D-Link DWL-8610AP

802.11ac Dual band Access Point

ユーザマニュアル

D-Link
Building Networks for People

目次

お使いになるまえに

1

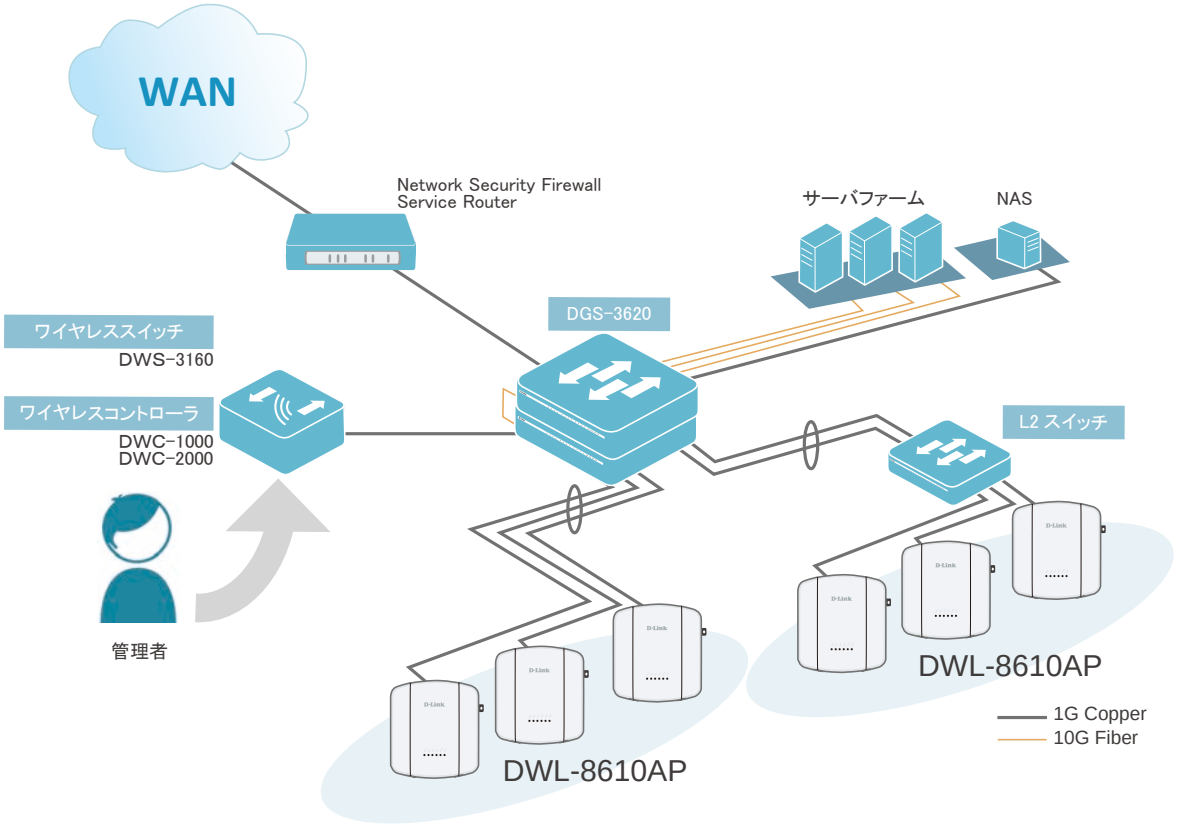
このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。必要な場合には、いつでもご覧いただけますよう大切に保管してください。

また、必ず本書、設置マニュアル、および同梱されている製品保証書をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

本製品について

■機能概要

DWL-8610AP はIEEE 802.11a/b/g/n/ac に準拠、2.4GHz/5GHz デュアルバンドの同時利用に対応し、最大1.3Gbps（理論値）の転送速度と優れたセキュリティ機能を兼ね備えた高性能なアクセスポイントです。ワイヤレスコントローラDWS-3160/DWC-1000/DWC- 2000 にDWL-8610AP を接続することにより、アクセスポイントは常に最適なチャンネルや転送出力に自動調整され、帯域内でもっとも安全で安定した通信を行うことができます。DWL-8610AP とワイヤレスコントローラを組み合わせて使用することで、不正AP の検出、ユーザ認証、各種統計情報のモニタリングなどビジネス環境における無線ネットワークに高パフォーマンスと高セキュリティを提供します。



■本製品の特長

- IEEE 802.11a/b/g/n/ac 準拠
- 2.4GHz/5GHzデュアルバンド（同時利用）
- WPA/WPA2 Enterprise/Personal 暗号方式
- 64/128ビットWEP暗号化
- MACアドレスフィルタリング
- SSIDステルス設定
- マルチSSID：最大32個
- APクラスタリング（スタンドアローン利用時のみ）
- WDS機能搭載
- SNMPv1/v2c/v3
- QoS（WMM 準拠）
- 不正AP検知
- 5GHz優先機能
- IEEE 802.3at PoE受電機能
- DWS-3160/DWC-1000/DWC-2000による集中管理
- GUI、SSH、Telnet、CLIによる設定/管理

本マニュアルについて

■マニュアルの構成

1章：お使いになるまえに
本マニュアルの紹介と、本製品をお使いになる前の注意事項を記載しています。

2章：設置と管理のしかた
本製品の設置方法と、Web GUIやCLIを使用した管理方法について説明します。

3章：Status
Statusメニューの設定内容について説明します。

4章：Manage
Manageメニューの設定内容について説明します。

5章：Service
Serviceメニューの設定内容について説明します。

6章：SNMPv3
SNMPv3メニューの設定内容について説明します。

7章：Maintenance
Maintenanceメニューの設定内容について説明します。

8章:Cluster
Clusterメニューの設定内容について説明します。

9章:Client QoS
Client QoSニューの設定内容について説明します。

10章：付録
製品を工場出荷時の設定に戻す方法と、いくつかの機能の設定例を記載しています。

■マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

■表記規則

本マニュアルでは以下の記号を使用します。

⚠警告 この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。

⚠注意 この表示を無視し、間違った使い方をすると、傷害または物損損害が発生するおそれがあります。

重要 設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

メモ 特長や技術についての詳細情報を記述します。

本マニュアル中での字体、・記号についての表記規則は以下のとおりです。

字体	解説	例
[XXXXX]	Web GUIのUI	[Relay Options]
『XXXXXX』	マニュアル内の参照先	『お使いになるまえに：p.5 』
[XXXXX] >[XXXXX]	Web GUIの操作手順	**[Status] >[Interface]**

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物損損害が発生するおそれがあります。

記号の意味　🚫 してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠危険

- 🚫 分解・改造をしない
  火災、やけど、けが、感電などの原因となります。
- 🚫 ぬれた手でさわらない
  感電の原因となります。
- 🚫 水をかけたり、ぬらしたりしない
  内部に水が入ると、火災、感電、故障の原因となります。
- 🚫 水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない
  火災、やけど、けが、感電、故障の原因となります。
- 🚫 各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く
  火災、やけど、けが、感電、故障の原因となります。
- 🚫 油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない
  火災、やけど、けが、感電、故障の原因となります。
- 🚫 内部に金属物や燃えやすいものを入れない
  火災、感電、故障の原因となります。
- 🚫 砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない
  火災、やけど、けが、感電、故障の原因となります。
- 🚫 電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない
  火災、やけど、けが、感電、故障の原因となります。

⚠警告

- 🚫 落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
  故障の原因となります。
- 🚫 発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
  感電、火災の原因になります。
  使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。
- 🚫 表示以外の電圧で使用しない
  火災、感電、または故障の原因となります。
- 🚫 たこ足配線禁止
  たこ足配線などで定格を超えると火災、感電、または故障の原因となります。
- ❗ 設置、移動のときは電源プラグを抜く
  火災、感電、または故障の原因となります。
- 🚫 雷鳴が聞こえたら、ケーブル / コード類にはさわらない
  感電の原因となります。
- 🚫 ケーブル / コード類や端子を破損させない
  無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。
- ❗ 本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
  火災、感電、または故障の原因となります。
- 🚫 各光源をのぞかない
  光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。
- 🚫 各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする
  火災、やけど、けが、感電または故障の原因となります。
- 🚫 使用中に布団で覆ったり、包んだりしない
  火災、やけどまたは故障の原因となります。
- ❗ ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
  引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。
- 🚫 カメラのレンズに直射日光などを長時間あてない
  素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。
- ❗ 無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
  電子機器や医療電気機器に悪影響を及ぼすおそれがあります。
- 🚫 本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
  火災、または故障の原因となります。
- ❗ 耳を本体から離してご使用ください
  大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。
- ❗ 無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
  医療電気機器に悪影響を及ぼすおそれがあります。
- ❗ 高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない
  電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。
- ❗ ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
  破損部や露出部に触れると、やけど、けが、感電の原因となります。
- ❗ ペットなどが本機に噛みつかないように注意する
  火災、やけど、けがなどの原因となります。
- 🚫 コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない
  火災、やけど、感電または故障の原因となります。
- 🚫 AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない
  発火、発熱、感電または故障の原因となります。

⚠警告

- AC アダプタもしくは電源プラグについたほこりは、拭き取る
  ほこりが付着した状態で使用すると、
  火災、やけど、感電または故障の原因となります。
- AC アダプタや電源ケーブルをコンセントに
  さしこむときは、確実に差し込む
  確実に差し込まないと、火災、やけど、
  感電もしくは故障の原因となります。
- 接続端子が曲がるなど変形した場合は、直ちに使用を中止する。
  また、変形をもとに戻しての使用も行わない
  端子のショートにより、火災、やけど、けが、
  感電または故障の原因となります。
- 各種接続端子を機器本体に接続する場合、斜めに差したり、
  差した状態で引っ張ったりしない
  火災、やけど、感電または故障の原因となります。
- 使用しない場合は、AC アダプタもしくは
  電源ケーブルをコンセントから抜く
  電源プラグを差したまま放置すると、火災、やけど、
  感電または故障の原因となります。
- お手入れの際は、AC アダプタもしくは
  電源ケーブルをコンセントから抜く
  抜かずに行うと、火災、やけど、感電または故障の原因となります。
- 禁止 SD や MicroSD カード、USB メモリの使用中は、
  カードやメモリを取り外したり、本製品の電源を切ったりしない
  データの消失、機器本体の故障の原因となります。
- 禁止 磁気カードや磁気を帯びたものを本製品に近づけない
  磁気カードのデータが消えてしまうおそれもしくは
  機器本体の誤作動の原因となります。
- ディーリンクジャパンが販売している無線機器は
  国内専用のため、海外で使用しない
  海外では国によって電波使用制限があるため、
  本製品を使用した場合、罰せられる場合があります。
  海外から持ち込んだディーリンク製品や並行輸入品を
  日本国内で使用する場合も同様に、罰せられる場合があります。

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 コードを持って抜かない
  コードを無理に曲げたり、引っ張ると、
  コードや機器本体の破損の原因となります。
- 禁止 振動が発生する場所では使用しない
  故障の原因となります。
- 付属品の使用は取扱説明書に従う
  本製品の付属品は、取扱説明書に従い、
  他の製品に使用しないでください。機器の破損の原因となります。
- 禁止 破損したまま使用しない
  火災、やけどまたはけがの原因となります。
- 禁止 ぐらついた台の上や傾いた場所などの
  不安定な場所や高所には置かない
  落下して、けがなどの原因となります。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 コンセントにつないだ状態で、AC アダプタや
  電源コンセントに長時間触れない
  やけど、感電の原因となります。
- 一般の電話機やコードレス電話、テレビ、ラジオなどを
  お使いになっている近くで使用しない
  近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、
  なるべく離れた場所で使用してください。
- 禁止 D-Link が指定したオプション品がある場合は、
  指定オプションを使用する
  不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。
この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。
さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

バッテリの取り扱いについて

⚠警告

不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

電源の異常

万一停電などの電源異常が発生した / する場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

無線LANについて

業界業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。
WLAN は家庭やオフィス環境のみならず、空港やコーヒーショップ、または大学など公共の施設においても幅広く利用されるようになってきました。
この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。
ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

■WLAN 技術を利用するさまざまな理由

可動性
WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。

低い実現コスト
WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします。

簡単な設置と拡張
煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。

低コストのソリューション
無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な複数のモードで多機能性を提供し、コスト削減を行います。

柔軟性
配置する無線 LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、自由自在に構築することができます。

世界基準対応の技術
無線機器は、IEEE802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n および IEEE 802.11ac に準拠しています。

● IEEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、最大 1.3Gbps までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

● IEEE 802.11n 規格

IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 450Mbps までと高速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。
これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが可能になります。OFDM(Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク（干渉）の発生を抑えることが可能です。
IEEE 802.11n 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。
WPA/WPA2 には企業向けの「 Enterprise」とホームユーザ向けの「Personal」の 2 種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「Pre-Shared Key（ 事前共有鍵）」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた時にアクセスが認められます。
「WPA-Enterprise」と「 WPA2-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。

ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」または「 WPA2-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。
EAP（ Extensible Authentication Protocol）は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべてのデバイスの EAP タイプを同一にする必要があります。

重要
最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

■無線に関するご注意

電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。

以下の注意をよくお読みになりご使用ください。

● 本製品を以下の場所では使用しないでください。

- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。
- 電気製品、AV 機器、OA 機器などの磁気を帯びているところや電磁波が発生しているところで使用すると下記のような影響があります。
    - 時期や電気雑音の影響を受けると雑音が大きくなったり、通信ができなくなったりすることがあります。
    - テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れたりすることがあります。
    - 近くに複数の無線 LAN アクセスポイントが存在し、同じチャネルを使用していると、正しく検索できない場合があります。

● 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局) 並びにアマチュア無線局 (免許を必要とする無線局) が運用されています。

● 本製品を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。

● 万一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。

● その他、本製品から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定 小電力無線局並びにアマチュア無線局の帯域を回避可能

5GHz 帯使用に関するご注意

無線 LAN の 5.2/5.3GHz（W52/W53）をご利用になる場合、電波法の定めにより屋外ではご利用になれません。

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

● 通信内容を盗み見られる

悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。

- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

● 不正に侵入される

悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。

- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/product-assurance-provision

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
https://www.dlink-jp.com/support

設置と管理のしかた

2

本製品の設置方法と、Web GUIやCLIを使用した管理方法について説明します。

パッケージの内容

本製品には、以下のものが同梱されています。

- 本体
- ACアダプタ
- RJ-45/DB9 変換ケーブル
- ネットワークケーブル
- マウントキット
- GNU GPLライセンスノート
- シリアルラベル
- CD-ROM

不足しているものや損傷を受けているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

ネットワーク接続前の準備

アクセスポイントの設置場所が性能に大きな影響を与えます。以下の注意事項に従って本製品を設置してください。

● 設置にあたってのご注意

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になります。
しかし、壁や天井など、無線信号が通過する物体の数や厚さ・場所などにより、動作範囲が制約を受ける場合があります。
一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

◎ 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は1 ～ 30 メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。

◎ ネットワークデバイス間の直線距離にご注意ください。厚さ50 センチの壁を45 度の角度で無線信号が通過する時、通り抜ける壁の厚みは約1メートルになります。2 度の角度で通過すると、通り抜ける厚みは14 メートルになります。信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。

◎ 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線LAN デバイスや無線LAN アダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。

◎ 周波数ノイズを発生する電気機器や家電製品からは、最低でも1、2 メートル離してデバイスを設置してください。

◎ 2.4GHz のコードレス電話またはX-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz 電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。

◎ 必ず付属のUTP ケーブル、AC アダプタをご使用ください。

⚠注意

本アクセスポイントは、IEEE 802.3at 準拠の給電スイッチまたは弊社が承認する給電機器から受電することができます。弊社が承認していないPoE 給電機器に本アクセスポイントを接続すると、本アクセスポイントが破損する場合があります。

システム要件

Web インタフェースを使用、またはTelnet やSSH 経由でCLI を使用して統合アクセスポイントを管理するためには、アクセスポイントにIP アドレスが必要になります。また、ネットワーク上でVLAN や IEEE 802.1X 認証を使用している場合、ネットワークに接続する前に、アクセスポイントに追加の設定をする必要があります。

⚠注意

本製品は、インターネットのゲートウェイとして動作しません。ご使用の無線LAN を他のLAN またはインターネットに接続するためには、別途ゲートウェイが必要です。

■管理者用コンピュータ推奨環境

Web ベースのユーザインタフェースを使用して統合アクセスポイントの設定および管理を行うための管理者用コンピュータの最小必要環境を説明します。

◎ イーサネットへの接続
本製品を最初に設定するためには、使用するコンピュータをシリアルケーブルまたはイーサネットケーブルで接続します。

◎ ネットワークへの無線接続
新規の無線ネットワークで最初にアクセスポイントの初期設定および起動を行うと、内部ネットワークへの無線接続を使用して、管理者用Web 画面で設定変更を行うことができます。
本製品への無線接続には、管理者用機器に無線クライアントと同様のWi-Fi 機能が必要になります。

- 本製品が準拠する1つ以上の IEEE 802.11 モードをサポートする、ポータブルまたは内蔵型の Wi-Fi クライアントアダプタ。
- 本製品と接続するよう設定した無線クライアントソフトウェア。

◎ Web ブラウザとオペレーティングシステム
本製品の設定および管理は、本製品に実装されたWeb ベースユーザインタフェースを経由して行います。
本製品の管理者用 Web 画面に接続するためには、以下のいずれかのブラウザを使用することをお勧めします。

- Microsoft® Internet Explorer® 8 以降
- Mozilla® Firefox 3.5 以降
- Safari 5 以降

管理者用Web ブラウザは、管理者インタフェースのインタラクティブ機能をサポートするため、必ずJavaScript を有効にしてください。

◎ セキュリティ設定
本製品の初期設定に使用する無線クライアントのセキュリティが無効になっていることを確認してください。

■無線クライアントの必要環境

統合アクセスポイントは、アクセスポイントが動作している802.11 モードに対し、Wi-Fi クライアントアダプタが適切に設定されていれば、どんなクライアントにも無線接続を提供します。本製品は、システムを運用している複数のクライアントをサポートします。クライアントとは、Wi-Fi アダプタやサポートドライバが装備されているノートパソコンやデスクトップコンピュータ、PDA、その他の携帯型や据え置き型のデバイスを意味します。

アクセスポイントに接続するためには、無線クライアントに以下に示すソフトウェアおよびハードウェアが搭載されている必要があります。

◎ Wi-Fi クライアントアダプタ
アクセスポイントが準拠する1 つ以上のIEEE 802.11 モードをサポートする、ポータブルまたは内蔵型のWi-Fi クライアントアダプタ。(IEEE 802.11a、802.11b、802.11g、802.11n 、802.11ac ををサポート。)

◎ 無線クライアントソフトウェア
本製品に接続するよう設定したクライアントソフトウェア(例：Microsoft Windows サプリカント)。

◎ クライアントセキュリティ設定
本製品の初期設定を行うために、クライアントのセキュリティは必ず無効にしてください。

本製品のセキュリティモードがテキスト以外で設定される場合、無線クライアントは本製品が使用する認証モードにプロファイルを設定して、有効なユーザ名、パスワード、証明書または同等のユーザ認証を提供する必要が生じます。
セキュリティモードとして、スタティックWEP、IEEE 802.1X、RADIUS サーバを持つWPA およびWPA-PSK があります。

本製品のセキュリティ設定に関する情報は、「VAP(仮想アクセスポイントの設定)」を参照してください。

ダイナミック/スタティック IP アドレス設定

本製品の電源を入れると、実装されているDHCP クライアントは、IP アドレスおよびその他のネットワーク情報を取得するためにネットワーク上のDHCP サーバを検索します。
本製品がネットワーク上のDHCP サーバを検出しない場合は、DHCP サーバからネットワーク情報の受信に成功するまで、スタティック IP アドレスの初期値（10.90.90.91）を使用します。

メモ

接続タイプの変更およびスタティック IP アドレスの割り当てのためにCLI を使用する場合は『CLI を使用したイーサネット設定：p.27 』、Web ユーザインタフェースを使用する場合は『Ethernet Settings（イーサネット設定）：p.43 』を参照してください。

■IPアドレスのリカバリ

本製品の接続に問題がある場合は、アクセスポイントの設定を工場出荷時の初期値にリセットしてスタティック IP アドレスを回復することができます。（『工場出荷時設定に戻す：p.125 』を参照）。
または、DHCP サーバを持つネットワークにアクセスポイントを接続して、ダイナミックにアドレスを割り当てることもできます。

■ダイナミックに割り当てられたIP アドレスの検出

ご使用のネットワーク上のDHCP サーバに接続してアクセスポイントのIP アドレスを取得すると、アクセスポイントのMAC アドレスに接続する新しい IP アドレスを参照することができます。
アクセスポイントに IP アドレスを割り当てるDHCP サーバに接続できない場合、またはアクセスポイントのMAC アドレスが不明の場合は、CLI を使用して新しい IP アドレスを検出する必要があります。

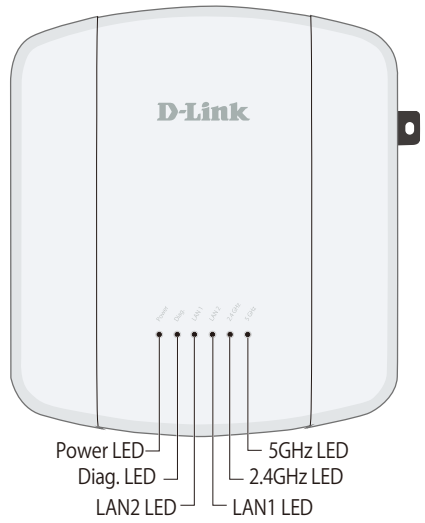
メモ

ダイナミックに割り当てられた IP アドレスの検出については、『CLI を使用した IP アドレスの参照：p.26 』を参照してください。

本体各部名称

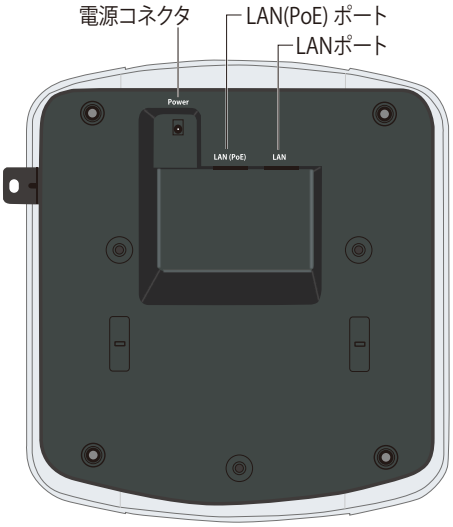
本製品の各部名称について説明します。

■上面



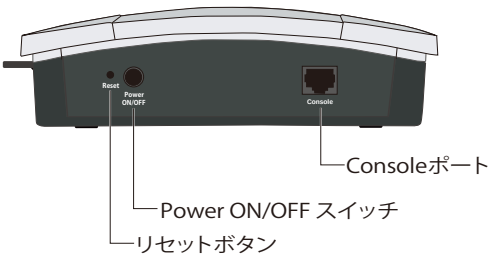
LED	色	状態	状況説明
Power LED	緑	点灯	電源が入っています。
Diag. LED	赤	点灯	システムが正しく動作していません。 診断を実行しています。
LAN1/LAN2 LED	緑	点灯	ネットワークのリンクが確立しています。
		点滅	ネットワーク上でデータを送受信しています。
2.4GHz LED	緑	点灯	2.4GHz帯域が有効になっています。
		点滅	2.4GHz帯域でデータを送受信しています。
5GHz LED	緑	点灯	5GHz帯域が有効になっています。
		点滅	5GHz帯域でデータを送受信しています。

■底面



名称	説明
電源コネクタ	付属のAC アダプタを接続します。
LAN(PoE)ポート	RJ-45ケーブルを挿入し、ネットワークへの接続とPoE受電を行います。
LANポート	RJ-45ケーブルを挿入し、ネットワークへの接続を行います。

■側面



名称	説明
リセットボタン	付属のAC アダプタを接続します。
Power ON/OFF スイッチ	RJ-45ケーブルを挿入し、ネットワークへの接続とPoE受電を行います。
Consoleポート	コンソールケーブルを接続します。 CLI（コマンドラインインタフェース）にアクセスする際に使用します。

製品の設置

■イーサネットケーブルの接続

1. イーサネットケーブルの一端を、本製品の背面にある RJ-45 コネクタに接続します。
2. イーサネットケーブルのもう一端を、ルータ／スイッチ等のネットワーク機器に接続します。

