適化するには [最大範囲] ボタンを、スループットを最適化するには [最大スループット] ボタンをクリックします。

注: 802.11g アクセス ポイント無線を、最適なスループットが得られるように構成すると、802.11g のすべてのデータ レートが基本レート (必須) に設定されます。この設定では 802.11b クライアント デバイスからの関連付けがブロックされます。

レートごとに [必須]、[有効にする]、または [無効にする] を選択します。

- [必須] - ユニキャストとマルチキャストの両方で、このレートでの転送がすべてのパケットで有効になります。1 つ以上のデータ レートが [必須] に設定さ

れている必要があります。クライアントは、必須のレートを関連付ける前にサポートする必要があります。

- **[有効にする]** - このデータ レートでの転送がユニキャストのパケットでのみ有効になります。
- **[無効にする] -** このデータ レートでの送信ができなくなります。

注: クライアントは選択する基本レートに対応している必要があります。対応していないと、アクセス ポイントに関連付けることができません。

Transmit Power (dBm) (送信電力 (dBm))

この設定は無線送信の電力レベルを決定します。デフォルトの電力設定は、該当する規制地域で許可されている最高の送信電力になっています。

注: 無線装置に使用できる最大電力レベルは法律で決められています。この設定は、デバイスを使用する国で定められている規格に従う必要があります。

アクセス ポイントの範囲を制限して混信を低減するか、または低い電力設定を使用して電力を節約してください。

802.11g 無線では、送信電力に CCK 送信電力と OFDM 送信電力の区別があります。CCK は 802.11g で低い周波数レートに使用される変調で、OFDM は 802.11g で高いデータ レート (20 Mbps 以上) に使用される変調です。

注: 100 mW は 12 Mbps を超えるレートには使用できません。

クライアントの電力を制限 **(mW)**

アクセス ポイントに関連付けるクライアント デバイスで使用できる最大電力レベルを決めます。クライアント デバイスがアクセス ポイントに関連付けると、アクセス ポイントは最大電力レベルの設定値をクライアントに送信します。設定値はすべて mW 単位です。

注: 100 mW は 12 Mbps を超えるレートには使用できません。

デフォルトの無線チャネル

使用可能な無線チャネルは規制地域によって決められています。デフォルトの設定では最も混雑の少ない周波数が使用されます。この設定では、デバイスが無線チャネルをスキャンして、最も混雑の少ないチャネルを探して選択します。デバイスは電源を入れたときと無線の設定が変更されたときにスキャンを行います。また、[デフォルトの無線チャネル] ドロップダウン メニューからチャネルの設定を選択することもできます。

最も混雑の少ないチャネルの検索

この選択リストは [デフォルトの無線チャネル] が [最も混雑の少ない周波数] に設定さ

れているときにのみ使用できます。最も混雑の少ないチャネルを検索するとき、問題のあることがわかっているチャネルや他のアプリケーションが使用しているチャネルを除外できます。デフォルトでは、すべてのチャネルが選択され検索されます。複数のチャネルを選択するには、Ctrl または Shift キーを押して複数のチャネルを強調表示します。

ワールド モード マルチドメイン オペレーション (802.11b および 802.11g のみ)

[有効にする] を選択すると、デバイスはチャネル キャリア セットの情報をそのビーコンに追加します。ワールドモードが有効になっているクライアント デバイスは、そのキャリア セット情報を受信して自分の設定値を自動的に調整します。[Dot11d] オプションを選択した場合は、ISO 国番号を入力する必要があります。[レガシ] オプションを選択すると、従来の Cisco ワールド モードが有効になります。

ワールド モードが有効になっていると、アクセス ポイントは使用可能な周波数や送信機の電力などのローカル設定を通知します。これに対応可能なクライアントは、通知したワールド設定値を検出して採用した後、最良のアクセス ポイントを検出するためにスキャンします。

国番号 ([dot11d] オプションにのみ必要)

上記の [ワールド モード] で [dot11d] オプションを選択した場合にのみ国番号が必要になります。2 文字の国番号を入力します。たとえば、米国の ISO 国番号は US です。ISO 国番号のリストについては ISO の Web サイトを参照してください。国番号の後に indoor、outdoor、または both を入力してアクセス ポイントの設置場所を指定する必要があります。

無線プリアンブル (802.11b および 802.11g のみ)

無線プリアンブルはデータの一部でパケットの先頭にあります。そこにはパケットの送受信時にアクセス ポイントとクライアント デバイスが必要とする情報が含まれています。長いプリアンブルでテストを行う場合を除いて、この設定は [短] にしておきます。無線プリアンブルを短いプリアンブルに設定しており、それに関連付けしているクライアントが、短いプリアンブルの関連付けに対応していない場合は、そのクライアントに対して長いプリアンブルのパケットのみが送信されます。

- **[短] -** 短いプリアンブルを使用するとスループットのパフォーマンスが向上します。Cisco Aironet 無線 LAN アダプタは短いプリアンブルに対応しています。アクセス ポイントとクライアント間で短いプリアンブルの使用についてネゴシエートします。Cisco Aironet 無線 LAN アダプタの初期のモデルには長いプリアンブルが必要です。

- **[長]** - 長いプリアンブルを使用すると、アクセス ポイントと Cisco Aironet 無線 LAN アダプタのすべての初期モデル間の互換性が保証されます。

[受信アンテナ] と [送信アンテナ]

- **[多様性] -** このデフォルト設定値は最適な信号を受信するアンテナが使用されるようにデバイスを設定します。デバイスに 2 つの固定 (取り外しできない) アンテナがある場合は、受信と送信の両方にこの設定を使用します。

- **[左]** - デバイスに取り外し可能なアンテナがあり、高ゲイン アンテナが左のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。背面パネルに向かって左にあるのが左側のアンテナになります。

- **[右] -** デバイスに取り外し可能なアンテナがあり、高ゲイン アンテナが右のコネクタに取り付けられている場合は、受信と送信の両方にこの設定を使用します。背面パネルに向かって右にあるのが右側のアンテナになります。

注: デバイスが送受信に使用するアンテナは常に 1 つです。したがって、高ゲイン アンテナを左右のコネクタに取り付けて一方を北向きに他方を南向きにしても範囲を広げることはできません。デバイスで北向きのアンテナが使用されている場合、アクセス ポイントでは南側のクライアント デバイスが無視されます。

Aironet 拡張機能

Cisco Aironet 802.11 拡張機能を使用するには [有効にする] を選択します。負荷分散、MIC、TKIP などを使用するには、この設定を [有効にする] に設定する必要があります。

イーサネット カプセル化の変換

イーサネット カプセル化の種類を設定するには [802.1h] または [RFC1042] を選択します。802.2 パケットではないデータ パケットは、802.1h または RFC1042 を使用して 802.2 の形式に変換する必要があります。Cisco Aironet 機器では相互運用性を最適化するために、RFC1042 をデフォルトに設定してあります。

- **[802.1h] -** Cisco Aironet ワイヤレス製品のパフォーマンスを最適化します。

- **[RFC1042] -** Cisco Aironet 以外のワイヤレス機器との相互運用性を保証するにはこの設定を使用します。RFC1042 には 802.1h ほどの高度な相互運用性はありませんが、他社のワイヤレス機器で使用されています。