■ACアダプタの接続

付属のACアダプタを使用して、本製品に電源を投入します。

1. 付属の AC アダプタを本製品に接続します。
2. AC アダプタのプラグを電源コンセントに接続します。

メモ

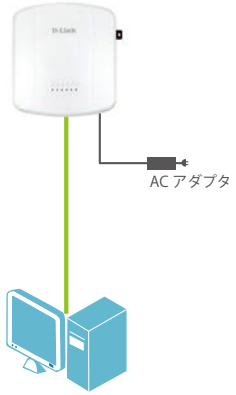
電源が供給されると、POWER LED が点灯します。

■管理用PCへの接続

本製品の設定を行うには、管理用PCを使用して本製品のWeb GUIにアクセスする必要があります。

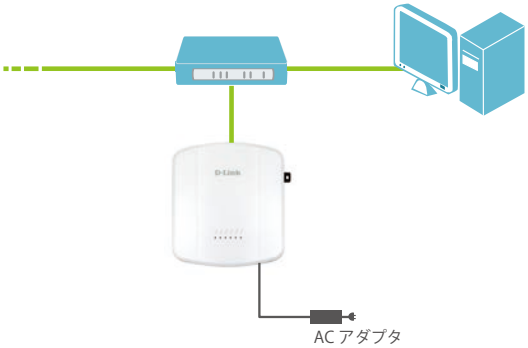
● 直接接続

本製品と管理用PCをUTPケーブルで直接接続します。



● LAN接続

本製品を、管理用PCが接続しているハブに接続します。



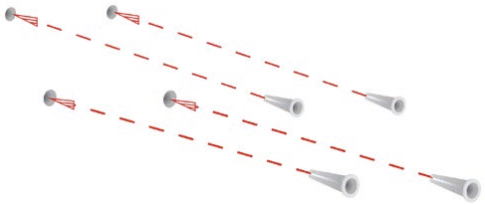
メモ

Web GUIへのアクセス、ログイン方法の詳細は『WEB GUI画面について：p.22 』を参照してください。

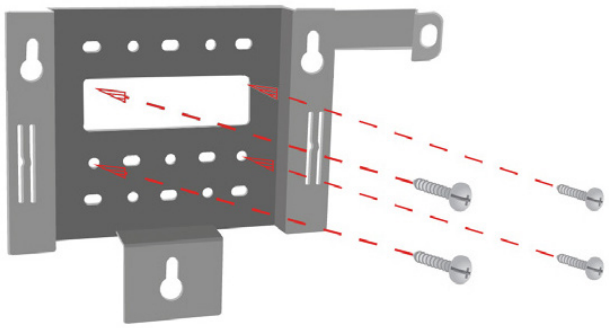
■マウントキットによる設置

本製品は、マウントキットを使用して壁面や天井に設置することができます。設置の際は以下の手順を参照してください。

1. アクセスポイントを取り付ける壁または天井にマウントプレートを合わせます。
2. プラスティックアンカーをつける場所にマークをつけます。
3. マークした場所に穴をあけ、アンカーを挿入します。

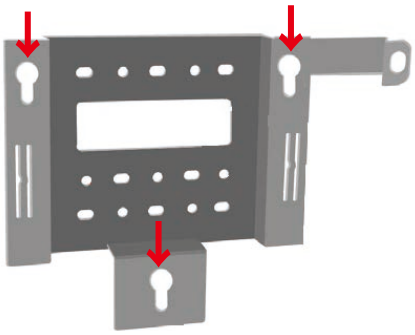


4. アンカー用の長いネジを使用し、マウントプレートを壁面に取り付けます。



5. 残りのネジを本製品の底面 3 箇所にとりつけます。

6. マウントプレートにある 3 箇所の溝に手順 5 でとりつけたネジを合わせ、スライドさせて取り付けます。



WEB GUI画面について

■Web GUI画面へのログイン

メモ

- 本製品の設定は、UTPケーブルで接続したPCから行います。設定を始める前に、本製品とPCをUTPケーブルで接続してください。
- 本製品のIPアドレスとPCのIPアドレスは、同じサブネット内に設定してください。
  例）本製品のIPアドレス：10.90.90.91/8、PCのIPアドレス：10.90.90.100/8
- PCのプロキシサーバ機能は無効にしてください。
  ■手順：
  Windowsの「スタート」＞「コントロールパネル」＞「インターネットオプション」＞「接続」タブ＞「LANの設定」の順にクリックし、「LAN にプロキシサーバを使用する」のチェックを外します。

1. Web ブラウザを起動します。

2. Web ブラウザに本製品の IP アドレスを入力します。

メモ

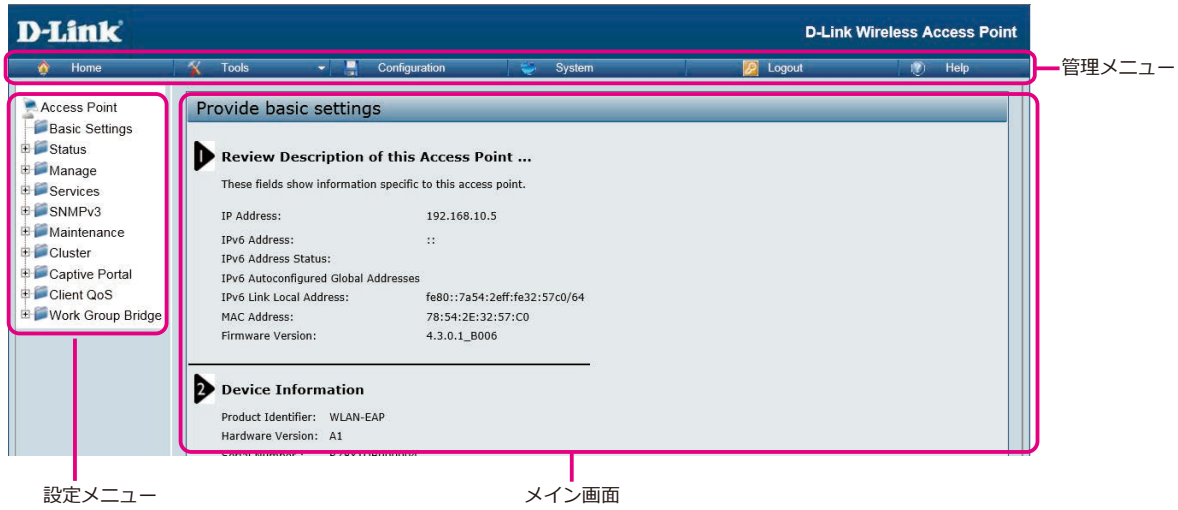
- IPアドレスの初期値は「10.90.90.91」です。
- ご使用のネットワークでDHCP サーバを使用していて自動的にネットワーク情報が設定される場合は、Web ブラウザに本製品の新しい IP アドレスを入力します。
  DHCPによって割り当てられた新しいIPアドレスがわからない場合は、以下の手順でIPアドレス情報を取得してください。
  - 管理者コンピュータとアクセスポイントをシリアルケーブルで接続し、端末エミュレーションソフトウェアを使用してCLI（command-line-interface）に接続します。
    ターミナルソフトウェアの設定は下記の通りです。
    ・ボーレート：115200
    ・データビット：8
    ・パリティ：none
    ・ストップビット：1
    ・フロー制御：none
  - ログイン画面で、ユーザ名およびパスワードに「admin」と入力します。
    プロンプトが表示されたら、「get management」と入力します。
  - コマンド出力としてアクセスポイントの IP アドレスが表示されます。
    このアドレスをWeb ブラウザのアドレスに入力してください。

3. ログイン画面で [User Name] と [Password] を入力 [Logon] をクリックします。

工場出荷時の設定は以下です。
- User Name：admin
- Password：admin

■Web GUI画面の構成

WEB GUI画面の構成について説明します。



● 管理メニュー

- Home :
  ホーム画面を表示します。ホーム画面では、IPアドレスやファームウェアバージョンなどの情報を確認できます。

- Tools :
  ファームウェアのアップロードや、時刻設定を行います。詳しい設定内容については以下を参照してください。
  - Basic Settings:『ホーム画面:p.24 』
  - Upgrade:『Upgrade (ファームウェアアップグレード) :p.80 』
  - Time Settings (NTP):『Time Settings (時間設定) :p.72 』

- Configuration :
  コンフィグレーションファイルのバックアップ／アップロードや、本製品の再起動／工場出荷時設定へのリセットを行います。詳しい設定内容については以下を参照してください。
  - 『Configuration (コンフィグレーションの保存・リストア) :p.79 』

- System :
  本製品の再起動／工場出荷時設定へのリセットを行います。詳しい設定内容については以下を参照してください。
  - 『Maintenance (メンテナンス) :p.80 』

- Logout :
  WEB GUIからのログアウトを行います。

- Help :
  ヘルプ画面が表示されます。

● 設定メニュー

設定メニューをクリックし、各機能の設定を行います。
詳しい設定内容についてはマニュアルの3章-9章を参照してください。

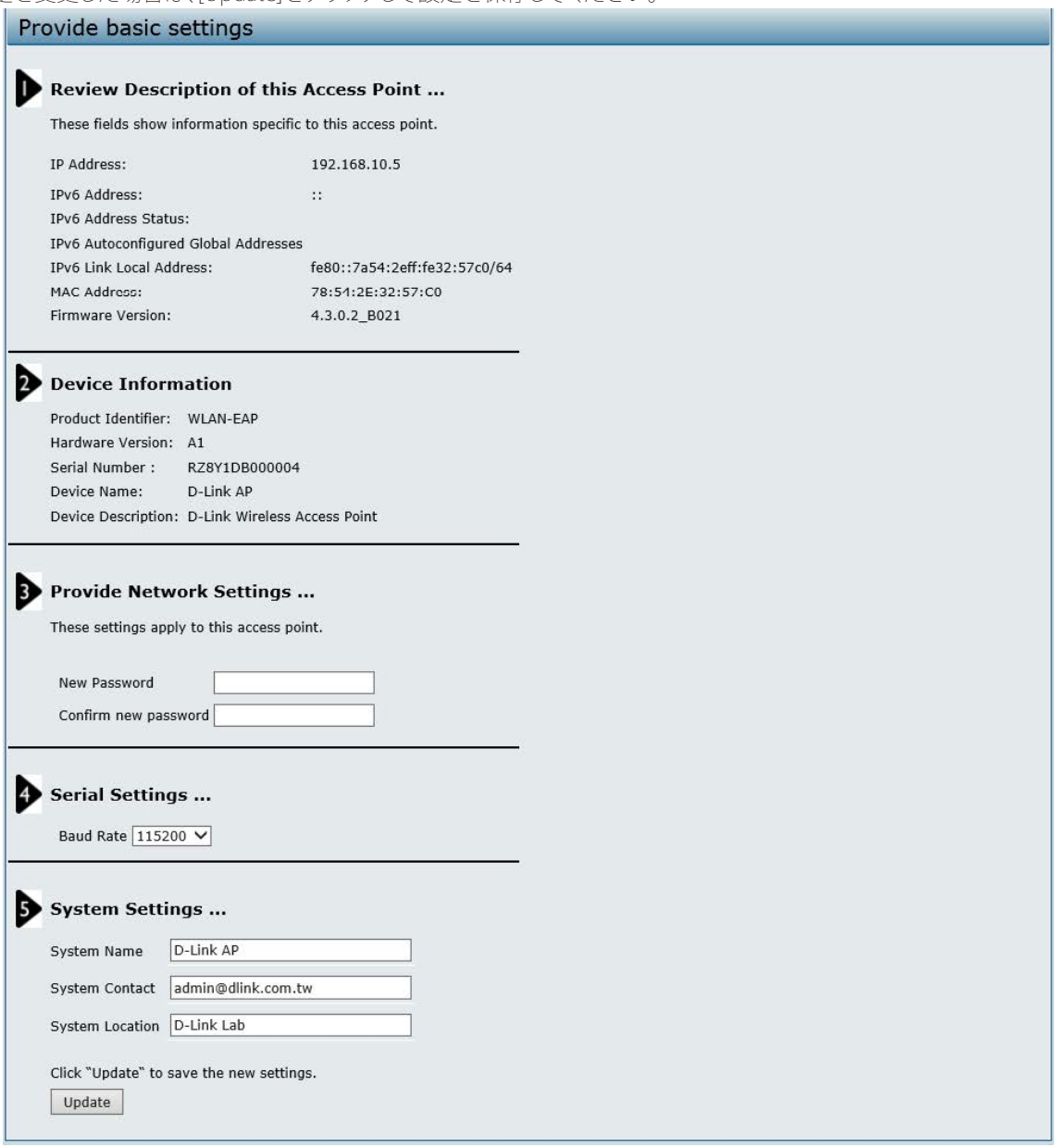
● メイン画面

設定メニューおよび管理メニューで選択した項目の設定画面が表示されます。

■ホーム画面

管理メニューの[Home]または設定メニューの[Basic Settings]をクリックすると、以下の画面が表示されます。
IPアドレスやファームウェアバージョンの確認のほか、システム名の変更やログインパスワードを変更することができます。

設定を変更した場合は、[Update]をクリックして設定を保存してください。



◆ **Review Description of this Access Point**	本製品のIPアドレスとMACアドレス、ファームウェアーバージョンが表示されます。 • [IP Address]：本製品に割り当てられているIP アドレスです。 • [IPv6 Address]：本製品に割り当てられているIPv6アドレスです。 • [IPv6 Address Status]： 本製品の管理インタフェースに設定されたスタティックIPv6 アドレスの状態を表示します。 - [Operational]：管理中 - [Tentative]：試験状態（初期値） • [IPv6 Auto Configured Global Addresses]：本製品の管理インタフェースに自動的に設定されたグローバルIPv6 アドレスを表示します。 • [IPv6 Link Local Address]：ローカルの物理的なリンクによって使用されるIPv6 リンクローカルアドレスです。IPv6 Neighbor 探索プロセスを使用して割り当てられるため、変更はできません。 • [MAC Address]：本製品のMAC アドレスを表示します。 • [Fimware Version]：現在のファームウェアバージョンです。
◆ **Device Information**	本製品のハードウェアバージョンやシリアルナンバーなど、デバイス情報が表示されます。 • [Product Identifier]：本製品のハードウェアモデルです。 • [Hardware Version]：本製品のハードウェアバージョンです。 • [Serial Number]：本製品のシリアルナンバーです。 • [Device Name]：本製品のデバイス名です。 • [Device Description]：本製品のハードウェア情報です。
◆ **Provide Network Settings**	シリアル接続を行う際のボーレートを設定します。接続をするときは、お使いのターミナルソフトウェアのボーレートをここで設定した数値にあわせる必要があります。 • 選択肢：[9600][19200][38400][57600][115200] • 初期値：[115200]
◆ **System Settings**	本製品の名称を入力します。 この名前はここでだけ表示されるもので、管理者が本製品を識別するための名称です。 64 文字までの半角英数字を入力します。（例：My AP）

コンソールポートを使用した管理

■CLI を使用した IP アドレスの参照

コンソールポートを使用し、CLIでネットワーク情報の設定を行う方法について説明します。

メモ

・本製品のDHCP クライアント機能は、初期設定で有効になっています。
DHCP クライアント機能が有効になっていると、本製品をDHCP サーバが存在するネットワークに接続した場合、自動的にIP アドレスを取得します。
Web GUIを使用して本製品を管理するためには、本製品のIP アドレスをWeb ブラウザに入力する必要があります。

1. モデムケーブルを使用して、VT100/ANSI 端末かワークステーションをコンソール（シリアル）ポートに接続します。

   PC、Apple やUNIX のワークステーションと接続する場合は、ハイパーターミナルなどの端末エミュレーションプログラムを起動してください。

2. 端末エミュレーションプログラムの設定を以下に合わせてください。
   - データ速度 : 115,200bps
   - データビット : 8
   - パリティ : なし
   - ストップビット : 1
   - フロー制御 : なし

3. 「Enter」キーを押すとログインプロンプトが表示されます。
   ユーザ名とパスワードを入力してください。
   - 初期値/ユーザ名 :「admin」、パスワード :「admin」

4. ログインに成功すると、画面のプロンプトが 「DLINK-WLAN-AP #」に変わります。

5. プロンプトが表示されたら、「get management」と入力し、IP アドレスを確認します。

```
#DLINK-WLAN-AP# get management
Property                    Value
------------------------------------------
vlan-id                     1
interface                   brtrunk
static-ip                   10.90.90.91
static-mask                 255.0.0.0
ip                          10.90.90.91
mask                        255.0.0.0
mac                         78:54:2E:32:57:C0
dhcp-status                 up
static-ipv6                 ::
static-ipv6-mask
ipv6
ipv6-mask
ipv6-status                 up
ipv6-autoconfig-status      up
static-ipv6                 ::
static-ipv6-prefix-length   0
dhcp6-status                up
```

■CLI を使用したイーサネット設定

以下の表のコマンドを使用してイーサネット（有線）インタフェースの値を参照および設定します。

アクション	コマンド
DNS 名を確認する	`get host id`
DNS 名を設定する	`set host id <host_name>` 例：`set host id lab-ap`
イーサネット（有線）内部インタフェースの現在の設定を確認する	`get management`
管理VLAN ID を設定する	`set management vlan-id <1-4094>`
タグなしVLAN 情報を参照する	`get untagged-vlan`
タグなしVLAN を有効にする	`set untagged-vlan status up`
タグなしVLAN を無効にする	`set untagged-vlan status down`
タグなしVLAN ID を設定する	`set untagged-vlan vlan-id <1-4094>`
接続タイプを参照する	`get management dhcp-status`
DHCP を接続タイプとして使用する	`set management dhcp-status up`
スタティック IP を接続タイプとして使用する	`set management dhcp-status down`
スタティック IP アドレスを設定する	`set management static-ip <ip_address>` 例：`set management static-ip 10.10.12.221`
サブネットマスクを設定する	`set management static-mask <netmask>` 例：`set management static-mask 255.255.255.0`
デフォルトゲートウェイを設定する	`set static-ip-route gateway <ip_address>` 例：`set static-ip-route gateway 10.10.12.1`
DNS ネームサーバモード（Dynamic= up Manual=down）を参照する	`get host dns-via-dhcp`

DNS ネームサーバにスタティックなIP アドレスを使用するように設定する（ダイナミックモードから手動モードへの変更）	`set host dns-via-dhcp down`
	`set host static-dns-1 <ip_address>`
	`set host static-dns-2 <ip_address>`
	例：`set host static-dns-1 192.168.23.45`

DNS ネームサーバにDHCP により割り振られるIP アドレスを使用するように設定する（手動モードからダイナミックモードへの変更）	`set host dns-via-dhcp up`

例:
管理用VLAN ID を「123」に設定し、すべてのトラフィックがタグ付けされてVLAN ID を持つように、タグなしVLAN を無効にします。

```
DLINK-WLAN-AP# set management vlan-id 123
dman: Restarting DHCPv6 client
DLINK-WLAN-AP# set untagged-vlan status down
dman: Restarting DHCPv6 client
DLINK-WLAN-AP# get management
Property                  Value
------------------------------------------
vlan-id                   123
interface                 brtrunk
static-ip                 10.90.90.91
static-mask               255.0.0.0
ip                        10.90.90.91
mask                      255.0.0.0
mac                       78:54:2E:32:57:C0
dhcp-status               down
static-ipv6               ::
static-ipv6-mask
ipv6
ipv6-mask
ipv6-status               up
ipv6-autoconfig-status    up
static-ipv6               ::
static-ipv6-prefix-length 0
dhcp6-status              up

DLINK-WLAN-AP#              get untagged-vlan
Property Value
---------------
vlan-id 1
status down
DLINK-WLAN-AP#
```

■CLI を使用したIEEE 802.1X 認証の設定

以下の表のコマンドを使用してイーサネット(有線)インタフェースの値を参照および設定します。

アクション	コマンド
802.1X サプリカント設定を表示する	get dot1x-supplicant
802.1X サプリカントを有効にする	set dot1x-supplicant status up
802.1X サプリカントを無効にする	set dot1x-supplicant status down
802.1X ユーザ名を設定する	set dot1x-supplicant user <name>
802.1X ユーザのパスワードを設定する	set dot1x-supplicant password <password>

例:802.1X サプリカント機能を有効にし、ユーザ名を「wlanAP」、パスワードを「 test1234」に登録します。

```
DLINK-WLAN-AP# set dot1x-supplicant status up
DLINK-WLAN-AP# set dot1x-supplicant user wlanAP
DLINK-WLAN-AP# set dot1x-supplicant password test1234
DLINK-WLAN-AP# get dot1x-supplicant
Property       Value
-------------------------
status         up
user           wlanAP
eap-method     md5
debug          off
cert-present   no
cert-exp-date  Not Present
DLINK-WLAN-AP#
```

インストールの確認

本製品がLAN に接続し、ネットワークに無線クライアントが接続していることを確認してください。無線ネットワークの基本設定を確認した後、詳細設定を行うことで、さらにセキュリティ性の高い詳細な設定を行うことができるようになります。

1. 本製品を LAN に接続します。

   本製品および管理者用コンピュータを1 つのハブに接続している場合、本製品は既にLAN に接続しています。次に無線クライアントのテストを行います。
   本製品を直接ケーブルでご使用のコンピュータに接続している場合は、以下の手順で行います。
   - 本製品とコンピュータのケーブルを外します。
   - 本製品をイーサネットケーブルでLAN に接続します。
   - イーサネットケーブルまたは無線LAN カードを使用して、コンピュータをLAN に接続します。

2. 無線クライアントと LAN の接続を確認します。

   無線クライアントデバイスから、本製品を検出して接続することで本製品を確認します。

3. 詳細設定により、本製品にセキュリティ設定をします。

   無線ネットワークが動作し、本製品が無線クライアントに接続した後に、セキュリティレイヤの追加、複数のVAP の作成、および性能設定を行うことができます。

重要

- 本製品において、同時に複数の設定変更を行うことはできません。1 人以上の管理者が管理者用Web 画面にログインして設定変更を行う場合、複数のユーザによって指定された設定の変更が適用される保証はありません。
- 初期設定ではセキュリティ設定が行われていないため、どの無線クライアントからもアクセスポイントやご使用のネットワーク に接続することができます。『VAP（仮想アクセスポイントの設定）：p.52 』を参照し、セキュリティの設定を行ってください。

無線アクセスポイントのセキュリティ設定

有効な各仮想アクセスポイント（VAP）にセキュリティ設定を行い、セキュアな無線クライアントを設定します。1 つの物理アクセスポイントで、最大16 個のVAP を設定して複数のアクセスポイントのように設定することができます。初期値では、有効なVAP は1 つです。各VAP に異なるセキュリティモードを設定して無線クライアントの接続を制御することができます。

それぞれの無線機器にはVAP ID が0-15 の16 個のVAP があります。初期値ではVAP 0 のみ有効です。
VAP 0 の初期設定は以下の通りです。

- VLAN ID：1
- Broadcast SSID：有効
- SSID：dlink1
- Security：なし
- MAC Authentication Type：なし
- Redirect Mode：なし

他のすべてのVAP は初期値で無効です。VAP 1-15 のSSID の初期値 は、dlinkx（x はVAP ID）になります。

本製品への不正アクセスを防止するために、VAP の初期値および有効にした各VAP のセキュリティオプションで「None」以外を選択して変更を行うことをお勧めします。

重要

- 本製品において、同各VAP のセキュリティ設定方法に関する詳細は、『VAP（仮想アクセスポイントの設定）：p.52 』を参照してください。

Status

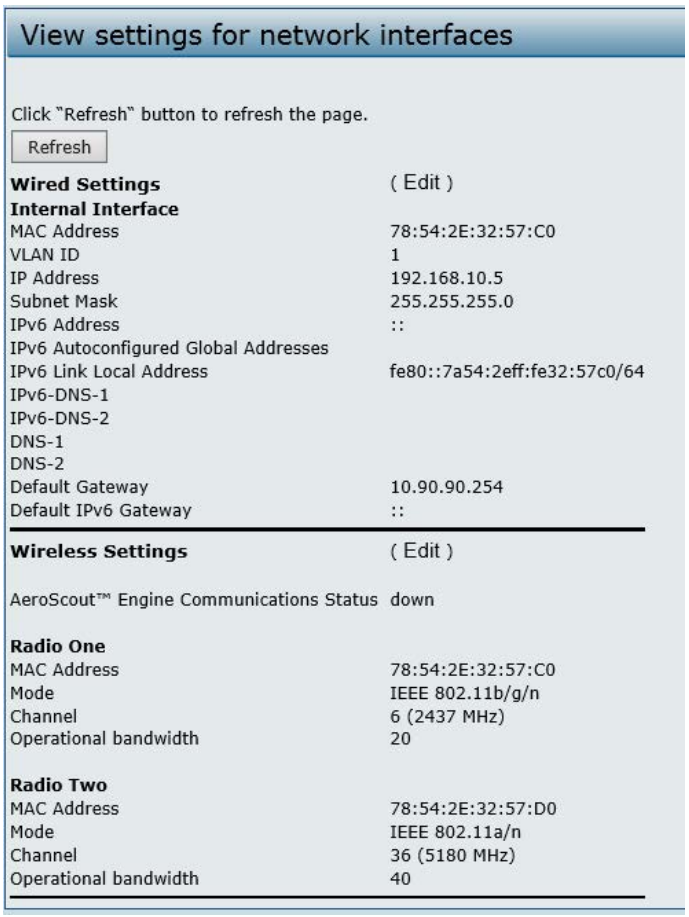
3

Statusメニューでは、アクセスポイントのステータスを参照することができます。

Interfaces（インタフェースステータスの参照）

[Status] > [Interface]

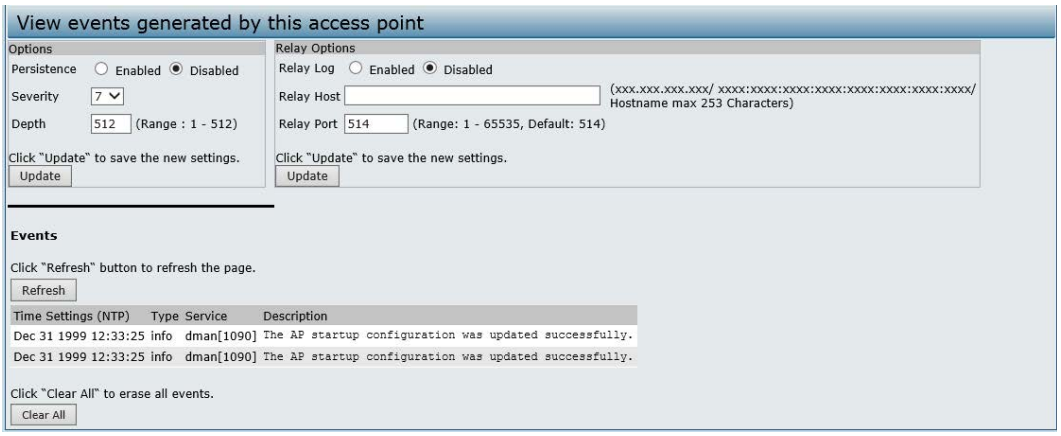
イーサネットLAN および無線LAN（WLAN）設定を参照します。



◆ **Refresh**	表示を更新します。
◆ **Wired Settings**	有線設定（内部インタフェース）の情報です。 イーサネットMACアドレス、管理VLAN ID、IPアドレス（IPv4 および IPv6）、サブネットマスク、およびDNS情報が表示されます。 これらの設定を変更する場合は、[Edit]をクリックして設定画面を表示します。有線設定の詳しい内容については、『Ethernet Settings（イーサネット設定）：p.43 』を参照してください。
◆ **Wireless Settings**	無線設定の情報です。 各無線インタフェースに関連するMAC アドレス（参照のみ）も表示されます。 設定を変更する場合には、[Edit]をクリックして設定画面を表示します。 無線設定の詳しい内容については、『Wireless Settings（無線設定）：p.46 』および『Radio（無線詳細設定）：p.47 』を参照してください。

Events（イベントの参照）

アクセスポイントへの無線クライアントの接続や認証など、アクセスポイントに発生するシステムイベントを表示します。
また、[Options]および[Relay Options]エリアでログ保存の詳細設定を行うことができます。



重要

- 本アクセスポイントは、ネットワークタイムプロトコル（NTP）を使用して日付と時間情報を取得します。このデータはUTC 形式（グリニッジ標準時）で通知されます。通知時間を使用する場所の時間に変換する必要があります。ネットワークタイムプロトコルの設定については、『Time Settings（時間設定）：p.72 』を参照してください。

■Options (持続性ログオプションの設定)

システムの再起動時にログを保持するか削除するか設定を行います。設定を適用するには、[Update]をクリックします。

重要

- ログの保持を有効にすると、不揮発性メモリが消耗して、ネットワーク性能が低下する可能性があります。問題をデバッグする場合にだけ、ログの保持を有効化してください。また、デバッグの終了後にログの保持を無効化してください。
- 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

◆ **Persistence**	アクセスポイントの再起動時のログの保持を有効または無効にします。 • [Enabled]: アクセスポイントの再起動時にログを削除しません。不揮発性メモリにログを保存します。 • [Disabled]: 揮発性メモリにログを保存します。揮発性メモリ内のログは、システムの再起動時に削除されます。
◆ **Severity**	不揮発性メモリに記載するログの重要度レベルを指定します。 • 0：emergency • 3：error • 6：info • 1：alert • 4：warning • 7：debug • 2：critical • 5：notice 例：2 を指定すると、critical、alert、およびemergency ログが不揮発性メモリに記載され、3-7 の重要度レベルを持つログメッセージが揮発性メモリに出力されます。
◆ **Depth**	不揮発性メモリに保存可能なログの数を設定します。ここで設定した数値を超過すると、最も古いログは新しいログに書き換えられます。(設定可能範囲：1-512)
◆ **Update**	設定を適用します。

■Relay Options (カーネルメッセージ用のログリレーホストの設定)

カーネルログはシステムログ内に記載されるシステムイベントやフレームの破棄のようなエラー状態を含むカーネルメッセージを持つ総合的なリストです。

Web マネージャを使用してアクセスポイントに対して直接カーネルログメッセージを参照することはできません。はじめにSyslog プロセスが動作し、ご使用のネットワークでSyslog のログリレーホストとして動作するリモートサーバを設定します。その後、リモートサーバにSyslog メッセージを送信するように本製品を設定することができます。
アクセスポイントのSyslog メッセージをリモートログサーバが収集することで、以下の機能を提供します。

- 複数のアクセスポイントからSyslog メッセージの収集を行うことができます。
- 単一のアクセスポイントで保持するメッセージよりも長いヒストリを保存することができます。
- スクリプト化された管理操作およびアラートを起動することができます。

カーネルログリレーを使用するためには、リモートサーバを設定してSyslog メッセージを受信する必要があります。リモートログホストを設定する手順は、リモートホストなどご使用のシステムタイプによって異なりま

重要

- Syslog プロセスは、ポート514 を初期値で使用します。このポートの初期値を使用することをお勧めします。
  ログポートを再設定する場合には、Syslog ポートに割り当てるポート番号が別のプロセスに使用されていないことをご確認ください。

● ログリレーホストの有効／無効化

ログリレーの有効／無効化、および設定を行うためには、以下の表に示すログリレーオプションを設定して[Update]をクリックします。設定を適用するには、[Update]をクリックします。

◆ **Relay Log**	ログリレーを有効または無効にします。 ・[Enabled]:リモートホストへのログメッセージの送信を本製品に許可します。 ・[Disabled]:すべてのログメッセージをローカルシステムに保持します。
◆ **Relay Host**	リモートログサーバのIP アドレスまたはDNS 名を指定します。
◆ **Relay Port**	リレーホストのSyslog プロセス用のポート番号を指定します。初期値は514 です。
◆ **Update**	設定を適用します。

重要

- 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

ログリレーホストを[Enabled]（有効）にして[Update]をクリックすると、リモートログ出力がアクティブになります。
アクセスポイントは、ログリレーホストを設定した方法により、リモートログサーバモニタ、定義したカーネルログファイル、または他のストレージに対して表示用のカーネルメッセージをリアルタイムに送信します。

ログリレーホストを[Disabled]（無効）にして[Update]ボタンをクリックすると、リモートログ出力は無効になります。

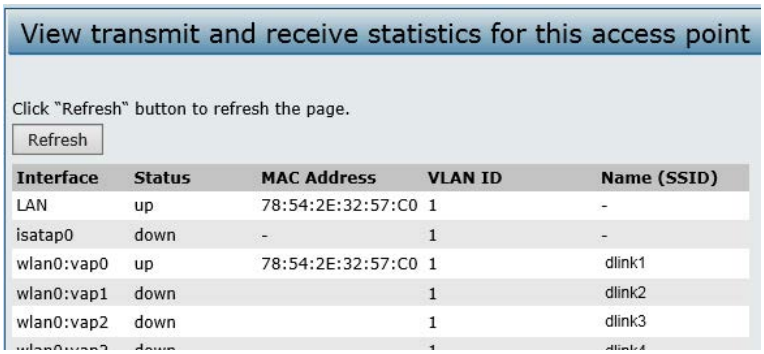
Transmit/Receive（送受信した統計情報の参照）

[Status] > [Transmit/Receive]

各インタフェースのステータス情報と、アクセスポイント上のイーサネットインタフェースおよび無線インタフェース上のVAP で送受信したデータの統計情報を表示します。

表示されるのは、アクセスポイントが最後に起動してから現在までの統計情報です。
アクセスポイントを再起動した場合、再起動後の送受信データの合計が表示されます。

● 各インタフェースのステータス情報



◆ Interface	イーサネットまたはVAPインタフェース名が表示されます。
◆ Status	各インタフェースのステータス（[Up]（アクティブ）または[down]（ダウン））が表示されます。
◆ MAC Address	各インタフェースのMACアドレスが表示されます。
◆ VLAN ID	各インタフェースのVLAN IDが表示されます。 VLAN を使用して、同じアクセスポイントに複数の内部ネットワークおよびゲストネットワークを確立することができます。VLAN IDの設定については、『VAP（仮想アクセスポイントの設定）：p.52 』を参照してください。
◆ Name (SSID)	ワイヤレスネットワークの名称（SSID）が表示されます。SSIDの設定については、『VAP（仮想アクセスポイントの設定）：p.52 』を参照してください。
◆ Refresh	表示を更新します。

● 送受信したトラフィックの統計情報

Transmit

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	1944	783347	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	1022	256535	0	0	0
wlan0:vap1	0	0	0	0	0

● 受信したトラフィックの統計情報

Receive

Interface	Total packets	Total bytes	Total drop packets	Total drop bytes	Errors
LAN	642	82085	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	1009	124104	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	0	0	0	0	0

◆ Interface	イーサネットまたはVAPインタフェースが表示されます。
◆ Total packets	送受信したパケットの合計が表示されます。
◆ Total bytes	送受信したバイト数の合計が表示されます。
◆ Total drop packets	送受信で破棄されたパケットの合計が表示されます。
◆ Total drop bytes	送受信で破棄されたバイト数の合計が表示されます。
◆ Errors	送受信したデータに関連するエラーの合計が表示されます。

Client Associations（無線クライアント情報）

[Status] > [Client Associations]

アクセスポイントに接続するクライアントの情報を参照します。

◆ **Refresh**	表示を更新します。
◆ **Network**	クライアントが接続しているネットワークが表示されます。
◆ **Station**	無線クライアントのMAC アドレスが表示されます。
◆ **Status**	IEEE 802.11 認証の認証状況および接続状態が表示されます。IEEE 802.1Xの認証および接続の状態を示すものではありません。 ・[Authenticated]:無線クライアントは認証済みです。 ・[Associated]:無線クライアントがアクセスポイントに接続されています。
◆ **From Station**	無線クライアントから受信したパケットおよびバイト数と、受信後に破棄されたパケットおよびバイト数が表示されます。
◆ **To Station**	アクセスポイントから送信したパケットおよびバイト数と、送信後に破棄されたパケットおよびバイト数が表示されます。

メモ

・[Network]でwlan0vap2 と表示されている場合、クライアントがRadio 1 上のVAP2 に接続していることを意味します。wlan0 と表示されている場合はRadio 1 上のVAP0 、wlan1と表示されている場合はRadio 2 のVAP0 に接続していることを意味します。

重要

・[Status]は、IEEE 802.1Xの認証および接続の状態を示すものではありません。
アクセスポイントのセキュリティモードが[None]または[Static WEP]に設定されている場合は、[Status]欄の表示内容が無線クライアントの認証および接続の状態と一致します。
アクセスポイントのセキュリティモードが[IEEE 802.1X]または[WPA]に設定されている場合、クライアントの接続がこのタブ上で（IEEE 802.11 セキュリティ経由で）認証されたものとして表示されますが、実際にはセキュリティの2 番目のレイヤを通じてアクセスポイントに認証されていません。

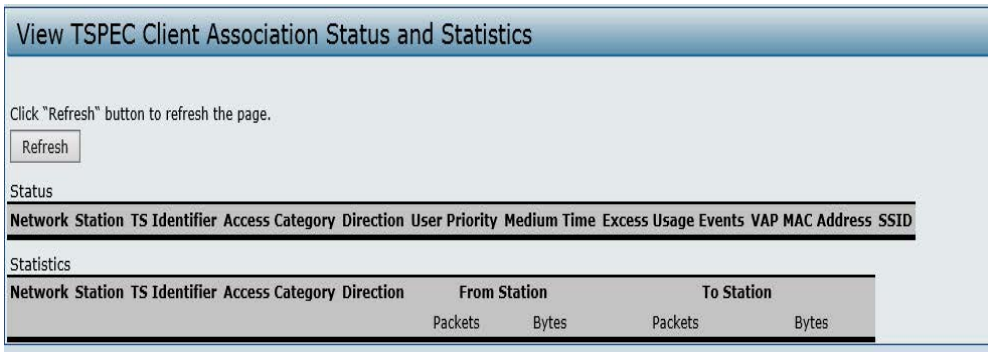
TSPEC Client Associations（TSPEC クライアント情報）

[Status] > [TSPEC Client Associations]

TSPECクライアントの送受信統計情報やクライアントのステータスなどの基本情報を表示します。
クライアントの動作が始まってから全ての送受信統計が表示されます。

メモ

- TSPEC（Traffic Specification）は、QoSの有効な無線クライアントとアクセスポイント間で必要な帯域を通信前に予約する機能です。音声やビデオのトラフィックストリームに対して動作します。
  トラフィックストリームとは、特定のユーザ優先度に属する無線クライアントによって識別されたデータパケットの集合体です。
  - 音声トラフィックストリームの例：WiFi認定電話からの音声優先トラフィックなどのCODEC 対応データパケット
  - ビデオトラフィックストリームの例：企業サーバからのビデオ会議の提供を優先する無線ラップトップからの映像トラフィック



◆ **Refresh**	表示を更新します。
Status	
◆ **Network**	クライアントが接続しているネットワークが表示されます。
◆ **Station**	無線クライアントのMAC アドレスが表示されます。
◆ **TS Identifier**	TSPEC トラフィックセッションを識別します。(範囲：0 - 7)
◆ **Access Category**	トラフィックストリームのアクセスカテゴリです。(voice（音声）/ video(ビデオ))
◆ **Direction**	トラフィックストリームの方向性です。以下の3 つがあります。 • uplink（アップリンク） • downlink（ダウンリンク） • bidirectional（双方向）
◆ **User Priority**	トラフィックストリームのユーザ優先値（UP）です。 UP はIP ヘッダのUP ポーションとして各パケットともに送信されます。 主な値は、6 または 7：音声、4 または 5：映像、です。 他の優先トラフィックセッションにより数値は変動します。
◆ **Medium Time**	トラフィックストリームが通信媒体で占める帯域の値（32μ 秒/ 秒単位で計算）です。
◆ **Excess Usage Events**	クライアントがTSPEC に構成された[Medium Time]を越えた数が表示されます。
◆ **VAP**	クライアントが接続する仮想アクセスポイントが表示されます。
◆ **MAC Address**	仮想アクセスポイントのMAC アドレスが表示されます。
◆ **SSID**	クライアントのSSIDが表示されます。
Statistics	
◆ **Network**	クライアントが接続しているネットワークが表示されます。
◆ **Station**	無線クライアントのMAC アドレスが表示されます。
◆ **TS Identifier**	TSPEC トラフィックセッションを識別します。(範囲：0 - 7)
◆ **Access Category**	トラフィックストリームのアクセスカテゴリです。(voice（音声）/ video(ビデオ))
◆ **Direction**	トラフィックストリームの方向性です。以下の3 つがあります。 • uplink（アップリンク） • downlink（ダウンリンク） • bidirectional（双方向）
◆ **From Station**	無線クライアントから受信したパケットの数と、受信後に破棄されたパケットの数が表示されます。また、以下のパケットについても表示されます。 • 超過TSPEC • AP にリクエストされても構築されなかったTSPEC
◆ **To Station**	無線クライアントから送信されたパケットの数と、送信後に破棄されたパケットの数が表示されます。また、以下のパケットについても表示されます。 • 超過TSPEC • AP にリクエストされても構築されなかったTSPEC

◆ Link Integrity モニタリング機能

本アクセスポイントでは、各接続クライアントに対して接続を検証するために。、Link Integrity モニタリング機能を提供します。Link Integrity モニタリング機能を使用すると、アクセスポイントはトラフィックが通過しない場合に数秒ごとにクライアントにデータパケットを送信します。これにより、通常のトラフィックの交換期間内であってもクライアントが範囲外に出てしまったことを検出することができます。データパケットが認識されないと、接続解除メッセージを受信しなくてもクライアントの接続は300秒以内にリストから破棄されます。

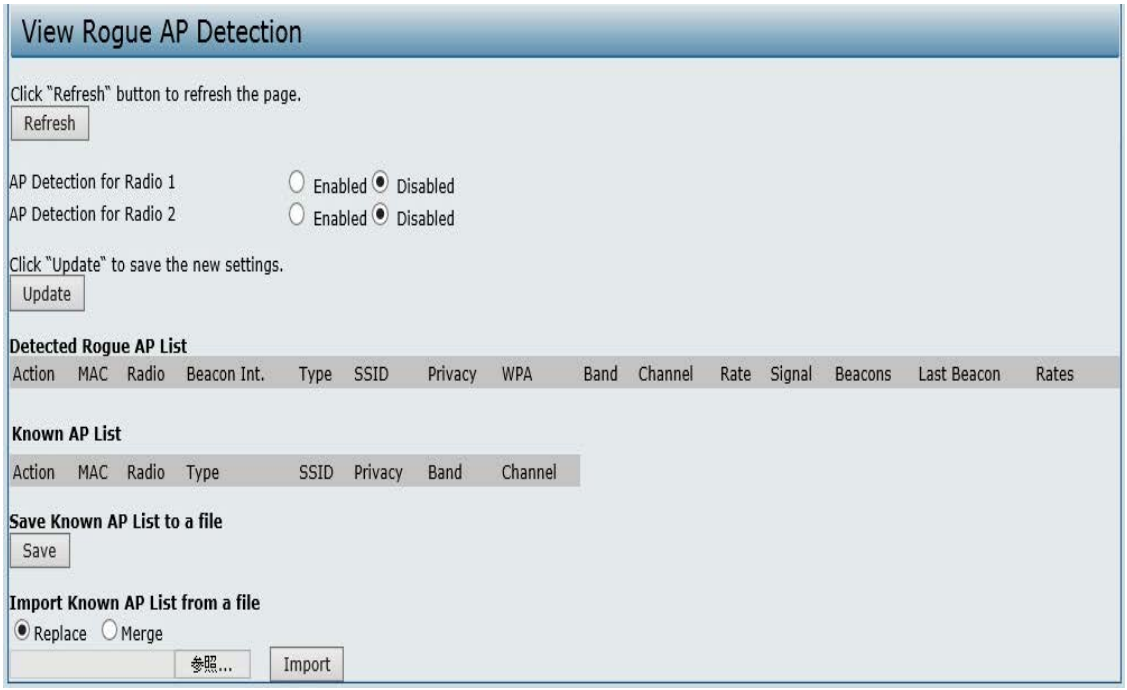
Rogue AP Detection（不正アクセスポイントの検知）

[Status] > [Rogue AP Detection]

周囲にある不正アクセスポイントの検知を行います。
検知を行うには、[AP Detection for Radio 1]または[AP Detection for Radio 2]で[Enabled]を選択し、検知を有効にする必要があります。設定を適用するには[Update]をクリックしてください。

メモ

- [Detected Rouge AP List]（検出された不正AP リスト）と[Known AP List]（既知のAP リスト）は検出したアクセスポイントの情報を表示するのみです。検出したアクセスポイントに対して、セキュリティポリシーの変更などの管理動作を行うことはできません。

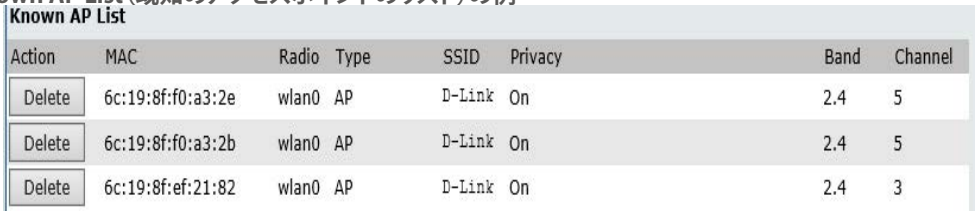


◆ Detected Rogue AP List（検出した不正アクセスポイントのリスト）の例

Detected Rogue AP List

Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates
Grant	6c:19:8f:ef:21:82	wlan0	100	AP	D-Link	On	On	2.4	3	1		2	Wed Dec 31 16:00:13 1969	1,2,5.5,11,6,9,12,18,24,36,48,54
Grant	6c:19:8f:f0:a3:2e	wlan0	100	AP	D-Link	On	On	2.4	5	1		2	Wed Dec 31 16:00:14 1969	1,2,5.5,11,6,9,12,18,24,36,48,54
Grant	6c:19:8f:ef:20:d7	wlan0	100	AP	D-Link	On	On	2.4	5	1		1	Wed Dec 31 16:00:14 1969	1,2,5.5,11,6,9,12,18,24,36,48,54

◆ Known AP List（既知のアクセスポイントのリスト）の例



Known AP List

Action	MAC	Radio	Type	SSID	Privacy	Band	Channel
Delete	6c:19:8f:f0:a3:2e	wlan0	AP	D-Link	On	2.4	5
Delete	6c:19:8f:f0:a3:2b	wlan0	AP	D-Link	On	2.4	5
Delete	6c:19:8f:ef:21:82	wlan0	AP	D-Link	On	2.4	3

◆ **Refresh**	表示を更新します。
◆ **AP Detection for Radio 1**	2.4GHz帯でのアクセスポイント検知を[Enabled]（有効）または[Disabled]（無効）にします。
◆ **AP Detection for Radio 2**	5GHz帯でのアクセスポイント検知を[Enabled]（有効）または[Disabled]（無効）にします。
◆ **Update**	設定を適用します。
Detected Rogue AP List	
検出したアクセスポイントのリストが表示されます。	
◆ **Action**	[Grant]をクリックし、検出した不正アクセスポイントを既知のアクセスポイントに変更できます。
◆ **MAC**	MAC アドレが表示されます。
◆ **Radio**	どの無線インタフェースがアクセスポイントを検出したかが表示されます。 • [wlan0]: 無線インタフェース1 • [wlan1]: 無線インタフェース2
◆ **Beacon Int.**	アクセスポイントのビーコン間隔が表示されます。
◆ **Type**	アクセスポイントのタイプが表示されます。 • [AP]: インフラストラクチャモードで動作するアクセスポイントです • [Ad hoc]: アドホックモードで動作するアクセスポイントです。 通常のアクセスポイントを使用せずに、アドホックモードに設定されたステーション同士が直接相互に通信します。
◆ **SSID**	アクセスポイントのSSIDが表示されます。
◆ **Privacy**	セキュリティ設定の有無が表示されます。 • [Off]: アクセスポイントにセキュリティ設定がされていません。 • [On]: アクセスポイントにセキュリティ設定がされています。
◆ **WPA**	WPA セキュリティが[On]（有効）または[Off]（無効）であるか表示されます。
◆ **Band**	クセスポイントの周波数帯が表示されます。 • [2.4]:周波数帯は2.4GHzです。接続モードはIEEE 802.11b、802.11g、または 802.11n のいずれかです。 • [5]:周波数帯は5GHzです。接続モードはIEEE 802.11a 、802.11n、または802.11acモードのいずれかです。
◆ **Channel**	アクセスポイントが現在ブロードキャストを行っているチャンネルを示します。
◆ **Rate**	アクセスポイントの現在のデータ伝送速度が表示されます。
◆ **Signal**	アクセスポイントが出力するシグナルの強さが表示されます。 バーの上でマウスポインタを動作させると、数値（dB）強さを示します。
◆ **Beacons**	最初に検出された後にアクセスポイントが受信したビーコンの総数を表示します。
◆ **Last Beacon**	アクセスポイントが最後のビーコンを受信した日時を表示します。
◆ **Rates**	アクセスポイントがサポートしているデータ伝送速度が表示されます。
Known AP List	
既知のアクセスポイントのリストが表示されます。	
◆ **Action**	[Delete]をクリックすると、既知のアクセスポイントを検出した不正アクセスポイントに変更できます。
◆ **MAC**	MAC アドレが表示されます。
◆ **Radio**	どの無線インタフェースがアクセスポイントを検出したかが表示されます。 • [wlan0]: 無線インタフェース1 • [wlan1]: 無線インタフェース2
◆ **Type**	アクセスポイントのタイプが表示されます。 • [AP]: インフラストラクチャモードで動作するアクセスポイントです • [Ad hoc]: アドホックモードで動作するアクセスポイントです。 通常のアクセスポイントを使用せずに、アドホックモードに設定されたステーション同士が直接相互に通信します。
◆ **SSID**	アクセスポイントのSSIDが表示されます。
◆ **Privacy**	セキュリティ設定の有無が表示されます。 • [Off]: アクセスポイントにセキュリティ設定がされていません。 • [On]: アクセスポイントにセキュリティ設定がされています。
◆ **Band**	アクセスポイントの周波数帯が表示されます。 • [2.4]:周波数帯は2.4GHzです。接続モードはIEEE 802.11b、802.11g、または 802.11n のいずれかです。 • [5]:周波数帯は5GHzです。接続モードはIEEE 802.11a 、802.11n、または802.11acモードのいずれかです。
◆ **Channel**	アクセスポイントが現在ブロードキャストを行っているチャンネルを示します。

● 既知のアクセスポイントのリストをエクスポートする

既知のアクセスポイントのリストは、以下の手順でファイルにエクスポートすることができます。

1. [Save Known AP List to a File] の [Save] をクリックします。
2. [保存] をクリックします。

メモ

ファイル名の初期値は「Rogue1.cfg」です。ファイルには既知のアクセスポイントとして登録されたアクセスポイントのMACアドレスが記載されています。ファイルはテキストエディタを使用して閲覧できます。

● 既知のアクセスポイントのリストをインポートする

既知のアクセスポイントのリストは、以下の手順でインポートすることができます。

1. [Import Known AP List from a file] の [Import] または [Merge] を選択します。
   - [Replace]:現在Web GUIに表示されている既知のアクセスポイントリストに、インポートするファイルを上書きします。
   - [Merge]:現在Web GUIに表示されている既知のアクセスポイントリストに、インポートするファイルをマージします。
2. [参照] をクリックしインポートするファイルを選択します。
3. [Import] をクリックします。

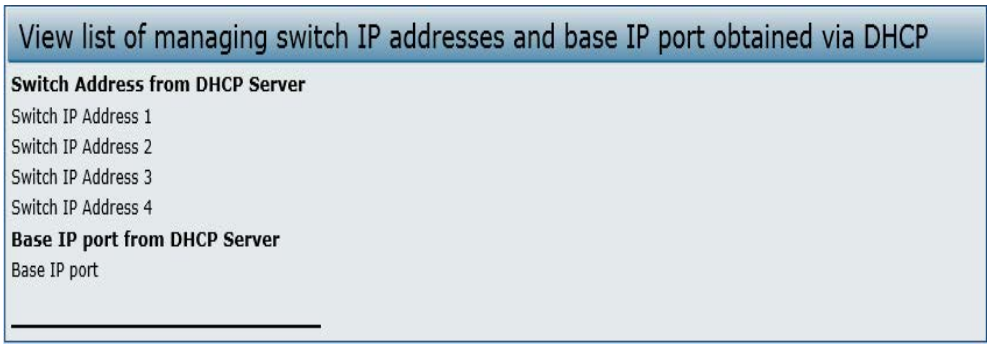
メモ

インポートするファイルの拡張子は「.cfg」または「.txt」である必要があります。

Managed AP DHCP（管理アクセスポイントのDHCP情報）

[Status] > [Managed AP DHCP]