信頼できる **WGB** へのマルチキャスト

通常、アクセス ポイントは WGB (ワークグループ ブリッジ) をインフラストラクチャ デバイスとして扱い、クライアントとしては扱いません。アクセス ポイントは、すべてのマルチキャスト パケットの配信を保証するために、信頼性の高いマルチキャスト プロトコルを使用します。信頼性の高い配信によって生じる余分なトラフィックによって、関連付け可能なワークグループ ブリッジの数が制限されます。[無効にする] を選択すると、ワークグループ ブリッジは非インフラストラクチャ デバイスとして扱われ、最大数のワークグループ ブリッジを関連付けできるようになります。

パブリック セキュア パケット転送

[パブリック セキュア パケット転送] (PSPF) は、アクセス ポイントに関連付けられているクライアント デバイスが不注意に、同じアクセス ポイントに関連付けられている他のクライアント デバイスとファイルを共有したり通信したりすることを防止します。これは、クライアント デバイスに、LAN の他の機能がないインターネット アクセスを提供します。

保護されているポート間では、ユニキャスト、ブロードキャスト、またはマルチキャスト トラフィックはやり取りされません。[有効にする] を選択すると、保護されているポートをセキュア モードの構成に使用できます。

PSPF は VLAN ごとに設定されている必要があります。

注: ワイヤレス LAN 上の異なったアクセス ポイントに関連付けされているクライアント間での通信を防止するには、アクセス ポイントが接続されているスイッチ上の保護

されているポートをセットアップする必要があります。

ビーコン間隔

キロマイクロ秒単位のビーコン間の間隔。1 Kμ秒は 1,024 マイクロ秒です。

データ ビーコン レート **(DTIM)**

この設定は常に [ビーコン間隔] の倍数で表され、ビーコンが DTIM (Delivery Traffic Indication Message) を格納する間隔を指定します。トラフィック通知メッセージはすべてのビーコンに含まれています。DTIM は電源節約モードのクライアント デバイスにパケットが待機していることを通知します。電源節約モードのクライアントがアクティブの場合、アクセス ポイントはマルチキャスト トラフィックをバッファに格納し、DTIM ビーコンの直後に配信します。DTIM ビーコンは常に電源節約ノードをアクティブにします。DTIM ビーコンの間隔が長くなるほど、アクセス ポイントのバッファ格納が行われる回数が増加し、マルチキャストの遅延時間が長くなります。

ビーコン間隔がデフォルトの 100 に設定されていて、[データ ビーコン レート] がデフォルトの 2 に設定されている場合、DTIM を格納するビーコンが 200 Kμ秒ごとに送信されます。1 Kμ秒は 1,024 マイクロ秒です。

最大データ再試行数

デバイスがパケットの送信を中止し、パケットを破棄して、クライアントの関連付けを解除するまでに送信を試行する回数。

RTS 最大再試行数

無線によるパケットの送信の試行を停止するまでに、デバイスが RTS を発行する回数の最大値。1 ～ 128 の値を入力します。

フラグメンテーションのしきい値

パケットがフラグメント化される (1 つのブロックではなく複数に分割して送信する) サイズを指定します。通信の感度が悪い場所や混信が激しい場所ではこの値を低く設定します。

RTS のしきい値

デバイスは、ここで指定されたサイズを超えるパケットに対して、その送信前に RTS (送信要求) を発行します。この値を低く設定すると、アクセス ポイントに多くのクライアント デバイスが関連付けられている場合や、クライアント間の距離が遠くて、互いを検出できないがアクセス ポイントだけは検出できる場合に役立ちます。

関連トピック**:** サービス: VLAN

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ:

Radio 080211b SSID

このリンクから [SSID Manager] ウィンドウにアクセスして、認証メソッドの指定と VLAN の定義を行うことができます。

SSID

クライアント デバイスがアクセス ポイントとの関連付けに使用する一意の識別子を指定します。

VLAN

現在割り当てられている VLAN を指定します。

オープン/共有/ネットワーク **EAP**

使用する認証メソッドを指定します。[オープン] を選択すると、すべてのデバイスで認証を行い、アクセス ポイントとの通信を試みることができます。[共有] を選択すると、アクセス ポイントとの通信を試みているすべてのデバイスに、暗号化されていないチャレンジ文字列が送信されます。[ネットワーク EAP] を選択すると、EAP と互換性のあるネットワーク上のサーバと EAP が連携して、ワイヤレス クライアント デバイスの認証を行います。

暗号化設定

[Radio0-802.11b 暗号化設定]、[Radio1-802.11a 暗号化設定]、または [Radio0-802.11g 暗号化設定] をクリックして、[Encryption Manager] ウィンドウにアクセスします。

VLAN

現在割り当てられている VLAN を指定します。

暗号化モード

クライアントがデバイスと通信するときにデータ暗号化を使用するかどうかを示します。[なし]、[WEP 暗号化]、[Cipher] のオプションがあります。暗号化モードの選択に応じて、適用されない残りのカラムは使用できなくなります。

MIC

MIC を有効にするかどうかを指定します。MIC を有効にするには、WEP 暗号化が [強制] に設定されている必要があります。

PPK

PPK を有効にするかどうかを指定します。WEP キー回転を有効にすると、アクセス ポイントからダイナミック ブロードキャスト WEP キーが提供され、指定の間隔でキーが変更されます。

TKIP

Cipher-TKIP を有効にするかどうかを指定します。

WEP40bit

Cipher-WEP40BIT を有効にするかどうかを指定します。

WEP128bit

Cipher-WEP128BIT を有効にするかどうかを指定します。

CKIP

Cipher-CKIP を有効にするかどうかを指定します。

CMIC

Cipher-CMIC を有効にするかどうかを指定します。

キー回転

ブロードキャスト キーを変更する頻度を表示します。

サーバベースのセキュリティ

このリンクから、認証に使用するリモート サーバを識別する [Server Manager] ページにアクセスできます。

サーバ名/IP アドレス

サーバの名前または IP アドレスを指定します。

タイプ

サーバのタイプを指定します。

EAP/MAC/プロキシ モバイル **IP/**管理**/**会計

サーバの使用目的を指定します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ: Encryption Manager - Radio0 - 802.11a/b/g

デバイスで送信した無線信号を暗号化し、受信した無線信号を復号するには、WEP (Wired Equivalent Privacy) が使用されます。このページでは、アクセス ポイントの認証タイプを選択できます。

暗号化モード

クライアントがデバイスと通信する際にデータの暗号化を使用するかどうかを示します。次の 3 つのオプションがあります。

- **[なし]** - デバイスは、WEP を使用していないクライアント デバイスのみと通信を行います。
- **[WEP 暗号化]** - [オプション] または [強制] を選択します。[オプション] を選択した場合、クライアント デバイスは、WEP の有無にかかわらず、このアクセス ポイントやブリッジと通信を行うことができます。[強制] を選択した場合、クライアント デバイスではアクセス ポイントとの通信時に WEP を使用する必要があります。WEP を使用しないデバイスは通信が許可されません。WEP (Wired Equivalent Privacy) は、802.11 標準暗号化アルゴリズムで、元来は有線 LAN でのプライバシー レベルを設定するために設計されたものです。この標準では、40 ビットまたは 104 ビット のサイズの WEP ベース キーが定義されています。
  - **Cisco 対応 TKIP 機能** - Temporal Key Integrity Protocol (TKIP) は、WEP に関係するアルゴリズム スイートで、WEP を稼動するレガシ ハードウェアで最良のセキュリティを達成することを目的に設計されています。TKIP によって WEP に次の 4 つの拡張機能が追加されます。
    1. パケット単位のキー ミキシング機能、これは脆弱鍵攻撃に対抗します。
    2. 新しい IV シーケンス処理の規定、これはリプレイ攻撃を検出します。
    3. 暗号メッセージ完全性チェック (MIC; message integrity check)、これは、ビット フリッピング、パケットの送信元と宛先の改変などの改ざんを検出します。
    4. IV 空間の拡張、これは、実質的に再入力の必要を解消します。
  - **MIC の有効化** - MIC は、ビット フリップ攻撃と呼ばれる暗号化パケットに対する攻撃を防止します。ビット フリップ攻撃では、侵入者が暗号化メッセージを横取りして、若干の変更を加えてから再送信し、受信者は再送信されたメッセージを正当のものであると錯覚して受け入れます。MIC が両方のアクセスポイントおよびすべての関連クライアントデバイスに実装されると、パケットのそれぞれに数バイトが追加され、パケットが不正加工されないようにします。MIC を有効にするには、WEP 暗号化を [強制] に設定する必要があります。
  - パケット単位のキーイングの有効化 - EAP authentication により、クラ

イアント デバイスにダイナミック ユニキャストの WEP キーが提供されますが、スタティックなキーが使用されます。ブロードキャストまたはマルチキャストで WEP キーローテーションが有効化されると、アクセス ポイントではダイナミック ブロードキャスト WEP キーが提供され、このキーは、[ブロードキャスト キー変更の頻度] フィールドで選択したインターバルで変更されます。ブロードキャスト キーの循環は、ご使用のワイヤレス LAN で Cisco デバイス以外の無線クライアント デバイスがサポートされる場合、または、Cisco クライアント デバイスの最新ファームウェアにアップグレードできない場合に優れた代替手段です。

- **Cipher** - Cipher スイートは、ワイヤレス LAN 上の無線通信を保護するように設計された暗号化と整合性のアルゴリズムのセットです。Wi-Fi Protected Access (WPA)、または Cisco Centralized Key Management (CCKM) を有効にするには、Cipher スイートを使用する必要があります。Cipher スイートでは、認証キー管理の使用が許可された状態で通信が保護されるため、暗号化モードの Cipher コマンドを使用して暗号化を有効にするようにお勧めします。ドロップダウン メニューを使用して、TKIP、CKIP、CMIC、WEP のいずれかを選択します。Cipher スイートでは、TKIP のセキュリティが最も強力で、WEP が最も弱くなります。

    - **CKIP**- (別名 Cisco Key Integrity Protocol) - 802.11i セキュリティ タスク グループで公開された初期のアルゴリズムを基盤とした Cisco の WEP キー置換技術です。
    - **CMIC**- (Cisco Message Integrity Check) - CMIC は、偽装攻撃を検出するように設計された Cisco のメッセージ完全性チェック メカニズムです。

VLAN の定義

このリンクをクリックすると、[サービス:VLAN] ページに移動します。このリンクをクリックする前に構成変更が適用されていない場合、これらの変更は失われます。このページでデフォルトの VLAN を設定し、現在の VLAN と ID および情報を割り当てます。たとえば、企業顧客は、さまざまな VLAN を使用して従業員のトラフィックとゲストのトラフィックを分け、さらにこれらのトラフィック グループを優先順位の高いものに分けることができます。さまざまなセキュリティ機能を持つワイヤレス クライアントの送受信トラフィックは、さまざまなセキュリティ ポリシーの VLAN に分けることができます。

暗号化モード

クライアントがデバイスと通信するときにデータ暗号化を使用するかどうかを示します。次の 3 つのオプションがあります。

- **[なし]** - デバイスは、WEP を使用していないクライアント デバイスとのみ通信を行います。
- **[WEP 暗号化]** - [オプション] か [強制] を選択します。オプションを選択した場合、クライアント デバイスは WEP の有無に関わらず、このアクセス ポイントまたはブリッジと通信を行うことができます。強制を選択した場合は、クライアント デバイスはアクセス ポイントとの通信に WEP を使用する必要があります。WEP を使用していないデバイスは通信できません。WEP (Wired Equivalent Privacy) は、802.11 標準暗号化アルゴリズムで、ワイヤード LAN で経験できるプライバシー レベルを提供するように設計されています。この標準では、40 ビットまたは 104 ビットの WEP ベース キー サイズが定義され

ています。

- **[Cipher] -** Cipher スイートは、ワイヤレス LAN 上の無線通信を保護するように設計された暗号化と整合性のアルゴリズムです。WPA (Wi-Fi Protected Access) または CCKM (Cisco Centralized Key Management) を有効にするには、Cipher スイートを使用する必要があります。Cipher スイートには、認証キーを管理しながら同時に通信を保護する機能があるため、暗号化モードの Cipher コマンドを使用して暗号化することをお勧めします。ドロップダウン メニューを使用して、TKIP、CKIP、CMIC、WEP から選択します。TKIP は最も安全性が高く、WEP は最も安全性が低い Cipher スイートです。
  - **[CKIP]** (別名 Cisco Key Integrity Protocol) - 802.11i セキュリティ タスク グループに提示された早期のアルゴリズムに基づく Cisco の WEP キー置換技術。
  - **[CMIC]** (Cisco Message Integrity Check) - CMIC は、偽造攻撃を検出するために設計された Cisco のメッセージ整合性確認メカニズムです。

暗号キー

送信キー

[送信キー] をクリックして、このデバイスが使用する WEP キーを選択してください。一度に 1 つのキーだけを選択できます。設定されたキーはすべて、データの受信に使用できます。

注: 送信キーとして選択するキーは常に、アクセス ポイントやブリッジと関連付けられるクライアント デバイスの同じキースロットに入力されている必要があります。ただし、そのクライアント デバイスで送信キーとして選択されている必要はありません。

暗号キー （**16 進数) 1 ～ 4**

WEP キーをいずれかの [暗号キー] フィールドに入力します。40 ビットの暗号化の場合は 10 桁の 16 進数を入力し、128 ビットの暗号化の場合は 26 桁の 16 進数を入力します。16 進数は、0 ～ 9 の数字、a ～ f までの英小文字、A ～ F までの英大文字から構成される文字列です。WEP キーには、これらの文字を自由に組み合わせて使用できます。WEP キーでは、大文字と小文字が区別されません。

WEP キーは、4 つまで入力できます。送信キーとして選択するキーは常に、アクセス ポイントやブリッジと関連付けられるクライアント デバイスの同じキースロットに入力されている必要があります。ただし、そのクライアント デバイスで送信キーとして選択されている必要はありません。

4 つの WEP キーが設定されており、WEP キー 2 が送信キーとして選択されている場合は、クライアント デバイスの WEP キー 2 も同様に設定されている必要があります。クライアント デバイスに WEP キー 4 が設定されていても、送信キーとして選択されていない場合は、アクセス ポイントの WEP キー 4 が設定されている必要はありません。

キー サイズ

各キーに対して、40 ビットまたは 128 ビットの暗号を選択します。

グローバル プロパティ

ブロードキャスト キー ローテーション インターバル

アクセス ポイントが、ランダムな最善のグループ キーを生成し、キー管理対応ステーションをすべて定期的に更新できるようにします。ブロードキャスト キー回転は、スタティックな WEP クライアントでは使用できません。この機能を使用すると、グループ キーが現在アクティブなメンバーにのみプライベートに保たれます。ただし、ネットワークのクライアントのローミング頻度が高い場合は、オーバーヘッドが生じることがあります。

WPA グループ キー更新

適切なチェックボックスを選択して、アクセス ポイントを変更する頻度と WPA が有効になっているクライアント デバイスにグループ キーを配布する頻度を決定します。