DHCPサーバから取得したワイヤレススイッチのIPアドレスとベースIPポートを確認できます。



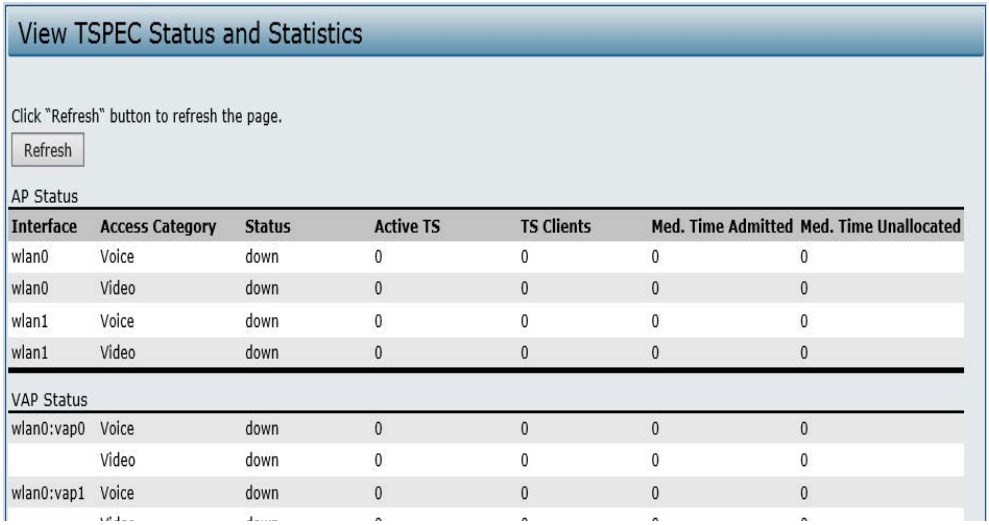
メモ

ワイヤレススイッチのIP アドレス情報を持つアクセスポイントのDHCP 要求に応じるようにDHCP サーバを設定する方法については、ワイヤレススイッチのマニュアルを参照してください。

TSPEC Status and Statistics（TSPEC ステータスと統計情報）

[Status] > [TSPEC Status and Statistics]

本画面では以下の情報を表示します。
- 無線によるTSPEC セッションの要約情報
- VAP によるTSPEC セッションの要約情報
- 全ての無線インタフェースのTSPEC VAP のリアルタイム送受信統計情報

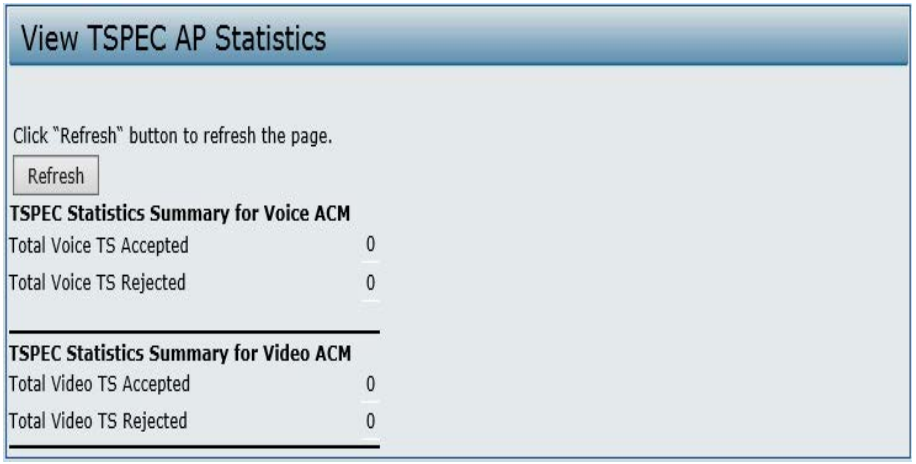


◆ **Refresh**	表示を更新します。
AP Status / VAP Status	
◆ **Interface**	[Radio]または[VAP]インタフェースのどちらかを表示します。
◆ **Access Category**	トラフィックストリームの種類（音声/ 映像）を示す現在のアクセスカテゴリを表示します。
◆ **Status**	関連するアクセスカテゴリのTSPEC セッションが有効または無効を表示します。 設定上のステータスを表示しています。現在の動作状況を表示しているとは限りません。
◆ **Active TS**	無線とアクセスカテゴリで現在動作中のTSPEC トラフィックストリームの数を表示します。
◆ **TS Clients**	無線とアクセスカテゴリで現在動作中のTSPEC トラフィックストリームクライアントの数を表示します。
◆ **Medium Time Admitted**	このアクセスカテゴリにおいて、トラフィックストリームが通信媒体で占めることができる時間（32μ 秒/ 秒単位で計算）です。本値はこのトラフィックストリームに許可された帯域の最大帯域以下である必要があります。
◆ **Medium Time Unallocated**	トこのアクセスカテゴリにおいて、トラフィックストリームが通信媒体で使用していない時間の値（32μ 秒/ 秒単位で計算）です。
Transmit and Receive Statistics	
◆ **Total Packets**	指定のアクセスカテゴリの無線で受信/ 送信されたTS パケットの総量が表示されます。
◆ **Total Bytes**	指定のアクセスカテゴリの無線で受信/ 送信されたTS バイトの総量が表示されます。
◆ **Total Voice Packets**	指定のVAP の無線で受信/ 送信されたTS 音声パケットの総量が表示されます。
◆ **Total Voice Bytes Total**	指定のVAP の無線で受信/ 送信されたTS 音声バイトの総量が表示されます。
◆ **Video Packets Total**	指定のVAP の無線で受信/ 送信されたTS 映像パケットの総量が表示されます。
◆ **Video Bytes**	指定のVAP の無線で受信/ 送信されたTS 映像バイトの総量が表示されます。

TSPEC AP Statistics（TSPEC AP 統計情報）

[Status] > [TSPEC AP Statistics]

本製品によって許可/ 破棄された音声/ 映像トラフィックストリームの情報について表示します。

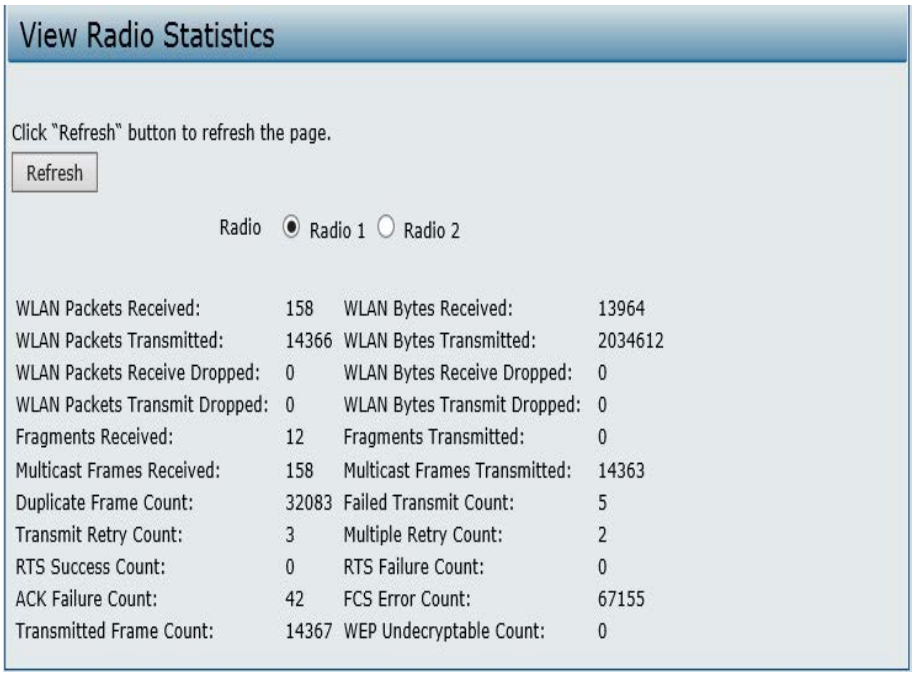


◆ **Refresh**	表示を更新します。
◆ **TSPEC Statistics Summary for Voice ACM**	許可された、または破棄された音声トラフィックストリームの総量が表示されます。
◆ **TSPEC Statistics Summary for Video ACM**	許可された、または破棄された映像トラフィックストリームの総量が表示されます。

Radio Statistics（無線統計情報）

[Status] > [Radio Statistics]

本製品で送受信されたパケット/ バイトについての詳しい情報を表示します。

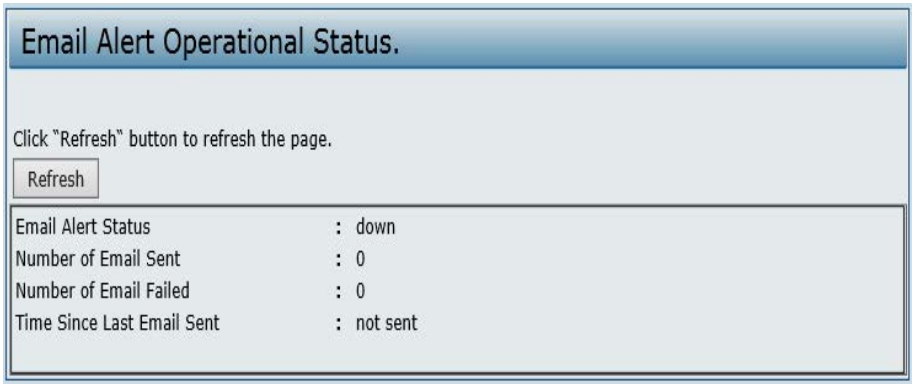


◆ **Refresh**	表示を更新します。
◆ **Radio**	[Radio 1]または[Radio 2]を選択し、参照する無線帯域を指定します
◆ **WLAN Packets Received**	無線インタフェース上でアクセスポイントが受信した総パケット数。
◆ **WLAN Bytes Received**	無線インタフェース上でアクセスポイントが受信した総バイト数。
◆ **WLAN Packets Transmitted**	無線インタフェース上でアクセスポイントが送信した総パケット数。
◆ **WLAN Bytes Transmitted**	無線インタフェース上でアクセスポイントが送信した総データ量。単位はバイトです。
◆ **WLAN Packets Receive Dropped**	無線インタフェース上でアクセスポイントが受信し、破棄されたパケット数。
◆ **WLAN Bytes Receive Dropped**	無線インタフェース上でアクセスポイントが受信し、破棄されたバイト数。
◆ **WLAN Packets Transmit Dropped**	無線インタフェース上でアクセスポイントが送信し、破棄されたパケット数。
◆ **WLAN Bytes Transmit Dropped**	無線インタフェース上でアクセスポイントが送信し、破棄されたバイト数。
◆ **Fragments Received**	タイプがデータまたは管理の、正しく受信されたMPDU フレーム数。
◆ **Fragments Transmitted**	タイプがデータまたは管理で個別アドレスまたはマルチキャストアドレスを含む、送信したMPDU フレーム数。
◆ **Multicast Frames Received**	宛先MAC アドレス中にマルチキャストビットが設定されている、受信したMSDUフレーム数。
◆ **Multicast Frames Transmitted**	宛先MAC アドレス中にマルチキャストビットが設定されている、正しく送信したMSDUフレーム数。
◆ **Duplicate Frame Count**	シーケンス制御フィールドでduplicate（冗長）と示されているフレームを受信した回数。
◆ **Failed Transmit Count**	超過により、MSDU が正しく送信されなかった回数。
◆ **Transmit Retry Count**	1 度以上のリトライ後にMSDUが正しく送信された回数。
◆ **Multiple Retry Count**	2 度以上のリトライ後にMSDUが正しく送信された回数。
◆ **RTS Success Count**	RTS フレームの応答として受信されたCTSフレームの数。
◆ **RTS Failure Count**	RTS フレームの応答として受信されなかったCTSフレームの数。
◆ **ACK Failure Count**	想定していたACKフレームが受信されなかった数。
◆ **FCS Error Count**	受信したMPDU により検知したFCSエラー数。
◆ **Transmitted Frame Count**	送信に成功したMSDUの数。
◆ **WEP Undecryptable Count**	暗号化されたフレームのうち、暗号化の必要なしと示されているもの、または受信デバイスがプライバシーオプションを使用していないために廃棄されたフレームの数。

Email Alert Status（Eメールアラートステータス）

[Status] > [Email Alert Status]

本製品のSyslogメッセージにより送信されたEメールアラートのステータスが表示されます。



◆ **Refresh**	表示を更新します。
◆ **Email Alert Status**	Eメールアラートのステータスが表示されます。初期値は[down]です。 ・[up]:Eメールアラートが動作しています。 ・[down]:Eメールアラートは動作していません。
◆ **Number of Email Sent**	送信したE-Mail の総量が表示されます。
◆ **Number of Email Failed**	送信に失敗したE-Mail が表示されます。
◆ **Time Since Last Email Sent**	最後にE-mail を送信した日時が表示されます。

Manage

4

イーサネット設定や無線設定など、本製品の管理方法について説明します。

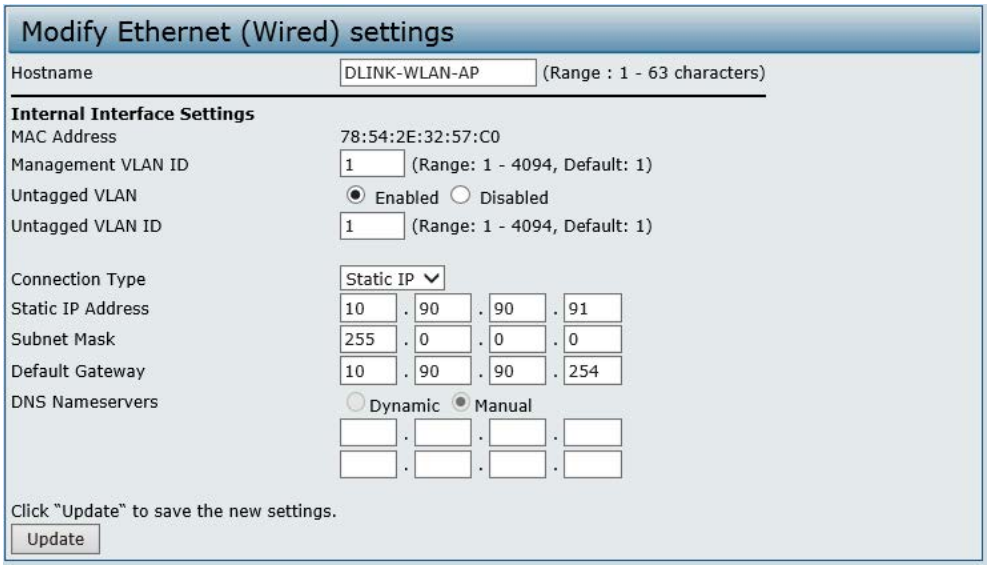
Ethernet Settings（イーサネット設定）

[Manage] > [Ethernet Settings]

イーサネットの設定を行います。
初期設定では本製品上のDHCP クライアントは自動的にネットワーク情報に関する要求をブロードキャストします。
スタティックIP アドレスを使用する場合、DHCP クライアントを無効にして、手動でIP アドレスおよび他のネットワーク情報を設定する必要があります。
マネジメントVLAN は初期値でVLAN 1 のタグなしVLAN です。ネットワーク上に異なるVLAN ID を使用した管理用VLAN が存在している場合は、アクセスポイントのマネジメントVLAN のVLAN ID を変更する必要があります。

重要

・設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

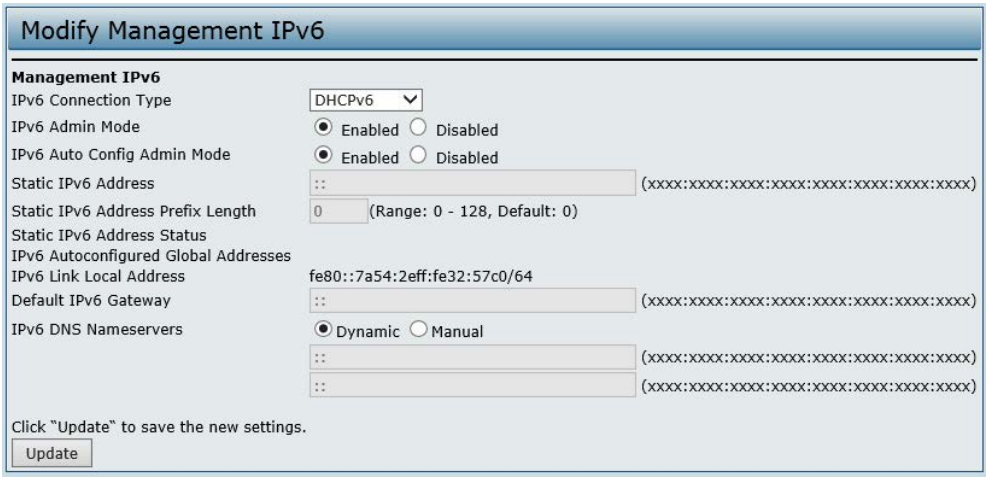


◆ **Hostname**	アクセスポイントのDNS 名（ホスト名）を入力します。 ・入力可能文字数：1-63 半角英字 ・入力可能な文字：英数字、および「-」（ダッシュ） ・条件：英字で開始し、英字または数字で終了する必要があります。
◆ **MAC Address**	イーサネットポートのLAN インタフェースのMAC アドレスが表示されます。
◆ **Management VLAN ID**	マネジメントVLANのIDを設定します。マネジメントVLANは、アクセスポイントへのアクセスに使用するIP アドレスに関連付けされているVLAN です。 ・設定可能範囲：1-4094
◆ **Untagged VLAN**	タグなし VLANを有効または無効にします。 ・[Enabled]:Untagged VLANを有効にします。 ・[Disabled]:Untagged VLANを無効にします。すべてのトラフィックはVLAN ID をタグ付けされます。
◆ **Untagged VLAN ID**	タグなしVLANのIDを設定します。ここで設定するVLAN 上のトラフィックは、VLAN ID をタグ付けされません。 ・設定可能範囲：1-4094
◆ **Connection Type**	接続タイプを設定します。 ・[Static IP]:スタティック（固定）のIP アドレス、サブネットマスク、DNS、およびゲートウェイを使用します。 ・[DHCP]:DHCP サーバから自動的にIP アドレス、サブネットマスク、DNS、およびゲートウェイ情報を取得します。
◆ **Static IP Address**	IPアドレスを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
◆ **Subnet Mask**	サブネットマスクを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
◆ **Default Gateway**	デフォルトゲートウェイを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
◆ **DNS Nameservers**	DNS のモードを選択します。 ・[Manual]:固定のIP アドレスを使用します。 ・[Dynamic]:DNS サーバのIP アドレスはDHCP を通じて自動的に割り当てられます。接続タイプを[Static IP]に設定した場合は選択できません。
◆ **Update**	設定を適用します。

Management IPv6（IPv6設定）

[Manage] > [Management IPv6]

IPv6アドレスの設定を行います。

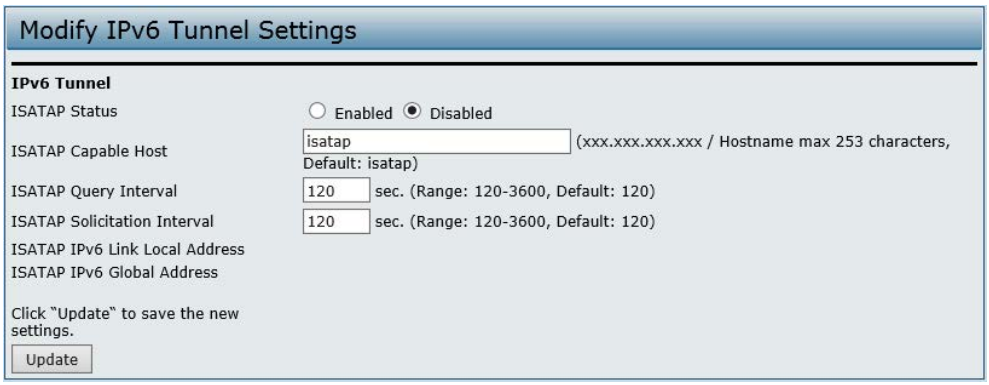


◆ **IPv6 Connection Type**	接続タイプを設定します。 • [Static IPv6]:固定のIPv6 アドレスを使用します。 • [DHCPv6]:DHCPv6サーバから自動的にIPv6 アドレスを取得します。
◆ **IPv6 Admin Mode**	アクセスポイントへのIPv6 管理アクセスを[Enabled](有効)または[Disabled](無効)にします。
◆ **IPv6 Auto Config Admin Mode**	アクセスポイントへのIPv6 自動アドレス設定を[Enabled](有効)または[Disabled](無効)にします。 有効にした場合、自動IPv6 アドレス設定とゲートウェイ設定は、LAN ポートで受信したルータ広告を処理することで許可されます。アクセスポイントは、複数の自動設定されたIPv6 アドレスを持つことができます。
◆ **Static IPv6 Address**	スタティック（固定）のIPv6 アドレスを入力します。 接続タイプを[DHCPv6]に設定した場合は入力できません。
◆ **Static IPv6 Address Prefix Length**	スタティックIPv6 のプレフィックス長入力します。 接続タイプを[DHCPv6]に設定した場合は入力できません。 • 設定可能範囲：1-128
◆ **Static IPv6 Address Status**	スタティックIPv6 アドレスのステータスが表示されます。
◆ **IPv6 Autoconfigured Global Addresses**	自動的に1 つ以上のIPv6 アドレスをアクセスポイントに割り当てている場合に、アドレスが表示されます。
◆ **IPv6 Link Local Address**	IPv6 Link Local アドレスを表示します。これは、ローカルな物理リンクによって使用されるIPv6 アドレスです。これは、IPv6 Neighbor Discovery プロセスを使用することで割り当てられるため、リンクローカルアドレスを設定するはできません。
◆ **Default IPv6 Gateway**	デフォルトゲートウェイを入力します。 接続タイプを[DHCP]に設定した場合は入力できません。
◆ **IPv6 DNS Nameservers**	DNS のモードを選択します。 • [Manual]:固定のIPv6アドレスを使用します。 • [Dynamic]:DNS サーバのIPv6 アドレスはDHCPv6 を通じて自動的に割り当てられます。接続タイプを[Static IPv6]に設定した場合は選択できません。
◆ **Update**	設定を適用します。

IPv6 Tunnel（IPv6トンネル設定）

[Manage] > [IPv6 Tunnel]

ISATAPによるIPv6トンネルの設定を行います。
ISATAP(Intra-Site Automatic Tunnel Addressing Protocol) は、あるサイト内のローカルIPv4ネットワークにおいて、IPv6通信を実現するトンネリング技術です。

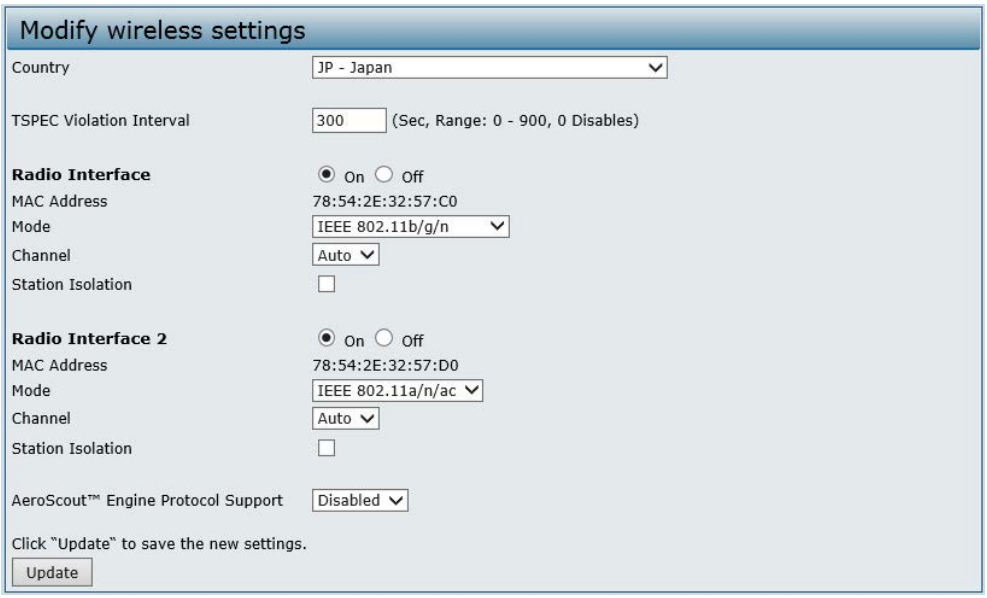


◆ **ISATAP Status**	ISATAPを[Enabled](有効)または[Disabled](無効)にします。
◆ **ISATAP Capable Host**	ホスト名を設定します。 ・初期値:isatap
◆ **ISATAP Query Interval**	クエリインターバルを設定します。 ・初期値:120 ・設定可能範囲:120-3600
◆ **ISATAP Solicitation Interval**	ソリシテーションインターバルを設定します。 ・初期値:120 ・設定可能範囲:120-3600
◆ **ISATAP IPv6 Link Local Address**	IPv6 Link Local アドレスを表示します。
◆ **ISATAP IPv6 Global Address**	IPv6 Globalアドレスを表示します。
◆ **Update**	設定を適用します。

Wireless Settings（無線設定）

[Manage] > [Wireless Settings]

無線の設定を行います。



◆ **Country**	国コードを選択します。
◆ **TSPEC Violation Interval**	クライアントが権限手順を遵守していない場合にレポート（システムログ、SNMP、トラップ）を送信するまでのインターバル（単位:秒）を指定します。
◆ **Radio Interface / Radio Interface2**	無線インタフェースを[On](オン)または[Off](オフ)にします。
◆ **MAC Address**	無線インタフェース1 と2 のMAC アドレスを表示します。
◆ **Mode**	無線インタフェースのモードを選択します。 ここで選択したモードに対応しているクライアントのみが、無線インタフェースに接続できます。 ・Radio Interface - 選択肢：[IEEE 802.11b/g][IEEE 802.11b/g/n][2.4 GHz IEEE 802.11n] ・Radio Interface2 - 選択肢：[IEEE 802.11a][IEEE 802.11a/n][IEEE 802.11a/n/ac][IEEE 802.11n/ac]
◆ **Channel**	無線インタフェースのチャンネルを選択します。 利用可能なチャンネルの範囲は、無線インタフェースのモードによって決定されます。 [Auto]を選択した場合、アクセスポイントは、チャンネルをスキャンして、利用可能なチャンネルを自動的に選択します。
◆ **Station Isolation**	チェックをいれるとステーションアイソレーションが有効になります。 ・無効にした場合： 無線クライアントは、通常通りアクセスポイントを経由してトラフィックを送信することで相互に通信できます。 ・有効にした場合： アクセスポイントは同じVAPおよび同じにある無線クライアント間の通信をブロックします。WDSリンクを経由した、異なるVAP上にあるクライアントとの通信についてはブロックしません。
◆ **AeroScout™ Engine Protocol Support**	AeroScout Engineプロトコルを[Enabled](有効)または[Disabled](無効)にします。
◆ **Update**	設定を適用します。