Enable Group Key Update on Membership Termination (メンバシップ解約時にグループ キー更新を有効にする) -

認証されているステーションがアクセス ポイントから関連付けを解除すると、新しいグループ キーが生成および配布されます。この機能を使用すると、グループ キーが現在アクティブなメンバーにのみプライベートに保たれます。ただし、ネットワークのクライアントのローミング頻度が高い場合は、オーバーヘッドが生じることがあります。クライアントがアクセス ポイントから頻繁にローミングする場合は、この機能を有効にしないことをお勧めします。

メンバシップの機能変更に対する更新 -

最後の非キー管理 (スタティック WEP) クライアントが関連付けを解除すると、ダイナミック グループ キーの生成と配布が行われ、最初の非キー管理 (スタティック WEP) クライアントが認証すると、スタティックに構成された WEP キーが配布されます。WPA 移行モードでこの機能を使用すると、アクセス ポイントに関連付けられているレガシ クライアントがない場合に、キー管理対応クライアントのセキュリティが大幅に向上します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ: SSID Manager

SSID プロパティ

現在の SSID リスト

クライアント デバイスがアクセス ポイントとの関連付けに使用する一意の識別子を入力します。SSID は、同じ近辺に存在する複数のワイヤレス ネットワークをクライアント デバイスが区別する際に役立ちます。SSID には、大文字と小文字を区別する 2 ～ 32 文字の半角英数字を使用できます。

SSID

Service Set Identifier (SSID、「無線 SSID」ともいいます) は、クライアントが無線との関連付けに使用する一意の識別子です。最大 16 の SSID を追加できます。

注: このテキスト フィールドでは、?、"、¥、]、+ の 6 文字の使用は許可されていません。さらに、!、#、; の 3 文字を最初の文字に使用することはできません。

VLAN

VLAN は、物理的または地理的な基準ではなく、機能、プロジェクト チーム、またはアプリケーション別に論理的にセグメント化したスイッチド ネットワークです。たとえば、特定のワークグループ チームで使用しているすべてのワークステーションとサーバを、ネットワークへの物理的接続や、他のチームと混在しているかどうかに関係なく、同じ VLAN に接続できます。

VLAN の定義

このリンクをクリックすると、[サービス:VLAN] ページに移動します。このリンクをクリックする前に構成変更が適用されていない場合、これらの変更は失われます。このページでデフォルトの VLAN を設定し、現在の VLAN と ID および情報を割り当てます。たとえば、企業顧客は、さまざまな VLAN を使用して従業員のトラフィックとゲストのトラフィックを分け、さらにこれらのトラフィック グループを優先順位の高いものに分けることができます。さまざまなセキュリティ機能を持つワイヤレス クライアントの送受信トラフィックは、さまざまなセキュリティ ポリシーの VLAN に分けることができます。

ネットワーク ID

SSID のレイヤ 3 モビリティ ネットワーク識別番号を指定します。

認証設定

受け入れたメソッド:

オープン認証

チェック ボックスをオンにして、[オープン認証] を選択します。これを選択すると、すべてのデバイスで認証を行い、アクセス ポイントとの通信を試みることができます。アクセス ポイントで WEP が使用されているのに他のデバイスでは WEP が使用されていない場合、他のデバイスが認証を試みることはありません。他のデバイスが WEP を使用しているのに、WEP キーがアクセス ポイントのキーと一致しない場合、他のデバイスはアクセス ポイントとの認証を行いますが、データは通過しません。

[オープン認証] を選択した後で、使用する別のメソッドをドロップダウン メニューから選択できます。ドロップダウンのオプションには、MAC 認証、EAP、MAC 認証と EAP、または MAC 認証、EAP があります。[EAP] を完全に有効にするには、このウィンドウまたは [Server Manager] ウィンドウで EAP 認証サーバを設定する必要があります。[MAC 認証] を完全に有効にするには、ローカルで MAC アドレスを入力する必要があります。[認証サーバのみ] (Authentication Server Only) オプションの場合、このページまたは [Server Manager] ページで MAC 認証サーバを設定する必要があります。

注: アクセス ポイントで EAP メソッドと [オープン認証] を使用してワイヤレス クライアント デバイスを認証することは可能ですが、アクセス ポイントで EAP を使用して別のアクセス ポイントを認証することはできません。つまり、アクセス ポイントでは、オープン、共有、またはネットワーク EAP 認証メソッドを使用して相互に認証する必要があります。

共有認証

[共有認証] チェック ボックスをオンにして、共有認証を選択します。アクセス ポイントとの通信を試みているすべてのデバイスに、暗号化されていないチャレンジ文字列が送信されます。認証をリクエストしているデバイスはチャレンジ テキストを暗号化して、アクセス ポイントに送り返します。チャレンジ テキストが正しく暗号化されていれば、リクエストしているデバイスの認証が可能になります。暗号化されていないチャレンジと暗号化されているチャレンジを両方監視することもできますが、こうすると、暗号化されていないテキスト文字列と暗号化されているテキスト文字列を比較して WEP キーを推測する侵入者からの攻撃を受けやすくなります。このような弱点があるため、共有キー認証はオープン認証ほど安全ではありません。共有認証を使用できるのは、1 つの SSID だけです。

[共有認証] を選択した後で、使用するメソッドをドロップダウン メニューから選択することができます。MAC 認証、EAP、MAC 認証と EAP から選択することができます。

ネットワーク **EAP**

[ネットワーク EAP] チェック ボックスをオンにして、ネットワーク EAP を選択します。デバイスは Extensible Authentication Protocol (EAP) を使用してネットワーク上に存在する EAP 互換 RADIUS サーバと相互作用し、ワイヤレス クライアント デバイスを認証します。ネットワークとの認証にはダイナミック WEP キーが使用されます。

[ネットワーク EAP] を選択した後で、[MAC 認証] を選択することがで

きます。[MAC 認証] を完全に有効にするには、ローカルで MAC アドレスを入力する必要があります。

このウィンドウまたは [Server Manager] ウィンドウで EAP 認証サーバを設定する必要があります。

サーバの優先順位:

この SSID における特定の RADIUS サーバの使用方法を指定します。[EAP] および [MAC 認証サーバ] のセクションでは、デフォルトを使用するよう選択するか、ドロップダウン メニューを使用して優先順位をカスタマイズすることができます。クリックしてデフォルトの使用を有効にした場合、[デフォルトを定義する] リンクをクリックすると [Server Manager] ウィンドウに移動します。

認証キー管理

WPA は、新しい認証キー管理ソリューションです。WPA (Wi-Fi Protected Access) は、WECA (Wireless Ethernet Compatibility Alliance) によって開発された新しい暫定ソリューションです。WPA は SSN (Simple Security Network) とほぼ同義ですが、IEEE 標準 802.11i の暫定バージョンに依存しています。WPA では、TKIP および WEP 暗号化アルゴリズムに対応しているほか、既存の認証システムと簡単に統合するために 802.1X および EAP もサポートしています。WPA キー管理では、クライアント デバイスとアクセス ポイント間の通信を保護するため、暗号化メソッドを組み合わせて使用します。現在 WPA キー管理では、相互に排他的な認証キー管理、WPA と WPA-PSK に対応しています。

認証キー管理が WPA の場合、クライアントと認証サーバは EAP 認証メソッド (EAP-TLS など) を使用して相互に認証を行い、PMK (Pairwise Master Key) を生成します。認証キー管理が WPA-PSK の場合は、事前共有キーが PMK として直接使用されます。

SSID の WPA を有効にするには、オープン認証またはネットワーク EAP、またはその両方を有効にする必要があります。

注: WPA を有効にする前に、SSID VLAN の暗号化モードをいずれかの Cipher スイート オプションに設定する必要があります。

キー管理

ドロップダウン メニューを使用して、キー管理を強制にするかオプションにするかを指定します。radio 802.11b または 802.11g と同時に WPA 認証キー管理を選択できます。radio 802.11a の場合は、キー管理を 1 つしか選択できません。

WPA 事前共有キー

スタティック WEP キーおよび WPA キー管理を使用してクライアント デバイスに対応するには、アクセス ポイントに事前共有キーを構成する必要があります。キーを入力し、このキーが　WPA を表すことを指定します。802.11b または g 無線の場合、認証キー管理に WAP を選択できます。

会計設定

会計を有効にする

このサーバで、アクセス ポイントに関連付けられたクライアントの使用状況データを記録するかどうかを指定します。使用状況データの一部は、請求または使用状況の追跡に使用できます。

会計サーバの優先順位

デフォルトを使用するか、ドロップダウン メニューを使用して優先順位をカスタマイズできます。デフォルトの使用を有効にした場合、[デフォルトを定義する] リンクをクリックすると [Server Manager] 画面に移動します。

全般設定

アソシエーション制限

特定の SSID に関連付けるクライアントの最大数。アクセス ポイントの過負荷を防ぎ、アソシエートされたクライアントに適切なレベルのサービスを提供することができます。

EAP クライアント (オプション)

ユーザ名

リピータ アクセス ポイントが親アクセス ポイントに関連付けられているときや、ホット スタンバイ アクセス ポイントが監視対象のアクセス ポイントに関連付けられているときに、ネットワーク EAP 認証に使用するユーザ名を示します。

パスワード

リピータ アクセス ポイントが親アクセス ポイントに関連付けられているときや、ホット スタンバイ アクセス ポイントが監視対象のアクセス ポイントに関連付けられているときに、ネットワーク EAP 認証に使用するパスワードを示します。

注: パスワードには、?、"、$、[、+ の 5 文字は使用できません。

グローバル **Radio0-802.11B SSID** プロパティ

ゲスト モード **SSID** の設定

アクセス ポイントのビーコン メッセージに、SSID をテキスト形式で表示します (ブロードキャスト SSID)。ゲスト モードを設定すると、SSID を持たないクライアントでも、このアクセス ポイントに関連付けることができるようになります。したがって、このパラメータを設定するときは十分に注意してください。

インフラストラクチャ **SSID** の設定

アクセス ポイントがリピータ モードのとき、この SSID を使用して親アクセス ポイントに関連付けます。

インフラストラクチャ デバイスに強制的にこの SSID のみを関連付ける場合は、ドロップダウン メニューからチェック ボックスを選択します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ: Server Manager

このページから、認証設定を入力できます。ネットワーク上の RADIUS/TACACS+ サーバは、EAP を使用してワイヤレス クライアント デバイスに認証サービスを提供します。

バックアップ RADIUS サーバ

バックアップ **RADIUS** サーバ

ローカル RADIUS サーバの役割を果たしているアクセス ポイントのホスト名または IP アドレスを入力します。ワイヤレス LAN 上の他のアクセス ポイントは、メインの RADIUS サーバからの応答がないときに、このバックアップ認証サーバを使用します。

共有シークレット

ローカル/バックアップ RADIUS サーバで使用する共有シークレットを入力します。デバイスの共有シークレットは、ローカル/バックアップ サーバの共有シークレットと一致する必要があります。

企業サーバ

現在のサーバ リスト

現在使用可能なサーバを識別します。

サーバ

サーバの名前または IP アドレスを入力します。

共有シークレット

RADIUS/TACACS+ サーバで使用する共有シークレットを入力します。デバイスの共有シークレットは、RADIUS/TACACS+ サーバの共有シークレットと一致する必要があります。

認証ポート (オプション)

RADIUS/TACACS+ サーバが認証に使用するポート番号を入力します。Cisco RADIUS サーバ (アクセス コントロール サーバ [ACS]) のポート設定は 1645 で、多くの RADIUS サーバのポート設定は 1812 です。お使いのサーバの製品ドキュメントで正しいポート設定を確認してください。

会計ポート (オプション)

RADIUS サーバが会計に使用するポート番号を入力します。Cisco RADIUS サーバ (アクセス コントロール サーバ [ACS]) のポート設定は 1646 で、多くの RADIUS サーバのポート設定は 1813 です。お使いのサーバの製品ドキュメントで正しい会計ポート設定を確認してください。

デフォルトのサーバ プロパティ

EAP 認証

EAP 認証に使用するサーバを必要な順に選択します。

MAC 認証

MAC 認証に使用するサーバを必要な順に選択します。

会計

会計に使用するサーバを必要な順に選択します。

管理認証 (RADIUS)

RADIUS 管理認証に使用するサーバを必要な順に選択します。

管理認証 (TACACS+)

TACACS 管理認証に使用するサーバを必要な順に選択します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ: **Server Manager** - グローバル サーバ プロパティ

サーバごとの単位で、次の値をすべての RADIUS/TACACS+ サーバにグローバルに構成できます。

会計更新間隔 (オプション)

会計更新を行う間隔を指定します。会計機能では、ユーザがアクセスしているサービスおよびユーザが消費しているネットワーク リソースの量を追跡します。

TACACS+ サーバ タイムアウト (オプション)

アクセス ポイントがリクエストを再送信する前に TACACS+ リクエストの応答を待つ秒数を指定します。デフォルトは 5 秒で、1 ～ 1000 秒の範囲で指定できます。

RADIUS サーバ タイムアウト (オプション)

アクセス ポイントがリクエストを再送信する前に RADIUS リクエストの応答を待つ秒数を指定します。デフォルトは 5 秒で、1 ～ 1000 秒の範囲で指定できます。

RADIUS サーバ再送信の再試行 (オプション)

アクセス ポイントから各 RADIUS リクエストをサーバに送信する試行回数を指定します。

デッド状態の **RADIUS** サーバ リスト

[有効にする] を選択すると、Cisco IOS ソフトウェアによって、認証リクエストに応答しなかったすべての RADIUS サーバに「デッド状態」のマークが付くので、構成されている次のサーバに進む前にリクエストがタイムアウトするのを防ぐことができます。全サーバがデッド状態とマークされるまでの追加のリクエストでは、デッド状態のマークが付いた RADIUS サーバにはアクセスされません。

RADIUS 呼び出し中/呼び出し済みステーション ID の書式

RADIUS サーバに送信される認証パケットの呼び出し済みステーション ID および呼び出し中ステーション ID (CSID) フィールドの書式を指定します。デフォルトは、Cisco IOS MAC アドレス形式です。IETF オプションは、IETF ドキュメントで推奨されている標準です。書式なしオプションは、VxWorks アクセス ポイントで使用される MAC アドレス形式です。

RADIUS WISPr 属性 (オプション)

WISPr 場所 ID 属性を設定するパラメータです。これらのパラメータで設定された情報は、認証リクエスト中に RADIUS サーバに送信されます。

ISO 国番号

一意の 2 文字のコードを指定します。ISO 3166 の 2 文字の国番号についての情報は、http://www.iso.ch/iso/en/prods-services/iso3166ma/index.html を参照してください。