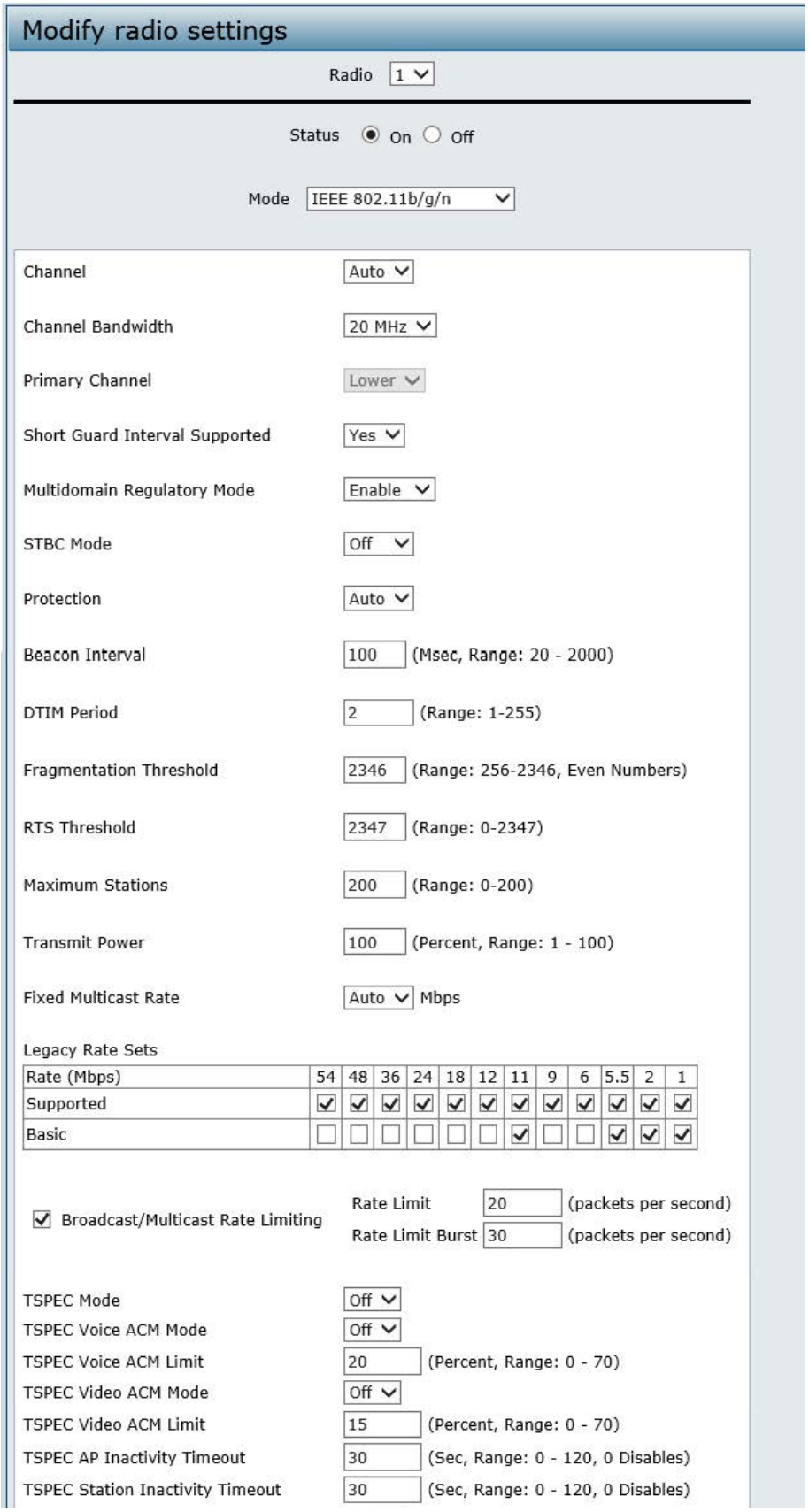
重要

- AeroScout Engineは無線ネットワークの位置情報提供サービスです。
有効にするとAeroscout対応のデバイスが認識され、分析のためデータがAeroscout Engine (AE)に送信されます。
AEは、802.11対応デバイス（アクセスポイントなど）の位置情報を定義します。
- AeroScoutのタグが「T2」「T3」タグのハードウェアのみサポートします。他のタグの場合は、対応しているAeroScout プロトコルが「AeroScout Engine - Access Point Interface Specification, version 2.1」に準じている場合のみサポートしています。
- AeroScoutタグは「802.11 b/g」モードでのみ使用できます。そのため、AeroScoutタグを使用するネットワーク管理者は少なくとも1 つは「802.11b/g」または「802.11b/g/n」モードで検出されるタグのAP の無線である必要があります。「 2.4 GHz IEEE 802.11」モード、または「 5GHZ」モードでは「AeroScout」タグは検出できません。
- AEプロトコルは、検出されたAPが不正APとして認識されることを許可します。本製品 はこの機能をサポートしないため、検出されたAPが不正APとしてレポートされることはありません。
- AEプロトコルはAE サーバとアクセスポイント間の認証や暗号をサポートしていません。
- AEプロトコルはAPスループットに影響する場合があります。

Radio（無線詳細設定）

[Manage] > [Radio]

無線の詳細設定を行います。
本画面の表示内容は、[Radio]で選択した無線帯域と[Mode]で選択したモードによって異なります。



◆ **Radio**	設定する無線帯域を選択します。 • [1]:2.4GHz帯の設定を行います。 • [2]:5GHz帯の設定を行います。
◆ **Status**	無線インタフェースを[On](オン)または[Off](オフ)にします。
◆ **Mode**	無線インタフェースのモードを選択します。 利用可能なモードは、国コードおよび[Radio]で選択した無線帯域によって異なります。 • [1]を選択した場合 - 選択肢：[IEEE 802.11b/g][IEEE 802.11b/g/n][2.4 GHz IEEE 802.11n] • [2]を選択した場合 - 選択肢：[IEEE 802.11a][IEEE 802.11a/n][IEEE 802.11a/n/ac][IEEE 802.11n/ac]
◆ **Channel**	無線インタフェースのチャンネルを選択します。 利用可能なチャンネルの範囲は、無線インタフェースのモードによって決定されます。 [Auto]を選択した場合、アクセスポイントは、チャンネルをスキャンして、利用可能なチャンネルを自動的に選択します。
◆ **Channel Bandwidth**	チャンネルの帯域幅を選択します。
◆ **Primary Channel**	プライマリチャンネルを選択します。 [Channel Bandwidth]を[40 MHz]に選択した場合のみ選択可能です。 • [Upper]:40MHz 帯域の上位20MHz のチャンネルとしてPrimary Channel を設定します。 • [Lower]:40MHz 帯域の下位20MHz のチャンネルとしてPrimary Channel を設定します。
◆ **DFS Support**	DFS機能を[On](オン)または[Off](オフ)にします。 DFS（Dynamic Frequency Selection）とは、無線LANの通信が気象レーダー等に影響を与えないよう、無線LANアクセスポイント側が使用周波数帯を変更する機能です。
◆ **Multidomain Regulatory Mode**	マルチドメイン制御を[Enabled](有効)または[Disabled](無効)にします。
◆ **Short Guard Interval Supported**	ショートガードインターバル機能を[Yes](有効)または[Off](無効)にします。 ガードインターバルとは、送信されるシンボル（ビット）とシンボルの間に挿入される間隔のことです。ショートガードインターバル機能を有効にすると、ガードインターバルを800ナノ秒から400ナノ秒へ短縮することができます。
◆ **STBC Mode**	STBCモードを[On](オン)または[Off](オフ)にします。 STBC（Space Time Block Coding）は、データ送信をより安定させる802.11nの技術です。データストリームが複数のアンテナから送信されるため、受信側がより確実にデータストリームを受信することができます。
◆ **Protection**	保護機能を[Auto](自動)または[Off](オフ)にします。 保護が[Auto]の場合、アクセスポイントの適用範囲内にレガシーデバイスがあると、保護メカニズムが呼び出されます。保護を[Off]にすると、、適用範囲内のレガシークライアントまたはアクセスポイントが802.11n 伝送によって影響を受けることがあります。 この設定はアクセスポイントに接続するクライアントの能力に影響しません。
◆ **Beacon Interval**	ビーコンを送信する間隔を設定します。 ビーコンとは無線ネットワークを同期させるためにアクセスポイントから一定間隔で送信するパケットのことです。 • 選択可能範囲:20 - 2000（ミリ秒）
◆ **DTIM Period**	DTIM間隔を指定します。 DTIM(Delivery Traffic Information Map)メッセージは、ビーコンフレームに含まれる要素です。省電力モードの無線クライアントに対して、送信待ちのデータがあることを伝えます。 DTIM間隔を10に設定した場合は、10 回のビーコンフレーム送信に対して1 度DTIMメッセージが送信されます。 • 選択可能範囲:1-255
◆ **Fragmentation Threshold**	フラグメントしきい値を設定します。 設定したしきい値よりも大きなサイズのパケットを送信する場合、パケットは分割して送信されます。初期設定は「2346」です。電波干渉の可能性がない場合は、初期設定での使用をおすすめします。 • 選択可能範囲:256-2346（バイト）
◆ **RTS Threshold**	RTSしきい値を設定します。 RTSしきい値は、製品が無線LAN機器へパケットを送信する前に、同一ネットワーク内（SSIDが同じ無線LAN機器）へ送信するRTS（Request To Send：送信要求）信号を送信するかどうかを決めるための境界値です。 • 選択可能範囲:256-2347
◆ **Maximum Stations**	本アクセスポイントに一度にアクセスできるステーションの最大数を指定します。 • 選択可能範囲:0-200

◆ **Transmit Power**	本アクセスポイントの送信電力レベルを設定します。 設定した数値が高いほど、アクセスポイントのブロードキャスト範囲が広くなります。 アクセスポイントの数や距離など、お使いの環境に適したレベルを選択してください。
◆ **Fixed Multicast Rate**	アクセスポイントのマルチキャストトラフィック通信速度を選択します。
◆ **Legacy Rate Sets**	アクセスポイントの通信速度設定、およびアクセスポイントが通知をする速度を指定します。 • [Rates]：レート（通信速度）が表示されます。 • [Supported]：サポートさせたいレートを選択します。 • [Basic]：本製品に接続してくるステーション（無線クライアントや他のアクセスポイント）が、本製品への接続を許されるために最低限サポートしていなければならないサポート・レートセットです。
◆ **Broadcast/ Multicast Rate Limiting**	マルチキャストとブロードキャスト速度制限を有効または無効いします。 有効にすると、ネットワークを経由して送信されるパケット数を制限することによって、全体的なネットワーク性能を改善することができます。
◆ **TSPEC Mode**	TSPEC モードを[On](オン)または[Off](オフ)にします。 Wi-Fi を利用した電話など QoS 有効の機器からのトラフィックにアクセスポイントが対応する際などに本機能をオンにします。 • [On]: アクセスポイントはTSPECリクエストに対応します。 • [Off]: アクセスポイントはTSPECリクエストに対応しません。
◆ **TSPEC Voice ACM Mode**	音声アクセスに対するTSPEC Voice ACM モードを[On](オン)または[Off](オフ)にします。 • [On]: 音声トラフィックを送信/ 受信する前にステーションが帯域のTSPEC リクエストをアクセスポイント に送信します。 • [Off]: ステーションはTSPEC リクエストの有無に限らず、音声優先トラフィックを送信/ 受信することが可能です。
◆ **TSPEC Voice ACM Limit**	アクセスポイントが、音声アクセスカテゴリの無線メディアに接続するために送信するトラフィックの上限を設定します。
◆ **TSPEC Video ACM Mode**	ビデオアクセスカテゴリにおける強制アクセス制御を[On](オン)または[Off](オフ)にします。 • [On]: ビデオトラフィックを送信/ 受信する前にステーションが帯域のTSPEC リクエストをAP に送信します。 • [Off]: ステーションはTSPEC リクエストの有無に限らず、ビデオ優先トラフィックを送信/ 受信することが可能です。
◆ **TSPEC Video ACM Limit**	アクセスポイントが、ビデオアクセスカテゴリの無線メディアに接続するために送信するトラフィックの上限を設定します。
◆ **TSPEC AP Inactivity Timeout**	アクセスポイントがアイドル状態のダウンリンクTS を検出し削除するまでの時間を設定します。
◆ **TSPEC Station Inactivity Timeout**	アクセスポイントがアイドル状態のアップリンクTS を検出し削除するまでの時間を設定します。
◆ **TSPEC Legacy WMM Queue Map Mode**	ACM のキュー操作でのレガシートラフィックの混在を許可します。
◆ **Update**	設定を適用します。

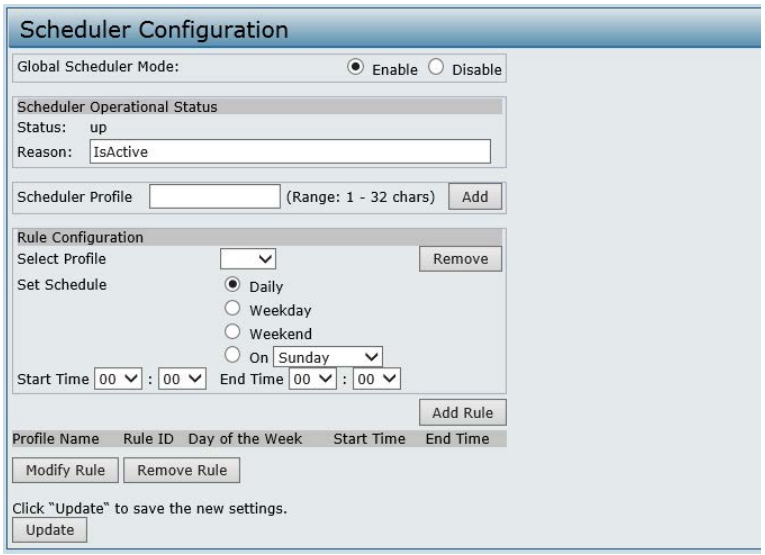
Scheduler Configuration（スケジューラの設定）

[Manage] > [Wireless Settings]

スケジューラの設定を行います。
スケジューラはスタンドアロン使用時に利用できる機能です。無線を自動的に有効/無効にしたり、一日のうちの限られた時間のみ無線クライアントをVAP にアクセスさせたりすることができます。

重要

- 有効なルールのみプロファイルに追加できます。
- 最大16 個までのルールをグループとして1 つのスケジューリングプロファイルにまとめることができます。
- 全く同じ時間ルールを1 つのプロファイルに2 つ以上設定することはできません。



◆ **Global Scheduler Mode**	スケジューラ設定を[Enabled](有効)または[Disabled](無効)にします。
Scheduler Operational Status	
◆ **Status**	スケジューラ設定の状態（[up]:有効、[down]:無効）が表示されます。
◆ **Reason**	ステータスの概要が表示されます。 • [IsActive]:スケジューラ設定が有効です。 • [ConfigDown]:スケジューラ設定が無効です。 • [TimeNotSet]:アクセスポイントの時間設定がされていないため、スケジューラ設定は使用できません。 • [ManagedMode]:アクセスポイントが管理モードであるため、スケジューラ設定は使用できません。
◆ **Scheduler Profile**	プロファイル名を設定→[Add]をクリックして追加します。 最大16 個までのスケジューラプロファイル名を設定できます。（入力可能文字数：32 英文字）
Rule Configuration	
プロファイルに適用するルールを設定します。 設定後、[Add Rule]をクリックして設定を追加します。ルールを修正する場合は[Modify Rule]、ルールを削除する場合は[Remove Rule]をクリックします。	
◆ **Select Profile**	プロファイルを選択します。[Remove]をクリックするとプロファイルを削除できます。
◆ **Set Schedule**	日を選択します。
◆ **Start Time**	無線/VAP の管理が可能な時間の開始時刻を選択します。 「時時：分分」の24 時間方式です。<00-24>:<00-59> から設定します。
◆ **End Time**	無線/VAP の管理が可能な時間の終了時刻を選択します。 「時時：分分」の24 時間方式です。<00-24>:<00-59> から設定します。
◆ **Update**	設定を適用します。

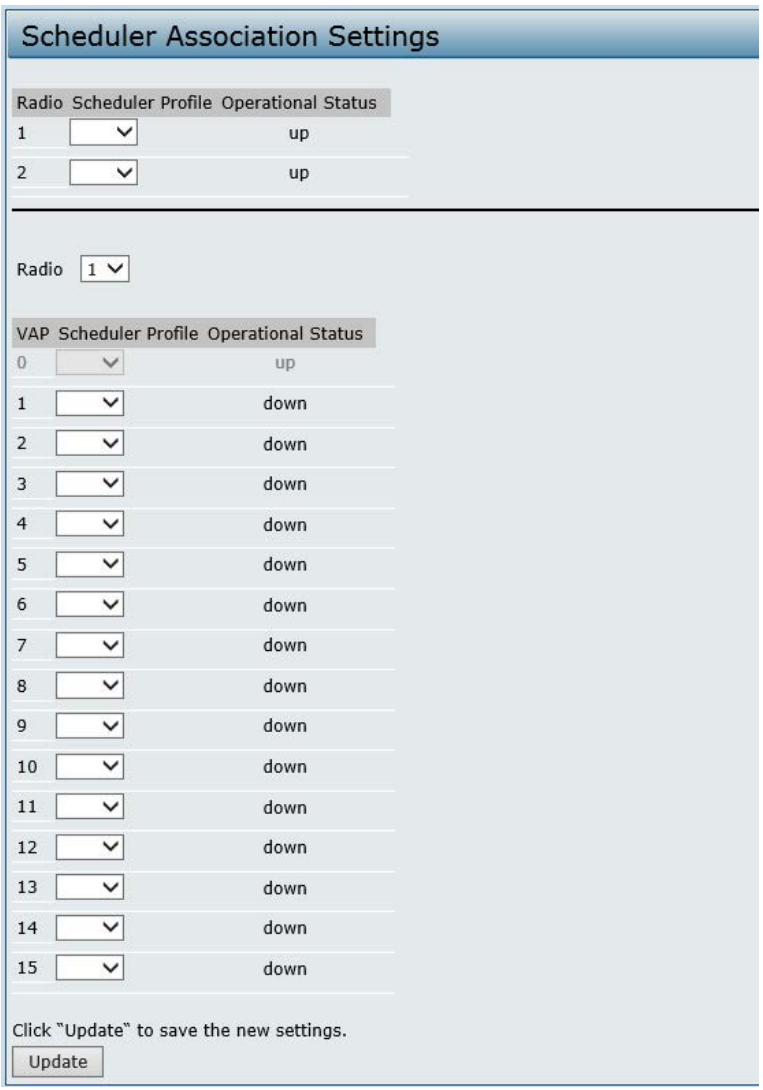
メモ

- アクセスポイントの時間設定については、『Time Settings（時間設定）：p.72 』を参照してください。

Scheduler Association Settings（スケジューラ関連設定）

[Manage] > [Scheduler Association Settings]

スケジューラプロファイルをの無線またはVAP と連携させます。



無線とスケジューラプロファイルを連携させます。	
◆ **Radio**	[1]は「Radio 1」、[2]は「Radio 2」を表します。
◆ **Scheduler Profile**	無線と連携させるスケジューラプロファイルを選択します。
◆ **Operational Status**	スケジューラ設定の状態（[up]:有効、[down]:無効）が表示されます。
無線とスケジューラプロファイルを連携させます。	
◆ **VAP**	VAPが表示されます。
◆ **Scheduler Profile**	VAPと連携させるスケジューラプロファイルを選択します。
◆ **Operational Status**	スケジューラ設定の状態（[up]:有効、[down]:無効）が表示されます。
◆ **Update**	設定を適用します。

VAP（仮想アクセスポイントの設定）

[Manage] > [VAP]

VAP(仮想アクセスポイント)の設定を行います。

イーサネットのVLAN と同様に、無線LAN はVAP により複数のブロードキャストドメインに分割することができます。VAP は 1 つの物理的なアクセスポイントに複数のアクセスポイントをシミュレートします。各無線帯域は最大16 個のVAP をサポートしています。

各VAP に対して、無線クライアントアクセスを制御するためにセキュリティモードをカスタマイズすることができます。また、各VAP は固有のSSID を持つことができます。複数のSSID は、ただ一つのアクセスポイントをネットワークにある別のシステムに対して2 つ以上であるように見せます。

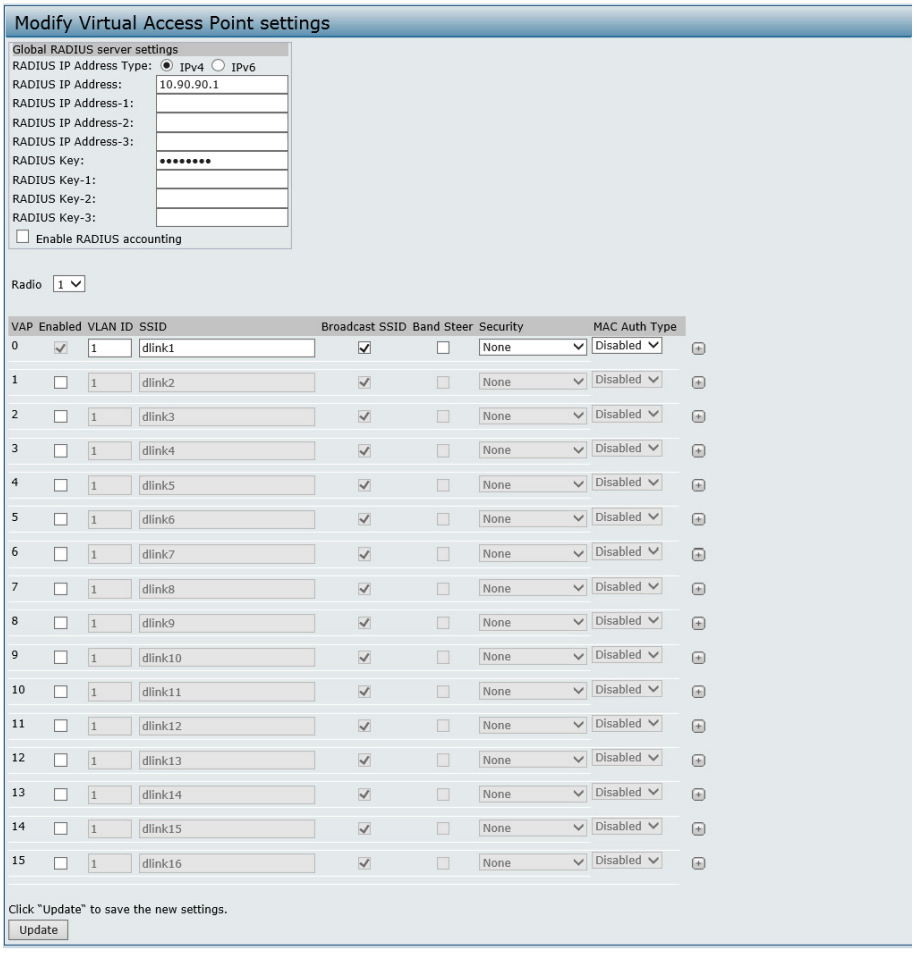
VAP を設定することで、ブロードキャストやマルチキャストのトラフィック管理が容易になり、ネットワークのパフォーマンスも向上します。VLAN が同じ無線帯域、または、異なる無線帯域にあっても、異なるVLAN を使用するためには各VAP の設定、または同じVLAN を使用するために複数のVAP の設定を行うことができます。VAP0 は、常に両方の帯域で有効であり、デフォルトVLAN1 に割り当てられます。

アクセスポイントは、VAP画面で設定するVLAN ID に基づいて、または、RADIUS サーバの割り当てを使用することで無線クライアントトラフィックにVLAN ID タグを追加します。外部のRADIUS サーバを使用する場合、各VAP で複数のVLAN を設定することができます。外部のRADIUS サーバは、無線クライアントが接続し、認証を行う場合にその無線クライアントをVLAN に割り当てます。

最大4 つのグローバルなIPv4 またはIPv6 RADIUS サーバを設定することができます。サーバの1 つはプライマリとして常に機能し、一方他のサーバはバックアップサーバとして機能します。ネットワークタイプ (IPv4 またはIPv6) とアカウンティングモードは、設定済みのすべてのRADIUS サーバを通過するのが一般的です。各VAP を設定してグローバルなRADIUS サーバの設定を使用することができます。また、VAP ごとに異なるRADIUS サーバ設定を行うことも可能です。例えば、あるVAP を設定して、IPv6 RADIUS サーバを使用します。一方、別のVAP ではグローバルなIPv4 RADIUS サーバ設定を使用します。無線クライアントがRADIUS サーバと通信しないセキュリティモードを使用している場合、またはRADIUS サーバがVLAN 情報を提供しない場合、各VAP にVLAN ID を割り当てることができます。アクセスポイントはそのVAP を通じてアクセスポイントに接続するすべての無線クライアントにVLAN を割り当てます。

重要

- アクセスポイントにVLAN を設定する前に、アクセスポイントが使用するスイッチとDHCP サーバが、IEEE 802.1Q VLAN のカプセル化をサポートしていることを必ず確認してください。