E.164 国番号

1 ～ 999 の正の数字を指定します。ISO 3166 の国番号の特別な使用方法については、http://www.iso.ch/ISO/en/prods-services/iso3166ma/index.html を参照してください。

E.164 市外局番

ITU-T 推奨に基づいて、3 桁の市外局番を指定します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ: ローカル RADIUS サーバ - 統計

ローカル RADIUS サーバ情報

成功した認証

クライアントが認証に成功した回数。

クライアント ブロック

クライアント認証が、認証失敗回数が多すぎてユーザ名がブロックされたために無視された回数。

不明な NAS

アクセス ポイント (NAS) が RADIUS サーバの使用を試みたにもかかわらず、構成されている有効な NAS のリストに IP アドレスがなかった回数。

不明なユーザ名

ユーザ名を認証するリクエストを受け取り、そのユーザ名がサーバの有効なユーザのリストになかった回数。

無効なパスワード

ユーザがサーバに構成されている値と一致しないパスワードを入力した回数。

NAS からの無効なパケット

NAS から受信したが、無効なために無視されたパケット数。ネットワーク アクセス サーバのいずれかの統計に、エラーの種類の特定のタイプが表示されます。

ネットワーク アクセス サーバ情報

次の情報を表示する: ネットワーク アクセス サーバ xx.xx.xx.xx

情報を表示するネットワーク アクセス サーバを選択します。ネットワーク アクセス サーバは、ローカル RADIUS サーバをバックアップ認証サーバに使用するよう構成されたアクセス ポイントです。

成功

成功した認証数。

クライアント ブロック

クライアント失敗が連続して多発したためにブロックされた認証数。

破損したパケット

受信済みパケットの全長を超えた RADIUS プロトコルの長さ、または個別の無線情報エレメントの長さ。

属性のないユーザ名

認証するユーザ名を示す属性が受信パケットから欠落していることを示す回数。

無効な認証属性 **(Invalid Authentication Attribute)**

認証属性が見つからない回数。サーバが受信するパケットはすべて、送信中に変更されるのを防ぐための認証属性が必要です。

不明な **EAP** メッセージ

EAP 属性メッセージのメッセージ タイプが不明だった回数。

不明なユーザ名

認証に渡されたユーザ名がサーバ データベースで見つからなかった回数。

無効なパスワード

クライアントが入力したパスワードが、サーバ データベースに設定されたパスワードと一致しなかった回数。

不明な **RADIUS** メッセージ

RADIUS メッセージのメッセージ タイプが不明だった回数。

一致しない共有キー

受信済みパケットにおける認証値の確認が失敗した回数。パケットが NAS から本当に送信されたかどうかを確認するため、NAS 用のキーを使用して受信パケットを作成することがあります。この確認でエラーが発生した場合、NAS とサーバ データベース間のキーが一致しなかった可能性があります。

無効な状態属性

NAS 状態情報属性が見つからないか、NAS によって変更された回数。NAS はサーバへの返信でこの情報をエコー バックすることになっています。

不明な **EAP** タイプ

サーバで LEAP 認証だけがサポートされている場合に、別のタイプの EAP 認証の使用を試みた回数。

ユーザ情報

ユーザ名

アクティブなユーザのユーザ名が表示されます。

成功

このユーザが認証に成功した回数。

失敗

このユーザが認証に失敗した回数。通常は、パスワードの不正が原因です。

ブロック

このユーザの認証が無視された回数。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

セキュリティ: ローカル RADIUS サーバ - 一般的なセットアップ

ネットワーク アクセス サーバ (AAA クライアント)

現在のネットワーク アクセス サーバ

バックアップ認証の際にこのアクセス ポイントをローカル RADIUS サーバとして使用するように構成されたアクセス ポイントのリストを表示します。

ネットワーク アクセス サーバ

このアクセス ポイントをローカル RADIUS サーバとして使用するアクセス ポイントの IP アドレスを入力します。

共有シークレット

このアクセス ポイントとネットワーク アクセス サーバ間で共有する共有シークレットを入力します。

個人ユーザ

現在のユーザ リスト

新しいユーザを作成する場合は、[現在のユーザ リスト] メニューで [<新規>] (デフォルト) が選択されていることを確認してください。既存のユーザ プロファイルを編集する場合は、[現在のユーザ リスト] メニューからユーザを選択します。ユーザを選択すると、パスワードとグループ名が表示されます。

ユーザ名

ユーザのユーザ名を指定します。

パスワード

ユーザに割り当てるパスワードを指定します。パスワードを変更する場合は、[パスワード] フィールドと [パスワードの確認] フィールドに必要なパスワードを再入力する必要があります。パスワードはアスタリスクで表示されるため、読み取れません。パスワード フィールドをテキスト文字列で表示するか、NT ハッシュとして暗号化するかを決定します。

パスワードの確認

ユーザのパスワードを再入力します。

グループ名

グループのメンバー全員に認証パラメータが割り当てられている作成済みのユーザ グループ。

ユーザ グループ

アクセス ポイントをローカル RADIUS サーバとして設定する場合、個人ユーザをセットアップする必要があります。各個人ユーザに同じパラメータを入力し直さなくてもいいように、ユーザ プロパティ グループを設定できます。

現在のユーザ グループ

既存のユーザ グループのリスト。

グループ名

VLAN や許可されている SSID などの認証パラメータをグループ内のメンバ全員に割り当てるユーザ グループを作成します。

セッション タイムアウト (オプション)

ローカル サーバがグループ メンバに認証を強制するまでの時間を入力します。

ロックアウト前に失敗した認証 (オプション)

グループに割り当てられたユーザが不正なパスワードを入力できる回数を入力します。この認証試行回数だけ失敗すると、そのユーザはロックアウトされます。この設定は、パスワードの「辞書」攻撃の防止や遅延に役立ちます。

ロックアウト (オプション)

ロックアウトされたユーザを手動でロック解除する場合は、[無限] を選択します。ユーザが認証を再試行できる前にアクセス ポイントがユーザをロックアウトする時間を入力する場合は、[間隔] を選択します。

VLAN ID (オプション)

ユーザ グループに結び付けられた仮想イーサネット LAN 識別番号を識別します。

SSID (オプション)

グループのユーザに許可された SSID。SSID には、大文字と小文字を区別する 2 ～ 32 文字の半角英数字を使用できます。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

エクスプレス セキュリティ セットアップ: : [エクスプレス セキュリティ] ページの使用

次の手順に従って、[エクスプレス セキュリティ] ページから SSID を作成します。

1. [SSID] エントリ フィールドに SSID を入力します。SSID には最大 32 文字の半角英数字を使用できます。
2. アクセス ポイント ビーコンに SSID をブロードキャストする場合は、[ビーコンで SSID をブロードキャストする] チェックボックスをオンにします。SSID をブロードキャストすると、SSID が指定されていないデバイスをアクセス ポイントに関連付けることができます。このオプションは、ゲストや公共の場所のクライアント デバイスが SSID を使用する場合に便利です。SSID をブロードキャストしないと、クライアント デバイスは、自分の SSID と、この SSID が一致しない限り、アクセス ポイントへの関連付けができません。アクセス ポイント ビーコンに含めることができる SSID は、1 つだけです。
3. (オプション)[VLAN ID を有効にする] チェックボックスをオンにし、VLAN 番号 (1 ～ 4095) を入力して、VLAN に SSID を割り当てます。既存の VLAN に SSID を割り当てることはできません。
4. (オプション)[ネイティブ VLAN] チェックボックスをオンにして、VLAN をネイティブの VLAN としてマークを付けます。
5. SSID のセキュリティ設定を選択します。設定は、セキュリティなし、から最も安全な WPA まで、強力な順にリストされています。EAP 認証または WPA を選択した場合は、ネットワーク上の認証サーバの IP アドレスと共有シークレットを入力します。
6. [適用] をクリックします。SSID が、ページ下部の SSID テーブルに表示されます。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

サービス: サービスの概要

このウィンドウには、メインのサービスがすべて現在有効になっているか無効になっているかが表示されます。任意のリンクをクリックすると、該当するページに移動して構成を変更できます。

フィルタ: [有効] または [無効]

VLAN: [有効] または [無効]

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

サービス: フィルタ - フィルタの適用

プロトコル フィルタを使用すると、インターフェイス全体を通じた特定のプロトコルの使用を禁じたり許可することができます。個別のプロトコル フィルタを設定することも、フィルタのセットを設定することもできます。このベース ページを使用すると、送受信用のイーサネットおよび 802.11b 無線インターフェイスにフィルタを適用できます。

フィルタは適用する前に作成する必要があります。

[MAC アドレス フィルタ] タブをクリックして、MAC アドレスのフィルタ インデックスを作成または編集します。[IP フィルタ] タブをクリックして、プロトコル フィルタを作成または編集します。

MAC アドレス、IP フィルタ、Ether タイプの [フィルタ] ページで設定したフィルタは、この [フィルタの適用] ページで有効にしなければ適用されません。

フィルタを適用する際には注意が必要です。不適切なフィルタを適用すると、アクセス ポイントからロックアウトされることがあります。ロックアウトされた場合の回復メソッドは、コンソール ポート アクセス (使用可能な場合) を使用するか、アクセス ポイントをデフォルト構成にリセットします。

受信

ドロップダウン メニューから MAC、Ether タイプ、および IP で有効にするプロトコル フィルタのセットを選択します。

送信

ドロップダウン メニューから MAC、Ether タイプ、および IP で有効にするプロトコル フィルタのセットを選択します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

サービス: フィルタ - MAC アドレス フィルタ

このページを使用して、特定の MAC アドレスに送受信されたユニキャストまたはマルチキャストのパケットの転送を許可したり禁止することができます。指定した以外のすべての MAC アドレスへのトラフィックを許可するフィルタを作成したり、指定した以外のすべての MAC アドレスへのトラフィックをブロックするフィルタを作成できます。作成したフィルタは、イーサネットおよび無線ポートのいずれかまたは両方に、また受信パケットと送信パケットのいずれかまたは両方に適用できます。

[IP フィルタ] タブをクリックして、プロトコル フィルタを作成または編集します。

フィルタ インデックスの作成/編集

新しい MAC アドレス フィルタを作成する場合は、[<新規>] (デフォルト) が選択されていることを確認してください。

フィルタ インデックス

フィルタに 700 ～ 799 の番号を付けます。割り当てた番号から、フィルタのアクセス コントロール リスト (ACL) が作成されます。

MAC アドレスの追加

送信先 MAC アドレスを、4 桁の文字で構成された 3 つのグループをピリオドで区切って入力します (例: 0040.9612.3456)。(注: フィルタが正しく動作できるように、入力する MAC アドレスのすべての文字に小文字を使用してください。)許可するように指定したアドレス以外のすべての MAC アドレスへのトラフィックをブロックする場合は、許可されている MAC アドレスのリストに指定の MAC アドレスを入力します。

マスク

MAC アドレスのマスクを入力します。マスクは、4 桁ごとにピリオドで 3 つのグループに区切って入力します (例: 1122.3344.5566)。マスクの入力方法は、リリースによって異なります。

マスクに 255.255.255.255 と入力すると、すべての IP アドレスが受け入れられます。0.0.0.0 と入力すると、[IP アドレス] フィールドに入力した IP アドレスと同一の IP アドレスが検索されます。このフィールドに入力したマスクは、CLI にマスクを入力したときと同じように動作します。

アクション

[転送] または [ブロック] を選択し、[追加] をクリックします。MAC ア

ドレスが、[フィルタ クラス] フィールドに表示されます。

デフォルトのアクション

[フィルタ クラス] に一致しないパケットは、[デフォルトのアクション] に従って処理されます。

[すべて転送する] または [すべてブロックする] を選択します。フィルタのデフォルトのアクションは、フィルタ内のアドレスの少なくとも 1 つのアクションと反対である必要があります。たとえば、複数のアドレスを入力してすべてのアドレスを [ブロック] するよう選択した場合、フィルタのデフォルトのアクションには [すべて転送する] を選択する必要があります。

注: [適用] をクリックすると、フィルタはアクセス ポイントに保存されますが、[フィルタの適用] ページで適用しなければ有効になりません。

フィルタ クラス

[フィルタ クラス] リストから MAC アドレスを削除するには、削除するアドレスを選択して、[クラスの削除] を選択します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

サービス: フィルタ - IP フィルタ

IP フィルタは、アクセス ポイントのイーサネットおよび無線ポートからの IP アドレス、IP プロトコル、TCP/UDP ポートの使用を禁じたり許可することができます。指定した以外のすべてのアドレスへのトラフィックを許可するフィルタを作成したり、指定した以外のすべてのアドレスへのトラフィックをブロックするフィルタを作成できます。1 つ、2 つ、または 3 つすべての IP フィルタ メソッドが含まれたフィルタを作成できます。作成したフィルタは、イーサネットおよび無線ポートのいずれかまたは両方に、また受信パケットと送信パケットのいずれかまたは両方に適用できます。

[MAC アドレス フィルタ] タブをクリックして、MAC アドレスのフィルタ インデックスを作成または編集します。[フィルタの適用] をクリックすると、送受信無線インターフェイスにフィルタが適用されます。

フィルタ名の作成/編集

新しいフィルタを作成する場合は、[フィルタ インデックスの作成/編集] メニューで [<新規>] (デフォルト) が選択されていることを確認してください。既存のフィルタを編集するには、[フィルタ インデックスの作成/編集] メニューからフィルタ名を選択します。

フィルタ名

新しいフィルタの説明となる名前を入力します。

デフォルトのアクション

[フィルタ クラス] に一致しないパケットは、デフォルトのアクションに従って処理されます。

フィルタのデフォルトのアクションに [すべて転送する] または [すべてブロックする] を選択します。フィルタのデフォルトのアクションは、フィルタ内のアドレスの少なくとも 1 つのアクションと反対である必要があります。たとえば、IP アドレス、IP プロトコル、および TCP/UDP ポートが含まれたフィルタを作成して、すべてのアクションに [ブロック] を選択した場合、フィルタのデフォルトのアクションには [すべて転送する] を選択する必要があります。

IP アドレス

送信先アドレス

フィルタにかける IP アドレスを入力します。許可するよう指定した以外の IP アドレスをすべてブロックする場合、許可されているアドレスのリストにお使いの PC のアドレスを入力して、アクセス ポイントへ

の接続が失われないようにします。

マスク

送信先 IP アドレスのマスクを入力します。マスクは、4 桁ごとにピリオドで 3 つのグループに区切って入力します (例: 112.334.556.778)。マスクに 255.255.255.255 と入力すると、すべての IP アドレスが受け入れられます。0.0.0.0 と入力すると、[IP アドレス] フィールドに入力した IP アドレスと同一の IP アドレスが検索されます。このフィールドに入力したマスクは、CLI にマスクを入力したときと同じように動作します。