◆ **RADIUS IP Address Type**	RADIUS サーバが使用するIP バージョン(IPv4 またはIPv6)を指定します。 アドレスタイプを切り替えてIPv4 とIPv6 のグローバルなRADIUS アドレスの設定を行いますが、アクセスポイントはこの欄で選択するアドレスタイプのRADIUS サーバまたはサーバだけとコンタクトをとります。
◆ **RADIUS IP Address** ◆ **RADIUS IPv6 Address**	プライマリグローバルRADIUS サーバのIPv4 またはIPv6 アドレスを入力します。 初期値では、各VAP は「VAP」画面の上部でアクセスポイントに定義するグローバルなRADIUS 設定を使用します。 [Radius IP Address Type]オプションで[IPv4]を選択した場合、すべてのVAP が初期値で使用するRADIUS サーバのIPアドレス(例192.168.10.23)を入力します。 [Radius IP Address Type]オプションで[IPv6]を選択した場合、プライマリのグローバルRADIUS サーバのIPv6 アドレス(例2001:0db8:1234::abcd)を入力します。
◆ **RADIUS IP Address 1-3** ◆ **RADIUS IPv6 Address 1-3**	バックアップRADIUS サーバとして使用する最大3 個のIPv4 またはIPv6 アドレスを入力します。 [Radius IP Address Type]オプションで[IPv4]を選択した場合、項目のラベル名は[IP Radius IP Address]となります。 [Radius IP Address Type]オプションで[IPv6]を選択した場合、項目のラベル名は[IPv6 Radius IP Address]となります。
◆ **RADIUS Key**	RADIUS キーを入力します。 RADIUS キーは、グローバルRADIUS サーバ用の共有秘密鍵です。63 文字以内の半角英数字および特殊文字を使用できます。キーは大文字と小文字を区別しており、アクセスポイントとRADIUS サーバに同じキーを設定する必要があります。入力した文字は"*" で表示されます。
◆ **RADIUS Key1-3**	設定済みのバックアップRADIUS サーバに関連付けるRADIUS キーを入力します。 RADIUS IP Address-1 のキーはRADIUS Key-1、RADIUS IP Address-2 のキーはRADIUS Key-2 というように使用します。
◆ **Enable RADIUS accounting**	RADIUS アカウンティングを有効にします。 有効にすると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。また、プライマリRADIUSサーバとすべてのバックアップサーバが有効になります。
◆ **Radio**	設定する無線帯域を選択します。VAP は各無線帯域で個別に設定されます。
◆ **VAP**	各無線インタフェースに16 個までのVAP を設定できます。VAP0 が物理的な無線インタフェースであるため、VAP0 を無効にするためには、無線インタフェースを無効にする必要があります。
◆ **Enabled**	設定したネットワークを[Enabled](有効)または[Disabled](無効)にします。特定のネットワークを無効にすると、 入力したVLAN ID は失われます。
◆ **VLAN ID**	VLAN IDを入力します。 無線クライアントがこのVAP を使用してアクセスポイントに接続する場合、タグなしVLAN ID の入力、またはRADIUSサーバを使用した無線クライアントのVLAN への割り当てを行わなければ、アクセスポイントは無線クライアントのトラフィックすべてに、ここで入力したVLAN ID をタグ付けします。(設定可能範囲:1-4094) クライアントにRADIUS ベースの認証を使用すると、クライアントにVLAN を設定するために以下の属性をオプションでRADIUS またはAAA サーバ内の適切なファイルに追加することができます。 ・Tunnel-Type ・Tunnel-Medium-Type ・Tunnel-Private-Group-ID RADIUS が割り当てたVLAN ID は、「VAP」画面で設定するVLAN ID を上書きします。 Ethernet Settings画面でタグなし、管理VLAN ID を設定します。詳しくは、『Ethernet Settings(イーサネット設定):p.45 』を参照してください。
◆ **SSID**	SSID(無線ネットワークの名称)を入力します。 ・入力可能文字数:32 文字以内の半角英数字 複数のVAP に同じSSID を使用することができます。または、各VAP に固有のSSID を選択することもできます。 無線クライアントとして、管理しているアクセスポイントと同じアクセスポイントに接続する場合、SSID をリセットするとアクセスポイントへ接続性を失います。この新しい設定を保存した後に新しいSSID に再接続する必要があります。
◆ **Broadcast SSID**	アクセスポイントがビーコンフレーム内のSSID をブロードキャストするかどうかを指定します。 初期値ではBroadcast SSID は有効です。VAP がSSID をブロードキャストしないと、クライアントステーション上の「使用可能ネットワークリスト」にネットワーク名が表示されなくなります。その代わりに、クライアントは接続前に、サプリカントに接続する相手の正しいネットワーク名を登録する必要があります。
◆ **Band Steer**	バンドステアリング(5GHz有線)機能を有効または無効にします。
◆ **Security**	このVAP に対して以下のセキュリティモードから一つ選択します。 [None]以外のセキュリティモードを選択すると、新しい欄が表示されます。(『Security 設定について:p.56 』参照) ・[None] ・[WPA Personal] ・[WPA Enterprise]

◆ **MAC Auth Type**	ネットワークへのアクセスを許可または拒否するMAC アドレスのグローバルなリストを設定することができます。プルダウンメニューで、使用するMAC 認証のタイプを選択します。 MAC認証については、『MAC Authentication（MAC 認証によるアクセス制御）：p.61 』を参照してください。 • [Disabled]: MAC 認証をしません。 • [Local]: MAC Authentication画面で設定したMAC 認証リストを使用します。 • [Radius]: 外部RADIUS サーバのMAC 認証リストを使用します。
◆ **Update**	設定を適用します。

重要

• 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

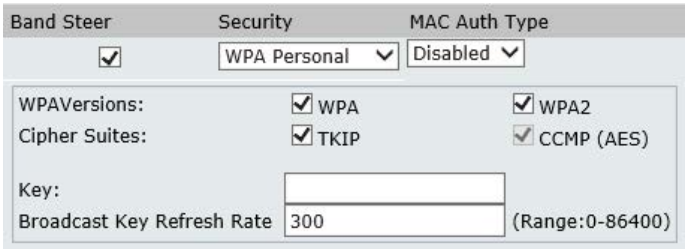
■Security 設定について

● NONE

[Security]で[None]を選択すると、そのアクセスポイントに対してそれ以上の設定は不必要です。
本モードでは、アクセスポイントへの（からの）データ転送には暗号化が行われません。本セキュリティモードは初期のネットワーク設定時、または問題解決時の使用に便利です。しかし、本モードの選択は、安全性が極めて低いため、内部用ネットワークでの通常使用にはお勧めできません。

● WPA Personal

WPA Personal はWi-Fi Alliance により発表されたIEEE 802.11i の規格で、AES-CCMP およびTKIP というメカニズムを採用しています。WPA PersonalはWPA Enterprise で使用する「IEEE 802.1X」や「EAP」の代わりに、「pre-shared key」(事前共有鍵) を使用します。PSK は証明書の初期チェックだけに使用されます。
このセキュリティモードは、オリジナルのWPA をサポートする無線クライアントと下位互換性を持っています。
以下の画面で設定を行います。

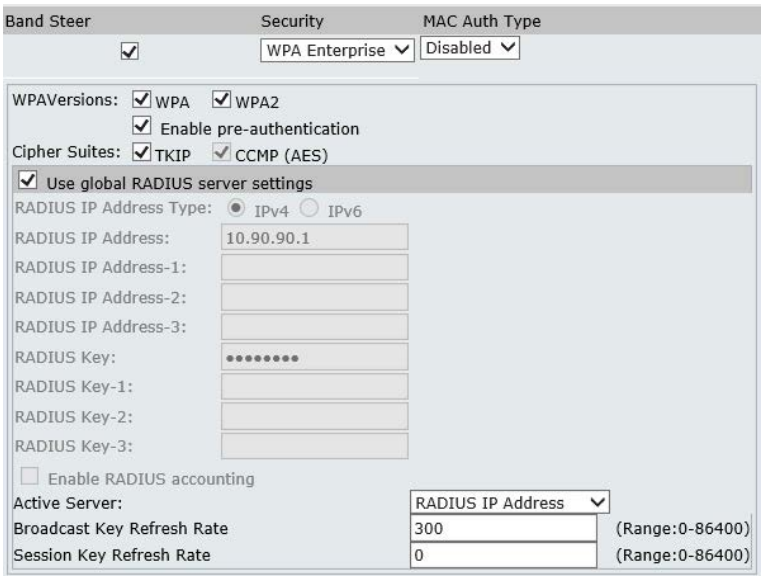


◆ **WPA Versions**	サポートするクライアントステーションのWPA のタイプを選択します。 • [WPA]:ネットワーク上のすべてのクライアントがWPA をサポートし、WPA2 をサポートしていない場合は、WPA を選択します。 • [WPA2]:ネットワーク上のすべてのクライアントがWPA2 をサポートしている場合は、IEEE 802.11i 規格で最も安全なセキュリティを提供するWPA2 を使用することをお勧めします。 • [WPA] と[WPA2]:WPA とWPA2 をサポートするクライアントが混在している場合は、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。本設定では相互運用性を実現する代わりに、セキュリティを若干低くしています。
◆ **Cipher Suites**	使用する暗号化方式を以下から選択します。 • [TKIP] • [CCMP(AES)] • [TKIP]と[CCMP(AES)] TKIP とAES サポートのクライアントのどちらも、アクセスポイントへの接続が可能です。アクセスポイントとの接続のために、WPA クライアントは以下のどちらかを持っている必要があります。 • 有効なTKIP キー • 有効な AES-CCMP キー WPA パーソナルを使用するように設定されていないクライアントは、アクセスポイントに接続することはできません。
◆ **Key**	Pre-shared Key を入力します。 Pre-shared Key は、WPA パーソナルで使用する共有秘密鍵です。8 から63 の半角英数字を入力します。アルファベットの大文字、小文字、数字、および@# などの記号が入力できます。
◆ **Broadcast Key Refresh Rate**	このVAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔時間を入力します。0 に設定した場合、ブロードキャストキーは更新されません。 • 設定可能範囲:0-86400（秒）

● WPA Enterprise

WPA EnterpriseはWi-Fi AllianceのIEEE 802.11i標準に準拠した規格で、CCMP（AES）およびTKIPというメカニズムを採用しています。Enterprise モードでは、ユーザを認証するためにRADIUS サーバの使用を必要とします。
このセキュリティモードはオリジナルのWPA をサポートする無線クライアントと下位互換性があります。

以下の画面で設定を行います。



◆ **WPA Versions**	サポートするクライアントステーションのWPA のタイプを選択します。 • [WPA]:ネットワーク上のすべてのクライアントがWPA をサポートし、WPA2 をサポートしていない場合は、WPA を選択します。 • [WPA2]:ネットワーク上のすべてのクライアントがWPA2 をサポートしている場合は、IEEE 802.11i 規格で最も安全なセキュリティを提供するWPA2 を使用することをお勧めします。 • [WPA] と[WPA2]:WPA とWPA2 をサポートするクライアントが混在している場合は、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。本設定では相互運用性を実現する代わりに、セキュリティを若干低くしています。
◆ **Enable pre-authentication**	WPA バージョンにWPA2、またはWPA2 とWPA の両方を選択すると、WPA2 クライアントに対して事前認証を有効にすることができます。 WAP2 対応の無線クライアントから事前認証パケットを送信する場合は「Pre-Authentication」チェックボックスにチェックを入れます。事前認証情報はクライアントが接続中のアクセスポイントから、送信先のアクセスポイントに受け渡されます。 本機能を有効にすると、複数のアクセスポイントと接続するローミングクライアントの認証を高速化することができます。 従来のWPA は本機能をサポートしていないため、「WPA Versions」にWPA を選択すると、本オプションは適用されません。
◆ **Cipher Suites**	使用する暗号化方式を以下から選択します。 • [TKIP] • [CCMP(AES)] • [TKIP]と[CCMP(AES)] TKIP とAES サポートのクライアントのどちらも、アクセスポイントへの接続が可能です。アクセスポイントとの接続のために、WPA クライアントは以下のどちらかを持っている必要があります。 • 有効なTKIP キー • 有効な AES-CCMP キー WPA パーソナルを使用するように設定されていないクライアントは、アクセスポイントに接続することはできません。
◆ **Use global radius server settings**	チェックをいれるとグローバルRADIUSサーバ設定が有効になります。 グローバルRADIUSサーバ設定が有効である場合、各VAPは「VAP」画面の上部でアクセスポイントに定義するグローバルなRADIUS 設定を使用します。各VAP に個別のRADIUS サーバを使用するためには、チェックボックスのチェックを外し、本欄にRADIUS サーバのIP アドレスを入力してください。
◆ **RADIUS IP Address Type**	RADIUS サーバが使用するIP バージョン（IPv4 またはIPv6）を指定します。 アドレスタイプを切り替えてIPv4 とIPv6 のグローバルなRADIUS アドレスの設定を行いますが、アクセスポイントはこの欄で選択するアドレスタイプのRADIUS サーバまたはサーバだけとコンタクトをとります。

◆ **RADIUS IP Address** ◆ **RADIUS IPv6 Address**	プライマリグローバルRADIUS サーバのIPv4 またはIPv6 アドレスを入力します。 初期値では、各VAP は「VAP」画面の上部でアクセスポイントに定義するグローバルなRADIUS 設定を使用します。 [Radius IP Address Type]オプションで[IPv4]を選択した場合、すべてのVAP が初期値で使用するRADIUS サーバのIPアドレス(例192.168.10.23)を入力します。 [Radius IP Address Type]オプションで[IPv6]を選択した場合、プライマリのグローバルRADIUS サーバのIPv6 アドレス(例2001:0db8:1234::abcd)を入力します。
◆ **RADIUS IP Address 1-3** ◆ **RADIUS IPv6 Address 1-3**	バックアップRADIUS サーバとして使用する最大3 個のIPv4 またはIPv6 アドレスを入力します。 [Radius IP Address Type]オプションで[IPv4]を選択した場合、項目のラベル名は[IP Radius IP Address]となります。 [Radius IP Address Type]オプションで[IPv6]を選択した場合、項目のラベル名は[IPv6 Radius IP Address]となります。
◆ **RADIUS Key**	RADIUS キーを入力します。 RADIUS キーは、グローバルRADIUS サーバ用の共有秘密鍵です。63 文字以内の半角英数字および特殊文字を使用できます。キーは大文字と小文字を区別しており、アクセスポイントとRADIUS サーバに同じキーを設定する必要があります。入力した文字は"*" で表示されます。
◆ **RADIUS Key1-3**	設定済みのバックアップRADIUS サーバに関連付けるRADIUS キーを入力します。 RADIUS IP Address-1 のキーはRADIUS Key-1、RADIUS IP Address-2 のキーはRADIUS Key-2 というように使用します。
◆ **Enable RADIUS accounting**	RADIUS アカウンティングを有効にします。 有効にすると、システム時間、送受信したデータ量など、特定のユーザのリソース使用状況を追跡して測定します。また、プライマリRADIUSサーバとすべてのバックアップサーバが有効になります。
◆ **Enable RADIUS FailThrough**	RADIUSフェイルスルーを有効にします。 有効にすると、プライマリRADIUS サーバの認証に失敗した場合、セカンダリRADIUS サーバが無線クライアントの認証を行います。
◆ **Active Server**	アクティブにするRADIUS サーバ(Radius IP Address、Radius IP Address-1、Radius IP Address-2、Radius IP Address-3)を選択します。
◆ **Broadcast Key Refresh Rate**	このVAP に接続するクライアントが使用するブロードキャスト(グループ)キーの更新間隔時間を入力します。0 に設定した場合、ブロードキャストキーは更新されません。 ・設定可能範囲:0-86400(秒)
◆ **Session Key Refresh Rate**	このVAP に接続する各クライアントが使用するセッション(ユニキャスト)キーの更新間隔時間を入力します。0 に設定した場合、ブロードキャストキーは更新されません。 ・設定可能範囲:0-86400(秒)

WDS（WDS の設定）

[Manage] > [WDS]

WDS（Wireless Distribution System）の設定を行います。
WDS を使用すると、アクセスポイント同士は標準化された方法でケーブルを使用せずに通信します。この機能はクライアントのローミングや複数の無線ネットワークの管理をシームレスに行うために重要です。
また、必要とされるケーブル接続の量を削減することでネットワーク構造を簡素化できます。接続するリンク数に基づいてポイントツーポイントまたはポイントツーマルチポイントのブリッジモードでアクセスポイントを設定することができます。

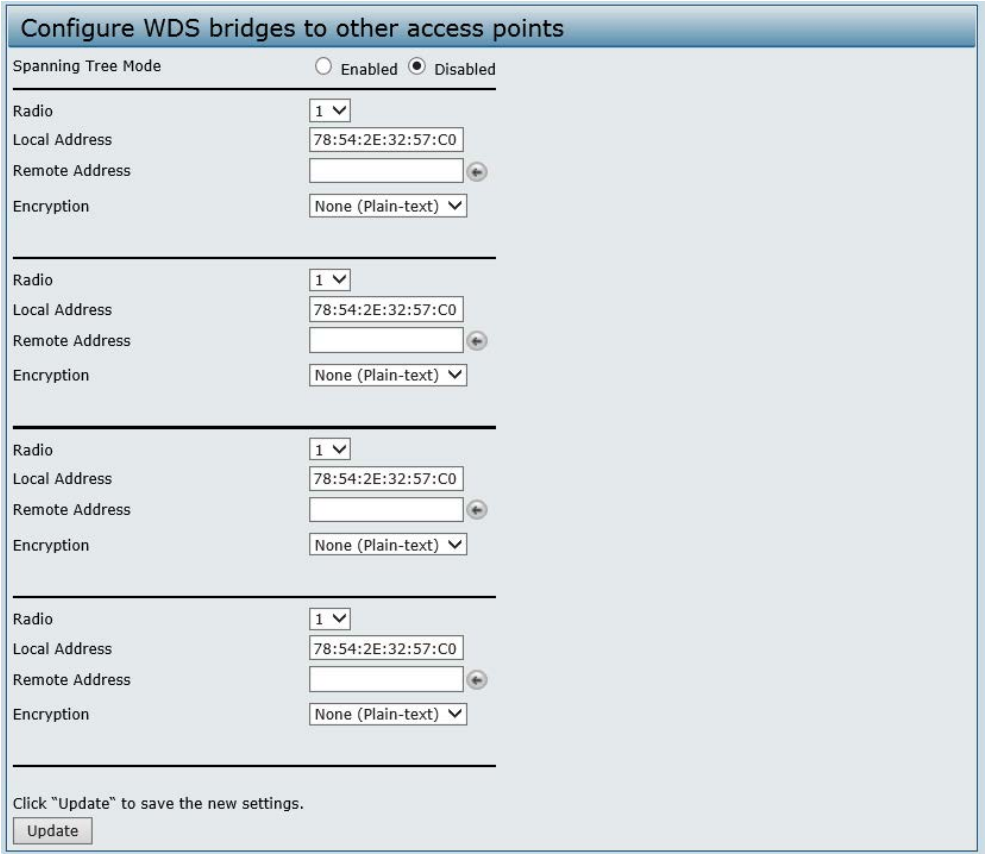
ポイントツーポイントモードでは、アクセスポイントは、クライアントの接続を許可して無線クライアントや他のリピータと通信を行います。アクセスポイントは、アクセスポイント間で確立されるトンネルを経由する他のネットワークに向けてすべてのトラフィックを転送します。ブリッジはホップ回数に加えません。これは、簡単なOSI のレイヤ2 ネットワークデバイスとして機能します。

ポイントツーマルチポイントブリッジモードでは、1 つのアクセスポイントが複数のアクセスポイント間で通常のリンクとして機能します。このモードでは、中央のアクセスポイントは、クライアントの接続を許可して無線クライアントや他のリピータと通信を行います。他のアクセスポイントのすべてが、ルーティングの目的のために適切な無線ブリッジにパケットを送信する中央のアクセスポイントとだけ接続します。

本製品はリピータとしても機能できます。本モードでは、アクセスポイントはセル範囲から極めて遠い2 つのアクセスポイント間を接続します。リピータとして機能する場合、アクセスポイントは、LAN との有線接続は行わず、無線接続を使用することで信号を中継します。アクセスポイントがリピータとして機能するために特別な設定は必要ではなく、リピータモード設定もありません。無線クライアントはリピータとして動作しているアクセスポイントに接続することができます。

重要

- アクセスポイントをスタンドアロンモードから管理モードに移行させると、WDS は無効になります。
  管理モードでは、D-Link 統合スイッチを使用することによって、アクセスポイントを設定します。アクセスポイントが管理モードにある場合、Web マネージャ、Telnet、SSH、およびSNMP アクセスは無効となります。
- 異機種間、異なるファームウェアバージョン間でWDS モードを使用することはできません。



アクセスポイントにWDS を設定する前に、以下のガイドラインに注意してください。

- アクセスポイントのペア間にWDS リンクだけを持つことができます。つまり、リモートMAC アドレスは特定のアクセスポイントのWDS 画面に一度だけ表示される可能性があります。
- WDS リンクに参加する両方のアクセスポイントが、同じ無線チャンネルにあり、同じIEEE 802.11 モードを使用する必要があります。（無線モードとチャンネルの設定に関する情報については、『Radio（無線詳細設定）：p.49 』を参照してください。）
- 無線1 を経由したWDS リンクでWPA 暗号化を使用する場合、無線1 のVAP0 はセキュリティモードとしてWPA Personal または WPA Enterpriseを使用する必要があります。無線2 を経由したWDS リンクでWPA 暗号化を使用する場合、無線2 のVAP0 はセキュリティモードとしてWPAPersonal または WPA Enterprise を使用する必要があります。

◆ **Spanning Tree Mode**	スパニングツリーを[Enabled](有効)または[Disabled](無効)にします。 スパニングツリープロトコル(STP)は、スイッチングのループを防ぎます。 WDS リンクを設定する場合は有効にすることをおすすめします。
◆ **Radio**	２つの無線帯域を持つアクセスポイントにおける各WDS リンクに対して、[1]または[2]を選択します。本項目の選択内容によって、参照される[Local Address]は変わります。
◆ **Local Address**	本アクセスポイントのMAC アドレスを示します。 ２つの無線帯域を持つアクセスポイントの各WDS リンクに対して、[Local Address]は選択された無線帯域(wlan0 ではRadio 1、またはwlan1 ではRadio 2)上の内部インタフェースのMAC アドレスを反映します。
◆ **Remote Address**	送信先アクセスポイントのMAC アドレスを指定します。 をクリックすると、ネットワークにおけるすべての利用可能なMAC アドレスとそれらに関連するSSID のリストを参照することができます。 リストで表示されるSSID は、送信先アクセスポイントの正しいMAC アドレスを特定するために役立ちます。このSSID はWDS リンクに設定するものとは別のSSID です。2 つを同じ値または名前にするべきではありません。
◆ **Encryption**	WDS リンクで使用する暗号化のタイプを以下から選択します。 • [Non (Plain - text)]: 暗号化を行いません。 • [WPA (PSK)]: WDS リンクにCCMP (AES) 準拠のWPA2-PSK 暗号化を使用します。 [WPA (PSK)]を選択した場合は、SSIDとKeyを入力します。 WDS リンクにWPA-PSK を設定するためには、選択した無線帯域のVAP0 がWPA-PSK またはWPA-Enterprise に設定される必要があります。
◆ **Update**	設定を適用します。

重要

• WDS リンクを無効にするためには、[Remote Address]欄に設定した値を削除する必要があります。

● WDS リンクにおけるWPA (PSK)

[Encryption]で[WPA(PSK)]を選択した場合、以下の設定を行います。

◆ **SSID**	作成した新しいWDS リンクに適切な名称を入力します。このSSID はこのアクセスポイントが使用する別のSSID と異なる必要があります。しかし、同じSSID がWDS リンクのもう一端にも入力されることが重要です。このSSID がWDS リンク上の両方のアクセスポイントで同じでないと、それらは通信およびデータ交換を行うことはできません。 SSID はあらゆる英数字の組合せで指定することができます。
◆ **Key**	WDS ブリッジに固有の共有キーを入力します。 また、WDS リンクのもう一端のアクセスポイントにもこの固有の共有キーを入力する必要があります。このキーが両方のアクセスポイントで同じでないと、それらは通信およびデータ交換を行うことはできません。 WPA-PSK キーは、8 文字以上63 文字以下の半角英数字の文字列です。アルファベットの大文字、小文字、数字、および@# などの記号が入力できます。

重要

• 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

MAC Authentication（MAC 認証によるアクセス制御）

[Manage] > [MAC Authentication]

本画面ではMACアドレス認証によるアクセス制御設定を行います。

Media Access Control（MAC）アドレスは、ネットワーク上の各ノードを特定するハードウェアアドレスです。通常、「:」（コロン）で区切られた12 個の16 進数（例00:DC:BA:09:87:65）として表されます。

無線クライアントのMAC アドレスに基づいてアクセスポイント経由でネットワークへのアクセスを制御するために、アクセスポイントのWeb マネージャを使用するか、または外部のRADIUS サーバを使用することができます。本機能は、MAC 認証またはMAC フィルタリングと呼ばれます。
アクセスを制御するためには、アクセスポイント上、または、外部RADIUS サーバ上にMAC アドレスのステーションリストをに設定します。これらのMAC アドレスを持つクライアントネットワークへのアクセスを許可または拒否するかどうかを指定するフィルタを設定することができます。
無線クライアントがアクセスポイントへ接続しようとすると、アクセスポイントは"ローカルなステーションリストにあるクライアント"または"RADIUS サーバ上のクライアントのMAC アドレス"を検索しまし、接続の許可または拒否を行います。