送信元アドレス

フィルタにかける IP アドレスを入力します。許可するよう指定した以外の IP アドレスをすべてブロックする場合、許可されているアドレスのリストにお使いの PC のアドレスを入力して、アクセス ポイントへの接続が失われないようにします。

マスク

送信元 IP アドレスのマスクを入力します。マスクは、4 桁ごとにピリオドで 3 つのグループに区切って入力します (例: 112.334.556.778)。マスクの入力方法は、リリースによって異なります。

マスクに 255.255.255.255 と入力すると、すべての IP アドレスが受け入れられます。0.0.0.0 と入力すると、[IP アドレス] フィールドに入力した IP アドレスと同一の IP アドレスが検索されます。このフィールドに入力したマスクは、CLI にマスクを入力したときと同じように動作します。

アクション

[転送] または [ブロック] を選択し、[追加] をクリックします。アドレスが、[フィルタ クラス] フィールドに表示されます。

IP プロトコル

IP プロトコル

IP プロトコルをフィルタにかけるには、ドロップダウン メニューからいずれかの共通プロトコルを選択するか、[カスタム] ラジオ ボタンを選択して [カスタム] フィールドに既存の ACL の番号を入力します。0 ～ 255 の ACL 番号を入力します。

アクション

[転送] または [ブロック] を選択し、[追加] をクリックします。プロトコルが、[フィルタ クラス] フィールドに表示されます。

UDP/TCP ポート

TCP ポート

TCP プロトコルをフィルタにかけるには、ドロップダウン メニューからいずれかの共通ポート プロトコルを選択するか、[カスタム] ラジオ ボタンを選択していずれかの [カスタム] フィールドに既存のプロトコルの番号を入力します。0 ～ 65535 のプロトコル番号を入力します。

アクション

[転送] または [ブロック] を選択し、[追加] をクリックします。プロトコルが、[フィルタ クラス] フィールドに表示されます。

UDP ポート

UDP プロトコルをフィルタにかけるには、ドロップダウン メニューからいずれかの共通ポート プロトコルを選択するか、[カスタム] ラジオ ボタンを選択していずれかの [カスタム] フィールドに既存のプロトコルの番号を入力します。0 ～ 65535 のプロトコル番号を入力します。

アクション

[転送] または [ブロック] を選択し、[追加] をクリックします。プロトコルが、[フィルタ クラス] フィールドに表示されます。

フィルタ クラス

プロトコルが、ウィンドウのこの部分に表示されます。[フィルタ クラス] リストからプロトコルを削除するには、削除するプロトコルを選択して、[クラスの削除] を選択します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

ヘルプの内容

サービス: VLAN

VLAN は、物理的または地理的な基準ではなく、機能、プロジェクト チーム、またはアプリケーション別に論理的にセグメント化したスイッチド ネットワークです。たとえば、特定のワークグループ チームで使用しているすべてのワークステーションとサーバを、ネットワークへの物理的接続や、他のチームと混在しているかどうかに関係なく、同じ VLAN に接続できます。VLAN によるネットワークの再設定は、デバイスやワイヤを物理的に取り外したり移動したりするのではなく、ソフトウェアを通じて行うことができます。

VLAN は、定義されたスイッチ セット内にあるブロードキャスト ドメインと考えることができます。VLAN は、1 つのブリッジング ドメインによって接続された複数のエンド システム、つまりホストまたはネットワーク機器 (ブリッジやルータなど) で構成されます。ブリッジング ドメインは、さまざまなネットワーク機器でサポートされています。たとえば LAN スイッチは、VLAN ごとに異なるグループを使用して、スイッチ間のブリッジング プロトコルを処理します。

VLAN の基本的な無線コンポーネントは、アクセス ポイントと、無線テクノロジーを使用してアクセス ポイントに関連付けられるクライアントです。基本的に、特定の VLAN に接続するようにアクセス ポイントを設定する際のポイントは、その VLAN を認識するように SSID を設定することです。VLAN は VLAN ID によって識別されるので、アクセス ポイントの SSID が特定の VLAN ID を認識するように設定された場合、VLAN との接続が確立されます。この接続が確立されると、同じ SSID を持つ、関連付けられた無線クライアント デバイスは、このアクセス ポイントを介して VLAN にアクセスできます。VLAN は、ワイヤード ネットワークとのやり取りと同様に、クライアントとやり取りしてデータを処理します。

VLAN ブリッジング。別のルータ インターフェイスと IP アドレスを共有する VLAN を設定します。

VLAN ルーティング。 トラフィックをルーティングできる VLAN を設定します。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

サービス: VLAN ブリッジング

グローバル VLAN プロパティ

現在のネイティブ VLAN

ネイティブ VLAN に指定した VLAN を指定します。[VLAN ID] フィールドの下の「ネイティブ VLAN」と示されているチェックボックスをオンにして選択します。

割り当て済み VLAN

現在の VLAN リスト

このリストから VLAN を選択すると、この VLAN の VLAN ID と SSID が表示されます。その後 [削除] をクリックして VLAN を削除するか、[SSID の定義] をクリックして [SSID Manager] ウィンドウに移動できます。

VLAN の作成

VLAN を追加する場合、このセクションから VLAN を作成し、SSID を割り当てます。

VLAN ID

SSID に結び付ける仮想イーサネット LAN 識別番号を指定します。

ブリッジ グループの仮想インターフェイスが構成されている場合は、ブリッジ グループ番号を入力します。

この VLAN ID をネイティブ VLAN にする場合は、チェックボックスをクリックします。

チェックボックスをクリックしてパブリック セキュア パケット転送を有効にし、保護されているポートをセキュア モード構成に使用できるようにします。

Cisco IOS リリース 12.2(8)JA 以降を使用している場合は、この VLAN ID に関連付ける無線インターフェイスをクリックして選択します。

SSID

VLAN に結び付ける SSID を指定します。

VLAN 情報

次の情報を表示する:

ドロップダウン メニューから、作成済みの VLAN のリストを表示します。リストの VLAN を強調表示すると、送受信済みのファスト イーサネット パケットと送受信済みの無線パケットの値が表示されます。

ワイヤレス アプリケーションのオンライン ヘルプ (12.2(15)JA)

サービス: VLAN ルーティング

ルーティングする Radio0-802.11g インターフェイスを構成した場合、このウィンドウに VLAN 情報を入力します。

グローバル VLAN プロパティ

現在のネイティブ VLAN

ネイティブ VLAN に指定した VLAN を指定します。[VLAN ID] フィールドの下の「ネイティブ VLAN」と示されているチェックボックスをオンにして選択します。

割り当て済み VLAN

現在の VLAN リスト

このリストから VLAN を選択すると、この VLAN の VLAN ID と SSID が表示されます。その後 [削除] をクリックして VLAN を削除するか、[SSID の定義] をクリックして [SSID Manager] ウィンドウに移動できます。

VLAN の作成

VLAN を追加する場合、このセクションから VLAN を作成し、SSID を割り当てます。

VLAN ID

SSID に結び付ける仮想イーサネット LAN 識別番号を指定します。

この VLAN ID をネイティブ VLAN にする場合は、チェックボックスをクリックします。

Radio0 802.11g インターフェイスの IP アドレスとサブネット マスクを入力します。

SSID

VLAN に結び付ける SSID を指定します。

VLAN 情報

次の情報を表示する:

ドロップダウン メニューから、作成済みの VLAN のリストを表示します。リストの

VLAN を強調表示すると、送受信済みのファスト イーサネット パケットと送受信済みの無線パケットの値が表示されます。