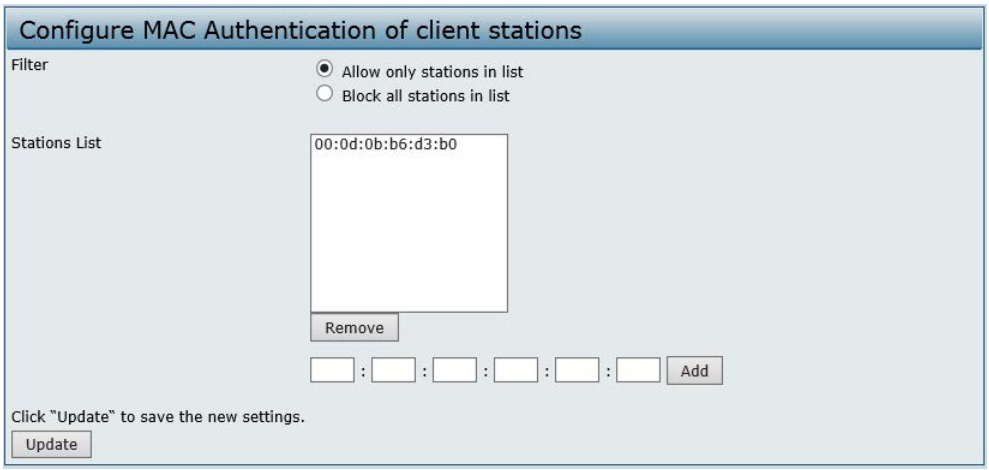
[VAP]画面の[MAC Auth Type]設定では、アクセスポイントが[MAC Authentication]画面で設定したステーションリストを使用するか、またはRADIUS サーバに設定されているステーションリストを使用するかを決定します。
MAC Authentication画面の[Allow/Block]設定は、ステーションリスト（localまたはRADIUS）内のクライアントがアクセスポイントを通じてネットワークにアクセスできるかどうかを決定します。
[VAP]画面のMAC 認証タイプの設定については『VAP（仮想アクセスポイントの設定）：p.54 』を参照してください。

■アクセスポイントにMAC フィルタとステーションを設定する

MAC アドレスに基づいたアクセスポイントへのアクセス制御を行います。フィルタの設定方法に基づいて、リストにあるMAC アドレスを持つクライアントステーションだけを許可するか、またはリストにあるステーションへのアクセスを拒否することができます。

重要

- グローバルなMAC 認証設定は両方の無線帯域にあるすべてのVAP に適用されます。



◆ **Filter**	フィルタリングの方法を以下から選択します。 • [Allow only stations in list]:ステーションリストにあるクライアントは、アクセスポイントを通じたネットワークへの接続を許可されます。 • [Block all stations in list]:ステーションリストにあるクライアントは、アクセスポイントを通じたネットワークへの接続を拒否されます。
◆ **Station List**	ステーションリストが表示されます。 VAP に対するMAC 認証タイプがRADIUS に設定されている場合、アクセスポイントは、このリストに設定されているMAC アドレスを無視して、RADIUS サーバに保存されているリストを使用します。
◆ **Remove**	ステーションリストからクライアントを削除します。
◆ **Add**	左の欄にMACアドレスを入力し、ステーションリストに追加します。
◆ **Update**	設定を適用します。

重要

- 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

■RADIUS サーバにMAC 認証を設定する

MAC ベースのアクセス制御にRADIUS MAC 認証を使用する場合、RADIUS サーバにステーションリストを設定する必要があります。ステーションリストにはクライアントのMAC アドレスエントリが含まれます。リストの形式については以下の表で説明します。

RADIUS サーバ属性	説明	値
User-Name (1)	クライアントステーションのMAC アドレス。	有効なイーサネットMACアドレス。
User-Password (2)	クライアントのMAC エントリ検索に使用する固定のグローバルパスワード。	NOPASSWORD

Load Balancing（ロードバランシングの設定）

[Manage] > [Load Balancing]

ネットワーク利用率のしきい値を設定し、クライアントがアクセスポイントに接続または接続を解除する場合に無線ネットワークの速度と性能を維持することができます。
ロードバランシング設定は両方の無線帯域に適用されます。
ロードバランシングを設定し、アクセスポイントの定義済みの稼動率によって起動されるように制限と動作を設定します。

◆ **Load Balancing**	ロードバランシングを[Enabled](有効)または[Disabled](無効)にします。
◆ **Utilization for No New Associations**	アクセスポイントが新しいクライアントの接続の受け入れを停止する前に、無線帯域で許可されるネットワーク帯域幅利用率 (%) を設定します。 0に設定した場合はロードバランシングが無効となります。
◆ **Update**	設定を適用します。

重要

・設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Managed Access Point（管理アクセスポイントの設定）

[Manage] > [Managed Access Point]

本アクセスポイントは、2 つのモード（スタンドアロンモードまたは管理モード）のいずれかで動作します。

スタンドアロンモード
本製品はネットワークで個々のアクセスポイントとして動作します。Web マネージャ、CLI、またはSNMP を使用することで管理します。

管理モード
D-Link 統合アクセスシステムの一部となり、D-Link 統合スイッチを使用して管理を行います。
アクセスポイントが本モードの場合、Web GUI、Telnet、SSH、およびSNMP サービスはアクセスポイントで使用できなくなります。

● モードの移行について

D-Link 統合スイッチは、管理するアクセスポイントのすべてに対し30 秒ごとにkeepalive メッセージを送信します。
各アクセスポイントは、SSL TCP 接続に関するkeepalive メッセージがないかどうかチェックします。アクセスポイントがkeepalive メッセージを通じてスイッチとの通信を維持する限り、管理モードが継続されます。

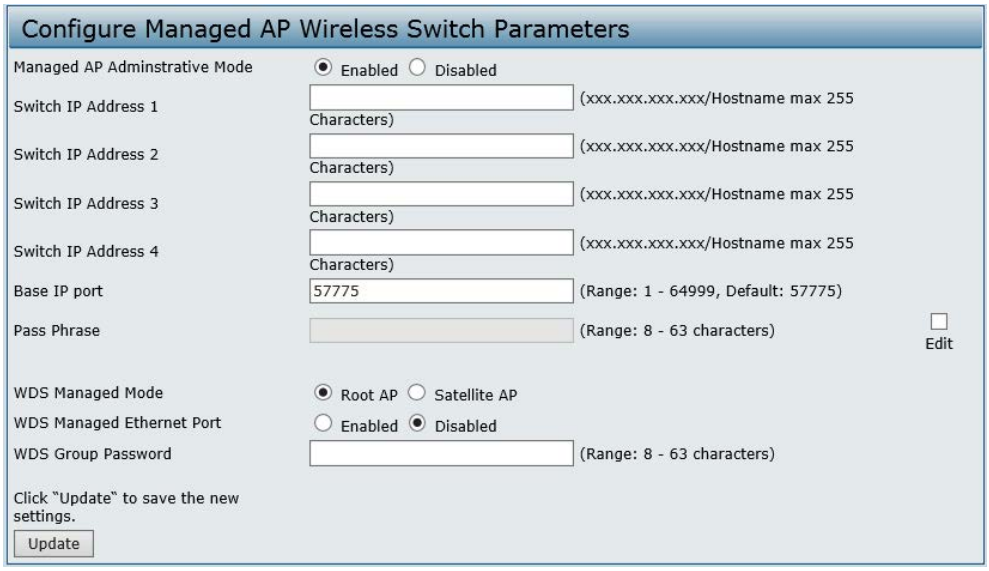
アクセスポイントが最後のkeepalive メッセージから45 秒以内にメッセージを受信しないと、アクセスポイントは、スイッチがエラーとなりスイッチへのTCP 接続を終了したものと見なして、スタンドアロンモードに入ります。

アクセスポイントは、一度スタンドアロンモードに移行すると、損失なしでトラフィックの送信を続けます。アクセスポイントは、VLAN Forwarding モード（標準のnon-tunneled モード）で設定されたVAP において設定を使用します。

アクセスポイントがスタンドアロンモードの場合、Web GUIまたはCLI（Telnet またはSSH 経由）を使用することで管理することができます。
アクセスポイントは、トンネルVAP を通じてアクセスポイントに接続するすべてのクライアントに対して、接続解除メッセージを送信し、トンネルVAP を無効にします。
[Managed AP Administrative Mode]が[Enabled]（有効）に設定されている間、アクセスポイントはディスカバリの手順を開始します。アクセスポイントが以前に接続したスイッチと同じまたは違う無線スイッチと接続を確立しても、スイッチはアクセスポイントにコンフィグレーションを送信し、アクセスポイントは無線スイッチに現在接続するすべてのクライアントに関する情報を送信します。スイッチから送信されたコンフィグレーションの適用後に、アクセスポイントの無線インタフェースは再起動します。無線インタフェースが動作状態となり、クライアントが再接続するまで、クライアントのトラフィックは中断されます。

■管理アクセスポイントの設定

D-Link 統合スイッチのIP アドレスをアクセスポイントに追加します。



◆ **Managed AP Administrative Mode**	管理アクセスポイントモードを[Enabled](有効)または[Disabled](無効)にします。 • [Enabled]: アクセスポイントとスイッチが相互にディスカバリを行うことを許可します。アクセスポイントが無線スイッチによる自身の認証に成功すると、Web Web GUIにアクセスできなくなります。 • [Disabled]:アクセスポイントは無線スイッチとコンタクトをとることができません。
◆ **Switch IP address 1-4**	アクセスポイントの管理に使用できる4 台までの無線スイッチのIP アドレスを入力します。 「.」(ドット) で区切った形式またはDNS 名でIP アドレスを入力します。 DHCP サーバを使用することで設定済みのご使用のネットワークの無線スイッチのリストを参照することができます。アクセスポイントは、最初に[Switch IP Address 1]とコンタクトを試みます。
◆ **Base IP Port**	無線システムがIP トラフィックの送受信に使用するIP ポート番号の範囲を指定します。 初期値では無線システムは「57775」から「57784」までのIP ポートを使用します。 [Base IP Port]を変更する場合、無線機能は自動的に無効となり、その後、再有効化されます。初期無線ポートはクラスタ設定関連コマンドのグローバルスイッチの一部として送信されないため、クラスタ内の全スイッチは個別に新しいIP 番号を設定される必要があります。 無線IP ポート番号が初期値から変わった場合、AP 側も変更する必要があります。
◆ **Pass Phrase**	[Edit]をクリックして、アクセスポイントが無線スイッチで認証されるためのパスフレーズを入力します。 • 入力可能文字数: 8 - 63 文字 パスワードを削除するためには[Edit]をクリックして既存のパスワードを削除し、[Update]ををクリックします。スイッチには同じパスフレーズを設定する必要があります。
◆ **WDS Managed Mode**	WDS グループ内にある時の管理モードを選択します。 • [Root AP]: ブリッジまたはリピータとして、有線リンク経由のスイッチと通信します。 • [Satellite AP]:WDS リンクのRoot APを経由してスイッチと通信をします。本モードではSatellite APによって「Root AP」とのWDS リンクを構築、または検出することを有効にします。
◆ **WDS Managed Ethernet Port**	AP がWDS グループの一部になる時、イーサネットポートが[Enabled](有効)または[Disabled](無効)になるか設定します。
◆ **WDS Group Password**	WDS リンク構築のためのWPA2 Personal認証のパスワードです。 Satellite APの場合のみ本設定が必要になりまります。 Root APは管理される時にスイッチからパスワードを入手します。
◆ **Update**	設定を適用します。

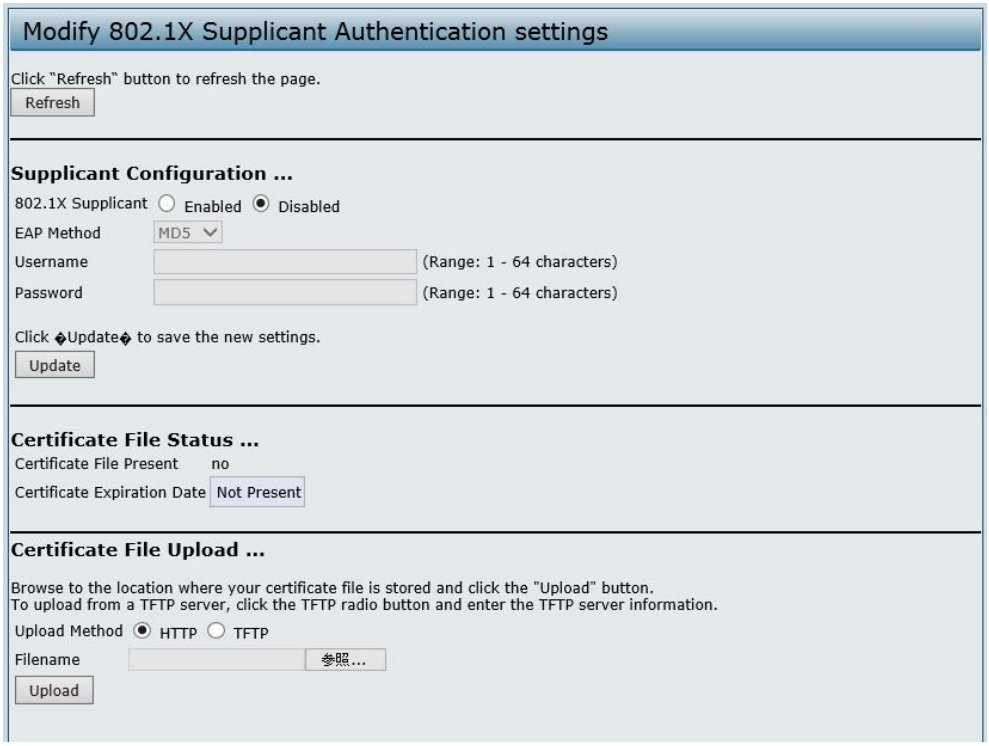
重要

• 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Authentication（802.1X 認証の設定）

[Manage] > [Authentication]

802.1X認証の設定を行います。
IEEE 802.1X のポートベースのネットワークアクセス制御を利用するネットワークでは、サプリカント（クライアント）は802.1X オーセンティケータにアクセスが許可されるまで、ネットワークへアクセスすることができません。
ットワークで802.1X 認証が使用されている場合は、アクセスポイントに802.1X 認証情報を登録する必要があります。



◆ **Refresh**	表示を更新します。
◆ **802.1X Supplicant**	802.1Xサプリカントを[Enabled](有効)または[Disabled](無効)にします。
◆ **EAP Method**	アクセスポイントと権限者が通信で使用するEAP方式を以下から選択します。 • [MD5] • [PEAP] • [TLS]
◆ **Username**	802.1X オーセンティケータからのリクエストに応じる場合にアクセスポイントが使用するMD5 ユーザ名を入力します。半角英数字64 文字以内で指定します。キータイプはASCII で、アルファベットの大文字、小文字、数字、および@# などの記号を含みます。
◆ **Password**	802.1X オーセンティケータからのリクエストに応じる場合にアクセスポイントが使用するMD5 パスワードを入力します。 半角英数字64 文字以内で指定します。キータイプはASCII で、アルファベットの大文字、小文字、数字、および@# などの記号を含みます。
◆ **Certificate File Status**	認証ファイルのステータスが表示されます。
◆ **Certificate File Upload**	認証ファイルをアップロードする方法を選択します。 • [HTTP]: HTTP経由で認証ファイルをアップロードします。[Browse]をクリックしてファイルを選択します。 • [TFTP]: TFTP経由で認証ファイルをアップロードします。[Filename]にファイル名、[Server IP]にTFTP サーバのIPアドレスを入力します。
◆ **Upload**	認証ファイルをアップロードします。

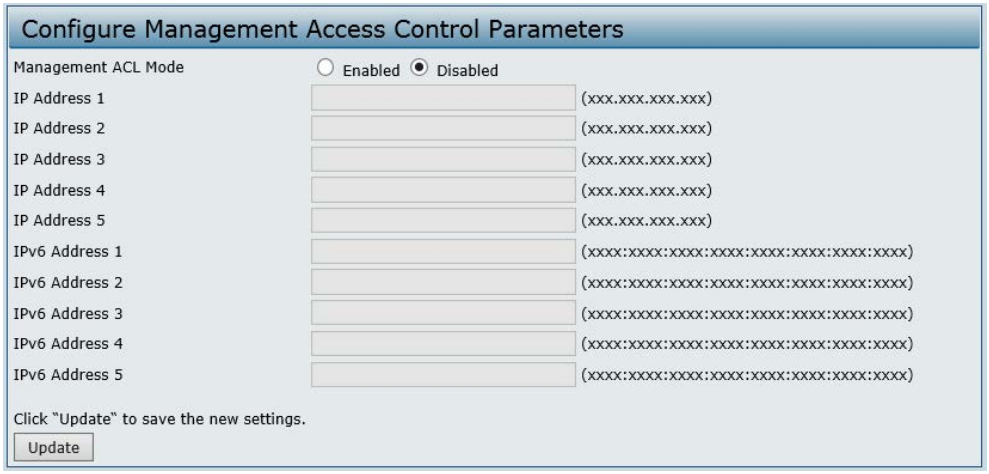
重要

• 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

Management ACL（管理アクセスコントロールリストの作成）

[Manage] > [Management ACL]

アクセスコントロールリスト（ACL）を作成します。
アクセスコントロールリストを有効にすると、リストに記載されたIPアドレス／IPv6アドレスを持つネットワーククライアントのみがWeb GUIにアクセスできるようになります。
本機能を無効にすると、正しいアクセスポイントのユーザ名とパスワードを入力することで、どのネットワーククライアントからもWeb GUIにアクセスできます。



◆ **Management ACL Mode**	管理アクセスコントロールリストを[Enabled](有効)または[Disabled](無効)にします。
◆ **IP Address 1-5**	管理アクセスコントロールリストを有効にした場合、Web GUIへのアクセスを許可するIPアドレスを入力します。IPアドレスは最大5つ設定できます。
◆ **IPv6 Address 1-5**	管理アクセスコントロールリストを有効にした場合、Web GUIへのアクセスを許可するIPv6アドレスを入力します。IPv6アドレスは最大5つ設定できます。
◆ **Update**	設定を適用します。

Service

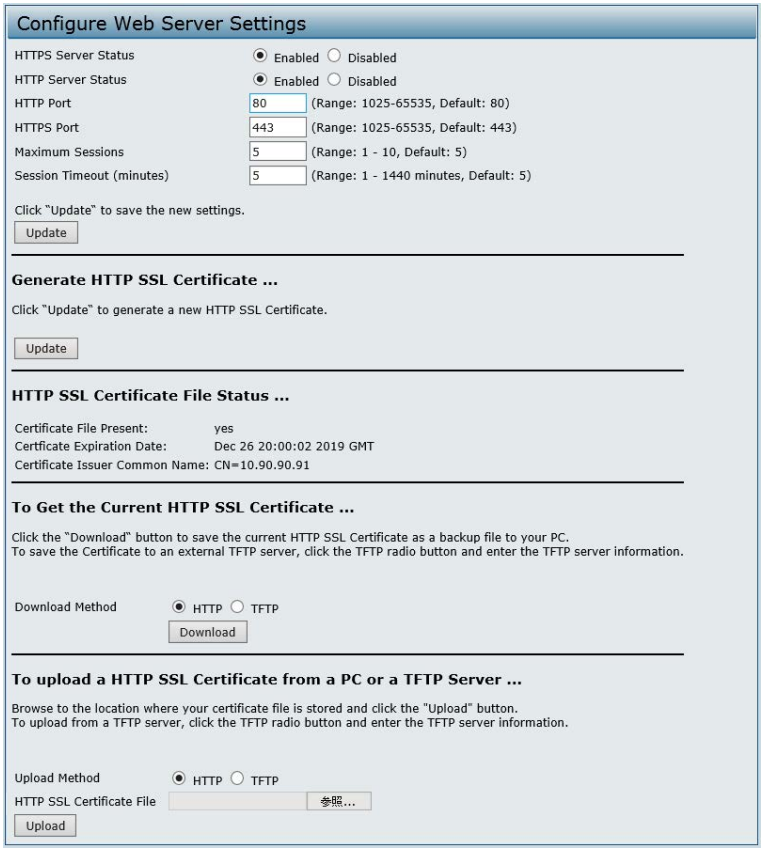
5

Webサーバ設定やSNMP設定など、本製品のサービス設定について説明します。

Web Server（Web サーバの設定）

[Service] > [Web Server]

アクセスポイントの管理を行うWebサーバ（HTTP またはHTTP）の設定を行います。



◆ **HTTPS Server Status**	HTTPS経由の通信を[Enabled](有効)または[Disabled](無効)にします。
◆ **HTTP Server Status**	HTTP経由の通信を[Enabled](有効)または[Disabled](無効)にします。
◆ **HTTP Port**	HTTPポートを指定します。(初期値：80)
◆ **HTTPS Port**	HTTPSポートを指定します。(初期値：443)
◆ **Maximum Sessions**	ユーザがWeb GUIにログオンする際の最大セッション数を設定します。 最大セッション数で設定した数のユーザが同時にWeb GUIにログオンできます。 ユーザ数が最大セッション数に達した場合、次にログオンしようとするユーザにはエラーメッセージが表示されます。 ・設定可能範囲: 1-10
◆ **Session Timeout (minutes)**	Web GUI上で操作を行わずにログオン状態を継続できる時間を設定します。 ・設定可能範囲: 1-1440 (単位:分)
◆ **Generate HTTP SSL Certificate**	[Update]をクリックし、HTTP SSL証明書を生成します。
◆ **HTTP SSL Certificate File Status**	HTTP SSL証明書のステータスが表示されます。
◆ **To Get the Current HTTP SSL Certificate**	現在のHTTP SSL証明書をダウンロードします。ダウンロード方法は以下から選択します。 ・[HTTP]を選択した場合：[Download]をクリックします。 ・[TFTP]を選択した場合:[HTTP SSL Certificate File]に証明書のファイル名、[Server IP]にTFTPサーバのIPアドレスを入力→[Download]をクリックします。
◆ **To upload a HTTP SSL Certificate from a PC or a TFTP Server**	HTTPまたはTFTP経由でSSL証明書をアップロードします。 ・[HTTP]を選択した場合：[参照]をクリックして証明書を選択→[Upload]をクリックします。 ・[TFTP]を選択した場合:[HTTP SSL Certificate File]に証明書のファイル名、[Server IP]にTFTPサーバのIPアドレスを入力→[Upload]をクリックします。
◆ **Update**	設定を適用します。

重要

・アクセスポイントの管理インタフェースにアクセスするために現在使用しているプロトコルを無効にすると、現在の接続は終了し、有効にするまで、そのプロトコルを使用したアクセスポイントへのアクセスはできなくなります。

SSH（SSHの設定）

[Service] > [SSH]

Secure Shell (SSH) は、リモートホストから本製品のCLI へのアクセスを提供するプログラムです。
SSH は、保証されていないチャンネル上に強健な認証とセキュアな通信を供給するため、リモートアクセスにおいては Telnet より安全性が高くなっています。
システムへのSSH アクセスを有効、または無効にすることができます。

◆ **SSH Status**	SSH経由の通信を[Enabled](有効)または[Disabled](無効)にします。
◆ **Update**	設定を適用します。

Telnet（Telnetの設定）

[Service] > [Telnet]

Telnet は、リモートホストから本製品のCLI へのアクセスを提供するプログラムです。
ここでは、システムへのTelnet アクセスを有効、または無効にします。

◆ **Telnet Status**	Telnet経由の通信を[Enabled](有効)または[Disabled](無効)にします。
◆ **Update**	設定を適用します。

QoS（QoSの設定）

[Service] > [QoS]

QoS (Quality of Service) 機能は、複数のキューにパラメータを指定することで、本製品を通過する従来のIP データをはじめVoIP (Voice over IP) や音声、映像、ストリーミングメディアなどの多くの無線トラフィックのスループットとパフォーマンスの向上を可能にします。

本製品に設定するQoS は、さまざまな種類の無線トラフィック用のキューにパラメータから構成され、伝送時の最大/ 最小待ち時間を（コンテンション画面により）効果的に指定することができます。ここで説明された設定は、データ伝送動作をアクセスポイントにだけ適用し、クライアントステーションには適用されません。

● EDCAについて

EDCA (Enhanced Distributed Channel Access) は、パケットを4つのアクセスカテゴリ (AC) に分類して各送信キューに格納し、それぞれの優先度に応じてパケットを送信する機能です。
4つのACは以下の通りです。優先順位は1→4で、優先度の高いトラフィックから送信キューから送信されていきます。

優先度	AC	Traffice Type
1	AC_VO	Voice
2	AC_VI	Video
3	AC_BE	Best Effort
4	AC_BK	Back Ground

AP EDCA parametersはアクセスポイントからクライアント向きのトラフィックフローに影響し、逆にStation EDCA parametersは、クライアントからアクセスポイント向きのトラフィックフローに影響します。

アクセスポイントとStation EDCA Parametersの初期値は、WMM仕様におけるWi-Fi アライアンスによって示されているものです。通常の使用では、これらの値を変更する必要はありません。これらの値を変更すると、提供されるQoS に影響します。

● EDCAパラメータについて

優先度ごとに設定するパラメータには以下の種類があります。これらの値を調整することにより優先制御を行います。

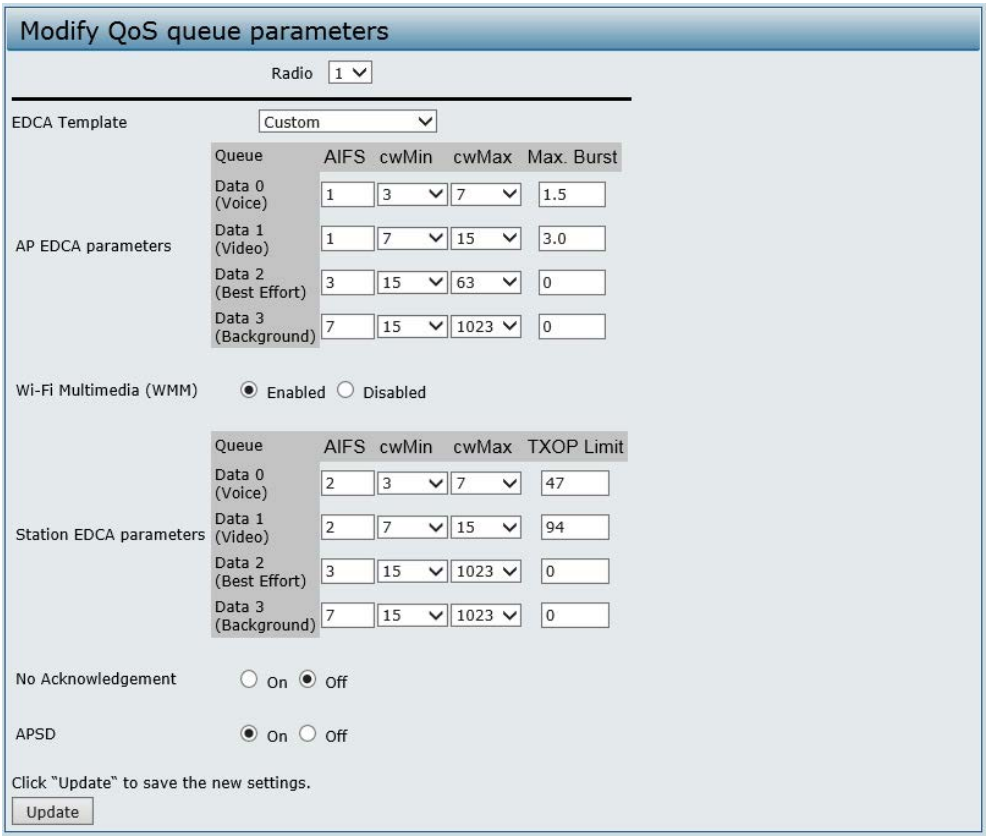
- CWmin
  CW (Contention Window) の最小値。送信待ちの時間を決めるパラメータです。
  送信待ちの時間が短い方がそのキューが送信権を得る確率が高くなるため、優先キューであればあるほど、この値を小さくする必要があります。

- CWmax
  CW (Contention Window) の最大値。送信待ちの時間を決めるパラメータです。
  送信待ちの時間が短い方がそのキューが送信権を得る確率が高くなるため、優先キューであればあるほど、この値を小さくする必要があります。

- AIFS
  AIFS (Arbitration Inter Frame Space) はフレームの送信間隔です。この値が小さいほどキューの優先度が高くなるので、優先キューであればあるほど、この値を小さくする必要があります。

- Max.Burst
  AP EDCA パラメータで、アクセスポイントからクライアントステーションへのトラフィックフローに対してのみ適用されます。本値は無線ネットワークでのパケットバーストに認められる最大バースト長です。パケットバーストとはヘッダ情報なしで送信できる複数のフレームの集まりです。オーバヘッドを少なくすることにより、高スループットと高パフォーマンスを実現できます。

- TXOP Limit
  Station EDCA パラメータで、クライアントステーションからアクセスポイントへのトラフィックフローに対してのみ適用されます。
  TXOP (Transmission Opportunity) は、チャネルの占有時間のこと。この値が大きいほど一度得た送信権でより多くのフレームを転送できるが、キューのリアルタイム性が損なわれるので調整が必要です。



◆ **Radio**	設定する無線帯域を[1]または[2]から選択します。
◆ **EDCA Template**	EDCAのテンプレートを以下から選択します。[Custom]以外を選択した場合、EDCAのパラメータは自動的に決定されます。 • [Default]:初期設定のテンプレート使用します。 • [Optimize for Voice]:音声トラフィックに最適なテンプレートを使用します。 • [Custom]:テンプレートをカスタマイズします。
◆ **AP EDCA parameters**	[EDCA Template]で[Custom]を設定した場合、以下のキューに対してアクセスポイントのEDCAのパラメータを設定します。キューの優先度はData 0が最も高く、Data 3が最も低くなります。 • [Data 0(Voice)]:優先度の高い音声トラフィックが本キューに送られます。 • [Data 1(Video)]優先度の高いビデオトラフィックが本キューに送られます。 • [Data 2(Best Effort)]:一般的なIP データは本キューに送られます。 • [Data 3(Background)]:高いスループットを要する大容量データや、遅延に敏感ではないデータ(例:FTPデータなど)が本キューに送られます。
◆ **Wi-Fi Multimedia (WMM)**	WMM(Wi-Fi Multimedia)を[Enabled](有効)または[Disabled](無効)にします。 WMM を有効にすると、QoS 優先制御や無線メディアアクセスの調整も有効になります。また、本アクセスポイントのQoS 設定は上りと下り両方のトラフィック(クライアントからアクセスポイント(Station EDCA パラメータ)、およびアクセスポイントからクライアント(AP EDCA パラメータ))に対して有効になります。 WMM を無効に設定すると、上りのトラフィック(クライアントからアクセスポイント)における Station EDCA パラメータのQoS 制御は無効になります。無効の状態でも、" アクセスポイントからクライアントへの下り方向(AP EDCA パラメータ)" のいくつかのパラメータは設定可能です。
◆ **Station EDCA parameters**	[EDCA Template]で[Custom]を設定した場合、以下のキューに対してステーションのEDCAパラメータを設定します。キューの優先度はData 0が最も高く、Data 3が最も低くなります。 • [Data 0(Voice)]:優先度の高い音声トラフィックが本キューに送られます。 • [Data 1(Video)]優先度の高いビデオトラフィックが本キューに送られます。 • [Data 2(Best Effort)]:一般的なIP データは本キューに送られます。 • [Data 3(Background)]:。高いスループットを要する大容量データや、遅延に敏感ではないデータ(例:FTPデータなど)が本キューに送られます。
◆ **No Acknowledgement**	[On]を選択すると、アクセスポイントがサービスクラス値としてQosNoAck を持つフレームを承認しません。
◆ **APSD**	[On]を選択すると、電源管理方法である自動省電力機能(APSD)が有効になります。APSDは、VoIP 電話がアクセスポイントを通じてネットワークにアクセスする場合にお勧めします。
◆ **Update**	設定を適用します。

重要

• 設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

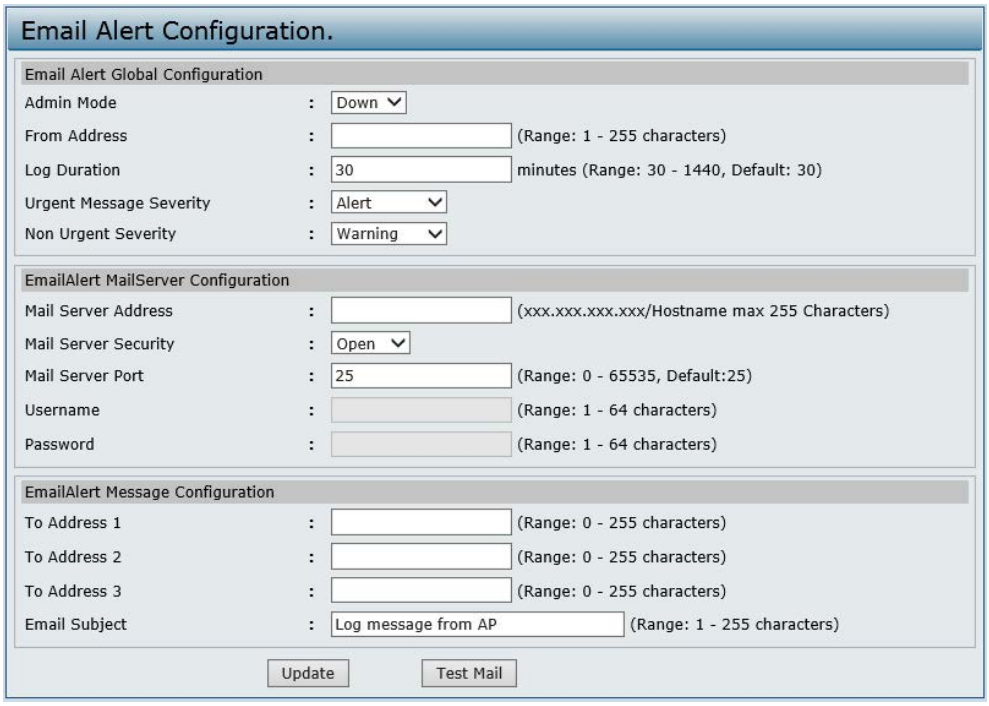
Email Alert（Eメールアラートの設定）

[Service] > [Email Alert]

Eメールアラート機能は、幾つかのレベル分けされたイベントによってアクセスポイントが自動的にE メールを送信する機能です。Eメールアラート機能の使用には、メールサーバの設定、警告発信トリガレベルの設定、3 つまでのメールアカウント設定（緊急時/ 非緊急時）などを設定する必要があります。

重要

・アクセスポイントが管理モードの場合本機能は使用できません。



Email Alert Global Configuration	
◆ **Admin Mode**	Eメールアラート機能を[Up](有効)または[Down](無効)にします。
◆ **From Address**	アクセスポイントから送信されるEメールの送信メールアドレスを設定します。 ・入力可能文字数:255 字（半角英数）
◆ **Log Duration**	緊急でないメッセージがSMTP サーバに送信される頻度を設定します。 ・設定可能範囲:30 -1440（分）
◆ **Urgent Message Severity**	メッセージの緊急度を以下から選択します。緊急度は[Energency]が最も高く、[Debug]が最も低くなります。 ・[Emergency]: システムが動作していない状態を示します。 ・[Alert]:すぐに対処するべき事項に関する警告です。 ・[Critical]: 危険な状態であることを示しています。 ・[Error]:エラーが発生してる状態であることを示します。 ・[Warning]: 警告状態であることを示します。 ・[Notice]:通常の状態ですが、通知すべき事項があります。 ・[Info]:お知らせがあります。 ・[Debug]:デバッグレベルのメッセージです。
◆ **Non Urgent Severity**	それほど緊急ではない（Non Urgent）状態を示すログメッセージのレベルを設定します。 本項目で選択されたセキュリティレベルとそれ以上のレベルは非緊急/Non Urgent として認識され、E メールで送信されることはありません このカテゴリのメッセージは、[Log Duration]で設定されたインターバル時間に従い、ダイジェストフォームで収集/ 送信されます。 セキュリティレベルについては[Urgent Message Severity]を参照してください

EmailAlert MailServer Configuration	
◆ Mail Server Address	ネットワーク上のSMTP サーバのIP アドレスまたはホスト名を指定します。
◆ Mail Server Security	メールサーバの認証を[TLSv1] または[Open](セキュリティなし) に設定します。
◆ Mail Server Port	SMTP のTCP ポート番号を設定します。 ・設定可能範囲:0-65535 ・初期値:25
◆ Username	メールサーバの認証が必要な場合のユーザ名を指定します。ユーザ名は64 バイト文字です。
◆ Password	ユーザ名に対応するパスワードを設定します。
EmailAlert Message Configuration	
◆ To Address 1	警告メールが送信される最初のアドレスを設定します。
◆ To Address 2	オプションとして警告メールが送信される2 番目のアドレスを設定します。
◆ To Address 3	オプションとして警告メールが送信される3 番目のアドレスを設定します。
◆ Email Subject	メールの件名部分を設定します。

重要

・設定を反映するには[Update]をクリックしてください。
・[Test Mail]をクリックすると、テストメールを送信できます。

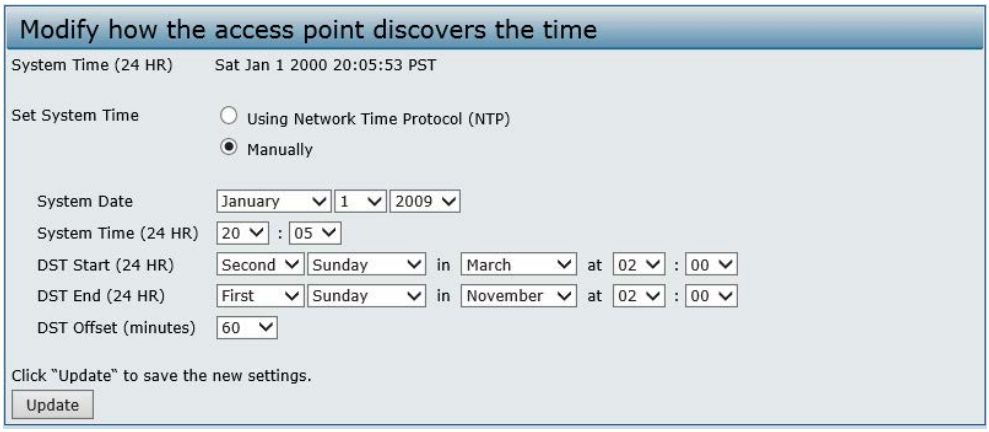
Time Settings（時間設定）

[Service] > [Time Settings]

本製品の時間設定を行います。
NTPサーバを使用するか、手動で時刻を設定するかを選択することができます。
また、サマータイムの設定を行うことも可能です。

メモ

・NTP（Network Time Protocol）は、ご使用のネットワークのコンピュータクロックタイムを同期させるインターネット標準プロトコルです。NTP サーバは協定世界時（また、グリニッジ標準時として知られている協定世界時）をそれらのクライアントシステムに送信します。NTP は定期的に時間の要求をサーバに送信し、返されたタイムスタンプを使用してクロックを調整します。タイムスタンプは、ログメッセージ内の各イベントの日時を示すのに使用されます。



◆ **System Time (24 HR)**	本製品に設定されている時刻が表示されます。
◆ **Set System Time**	時間の設定方法を以下から選択します。 ・[Using Network Time Protocol (NTP)]:NTPサーバを使用して時間設定を行います。 ・[Manually]:手動で時間設定を行います。
◆ **NTP Server IPv4/IPv6 Address/Name**	NTPサーバのホスト名またはIPv4/IPv6アドレスを設定します。 本項目は[Using Network Time Protocol (NTP)]を選択した場合にのみ表示されます。
◆ **Time Zone**	本項目は[Using Network Time Protocol (NTP)]を選択した場合にのみ表示されます。
◆ **Adjust Time for Daylight Savings**	本項目は[Using Network Time Protocol (NTP)]を選択した場合にのみ表示されます。
◆ **System Date**	本製品に設定する日付を設定します。 本項目は[Manually]を選択した場合にのみ表示されます。
◆ **System Time (24HR)**	本製品に設定する時刻を設定します。 本項目は[Manually]を選択した場合にのみ表示されます。
◆ **DST Start (24 HR)**	Daylight Savings Time（サマータイム）の開始日時を設定します。
◆ **DST End (24 HR)**	Daylight Savings Time（サマータイム）の終了日時を設定します。
◆ **DST Offset (minutes)**	Daylight Savings Time（サマータイム）のオフセット時間（単位:分）を設定します。
◆ **Update**	設定を適用します。

重要

・設定変更によってはアクセスポイントが停止し、システム処理が再起動する可能性があります。
これが発生すると、無線クライアントは一時的に接続できなくなります。WLAN のトラフィックが低い時にアクセスポイントの設定変更を行うことをお勧めします。

SNMPv3

6

SNMPv3の設定を行います。
SNMP（Simple Network Management Protocol）とは、TCP/IPネットワークにおいて、ルータやコンピュータ、端末など様々な機器をネットワーク経由で監視・制御するためのプロトコルです。
SNMPでは、機器の状態に関する情報をMIB(Management Information Base)と呼ばれるデータモデルで管理しており、マネージャとエージェントが同じMIBに基いて情報をやりとりします。

SNMPv3 Views（SNMPv3ビューの設定）

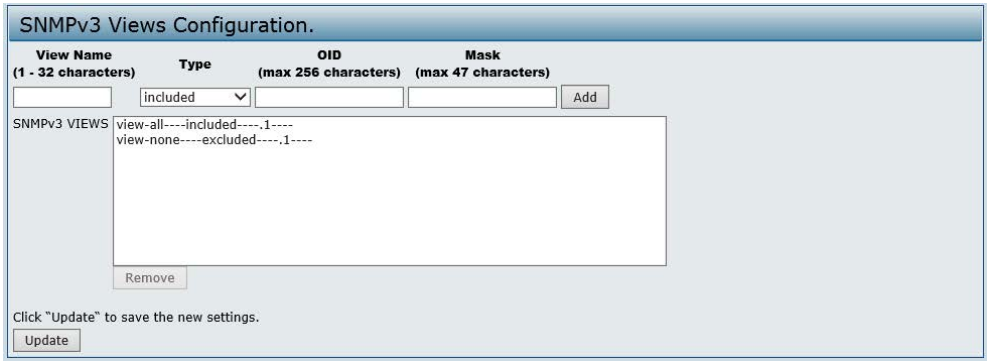
[SNMPv3] > [SNMPv3 Views]

SNMPv3のMIBビュー設定を行います。

MIBビューは、1つまたは複数のサブツリーで構成されます。サブツリーは、OID(オブジェクト識別子)、OIDに対応するマスク、およびビュータイプの組み合わせで設定します。
SNMPv3ユーザがアクセスできるOID範囲をコントロールするために、MIBビューを作成します。

重要

- [all]のMIB ビューは、システムに初期値で作成されています。このビューはシステムによってサポートされるすべての管理オブジェクトを含んでいます。
- Excluded ビューサブツリーを作成する場合、Excluded サブツリーの外側のサブツリーを含めることを許可するために、同じビュー名を持つ対応するIncluded エントリを作成します。
  例) サブツリー1.3.6.1.4 を除くビューを作成する場合：
  OID 1.3.6.1.4 を持つExcluded エントリを作成します。その後、同じビュー名を持つOID.1 のIncluded エントリを作成します。



◆ **View Name**	MIB ビューの名称を入力します。
◆ **Type**	MIBビューのタイプを設定します。 • [included]:MIB ビューにビューサブツリーまたはサブツリーのファミリーを含めます。 • [excluded]:MIB ビューからビューサブツリーまたはサブツリーのファミリーを除外します。
◆ **OID**	OID(オブジェクト識別子)を入力します。 例：システムサブツリーは、OID 文字列1.3.6.1.2.1.1 で指定されます。
◆ **Mask**	OID マスクを設定します。 OID マスクの長さは47 文字です。OID マスクのフォーマットは、「xx.xx.xx...」であり、長さは16 オクテットです。各オクテットは「.」(ピリオド)または「:」(コロン)のどちらかによって区切られた2 桁の16 進数です。 例：OID マスク「FA.80」は「11111010.10000000」です。
◆ **Add**	MIBビューを追加します。
◆ **SNMPv3 VIEWS**	MIBビューが表示されます。
◆ **Remove**	MIBビューを削除します。
◆ **Update**	設定を適用します。

SNMPv3 Groups（SNMPv3グループの設定）

[SNMPv3] > [SNMPv3 Groups]

SNMPv3グループの設定を行います。

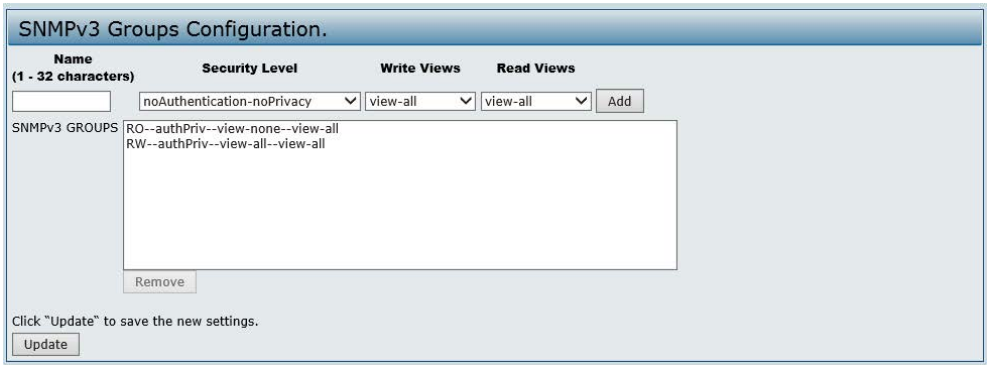
SNMPv3 グループにより、異なる許可とアクセス権のグループにユーザをまとめることができます。
初期値では以下のグループがあります。

- RO
  認証とデータの暗号化のない読み取り専用グループ。本グループには何のセキュリティも提供されません。初期値では、本グループのユーザは、ユーザが編集できるすべてのMIB ビューの初期値を参照することができます。
- RW)
  認証とデータ暗号化を使用するread/write（読み書き）グループ。本グループにおけるユーザは、認証にはMD5 キー/ パスワード、および暗号化にはDES キー/ パスワードを使用します。MD5 とDES キー/ パスワードの両方を定義する必要があります。初期値では、本グループのユーザは、ユーザが編集できるすべてのMIB ビューの初期値を読み書きすることができます。

メモ

- 最大8個のグループを設定することができます。

本画面では追加グループを定義することができます。

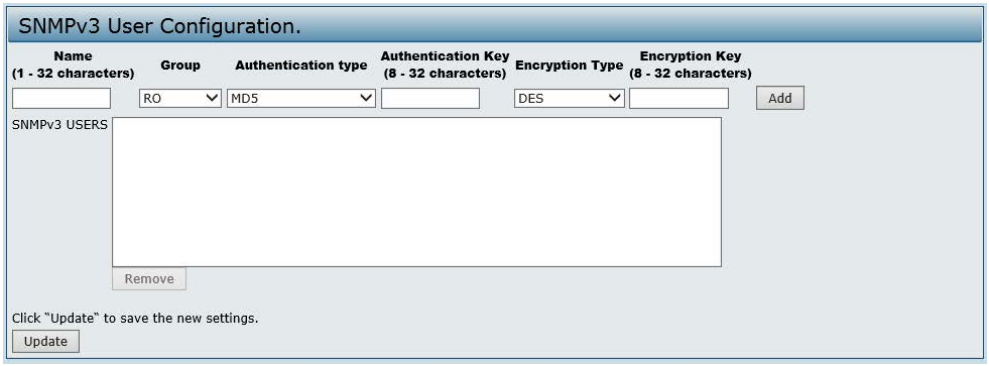


◆ **Name (1 - 32 characters)**	グループの名称を入力します。 • 入力可能文字数:半角英数字32文字以内
◆ **Security Level**	セキュリティレベルを以下から選択します。 • [noAuthentication-noPrivacy]: 認証とデータ暗号化の両方がありません。(セキュリティなし) • [Authentication-noPrivacy]: 認証を行いますが、データ暗号化は行いません。 ユーザは、認証にはMD5 キー/パスワードを使用するメッセージをSNMP に送信しますが、暗号化のためのDES キー/パスワードは送信しません。 • [Authentication-Privacy] : 認証とデータ暗号化を行います。 ユーザは、認証にはMD5 キー/パスワード、暗号化にはDES キー/パスワードを送信します。
◆ **Write Views**	グループに管理オブジェクト (MIBs) に対するアクセス (書き込み) を選択します。 • [view-all]: グループは、MIBを作成、変更、および削除できます。 • [view-none]: グループは、MIBを作成、変更、または削除できません。
◆ **Read Views**	グループに管理オブジェクト (MIBs) に対するアクセス (読み出し) を選択します。 • [view-all]: グループは、MIBの参照および読み出しができます。 • [view-none]: グループは、MIBの参照も読み出しもできません。
◆ **Add**	グループを追加します。
◆ **SNMPv3 VIEWS**	グループが表示されます。
◆ **Remove**	グループを削除します。
◆ **Update**	設定を適用します。

SNMPv3 Users（SNMPv3ユーザの設定）

[SNMPv3] > [SNMPv3 Users]

SNMPv3ユーザの設定を行います。
複数のユーザを定義し、各ユーザに希望するセキュリティレベルの割り当て、セキュリティキーの設定を行うことができます。認証にはMD5 タイプ、暗号化にはDES タイプだけがサポートされています。



◆ **Name**	SNMPv3ユーザの名称を入力します。 ・入力可能文字数:半角英数字32文字以内
◆ **Group**	ユーザをグループにマップします。初期グループは[RO]および[RW] です。 [SNMPv3 Groups]画面で追加グループを定義することができます。
◆ **Authentication Type**	ユーザからのSNMP リクエストに使用する認証タイプを選択します。 ・[MD5]: ユーザからのSNMPv3 リクエストにMD5 認証を必要とします。 ・[None]: ユーザからのSNMPv3 リクエストに対し認証を必要としません。
◆ **Authentication Key**	認証タイプとしてMD5 を指定した場合、パスワードを入力します。 ・入力可能文字数:8-32文字
◆ **Encryption Type**	ユーザからのSNMP リクエストに使用する暗号化のタイプを選択します。 ・[DES]: ユーザからのSNMPv3 リクエストにDES 暗号化を使用します。 ・[None]: ーザからのSNMPv3 リクエストに対し認証を必要としません。
◆ **Encryption Key**	暗号化タイプとしてDES を指定した場合、SNMP 要求を暗号化するためのキーを入力します。 ・入力可能文字数:8-32文字
◆ **SNMPv3 USERS**	アクセスポイントに定義したSNMPv3ユーザが表示されます。
◆ **Update**	設定を適用します。

SNMPv3 Targets（SNMPv3ターゲットの設定）

[SNMPv3] > [SNMPv3 Targets]

SNMPv3ターゲットの設定を行います。
SNMPv3ターゲットは、SNMP マネージャにトラップメッセージを送信します。
各ターゲットはターゲット名で識別され、ターゲットIP アドレス、UDP ポート、およびSNMP ユーザ名に関連付けられます。

◆ **IPv4/IPv6 Address**	リモートのSNMP マネージャのIP アドレスを入力し、トラップメッセージを受信するターゲットホストを指定します。
◆ **Port**	SNMPv3ターゲットを送信するために使用するUDP ポートを入力します。
◆ **Users**	ターゲットに割り当てるSNMPv3ユーザ名を入力します。 SNMPv3ユーザの設定方法については、を参照してください。 ・[MD5]: ユーザからのSNMPv3 リクエストにMD5 認証を必要とします。 ・[None]: ユーザからのSNMPv3 リクエストに対し認証を必要としません。
◆ **SNMPv3 TARGETS**	SNMPv3ターゲットが表示されます。
◆ **Update**	設定を適用します。

Maintenance

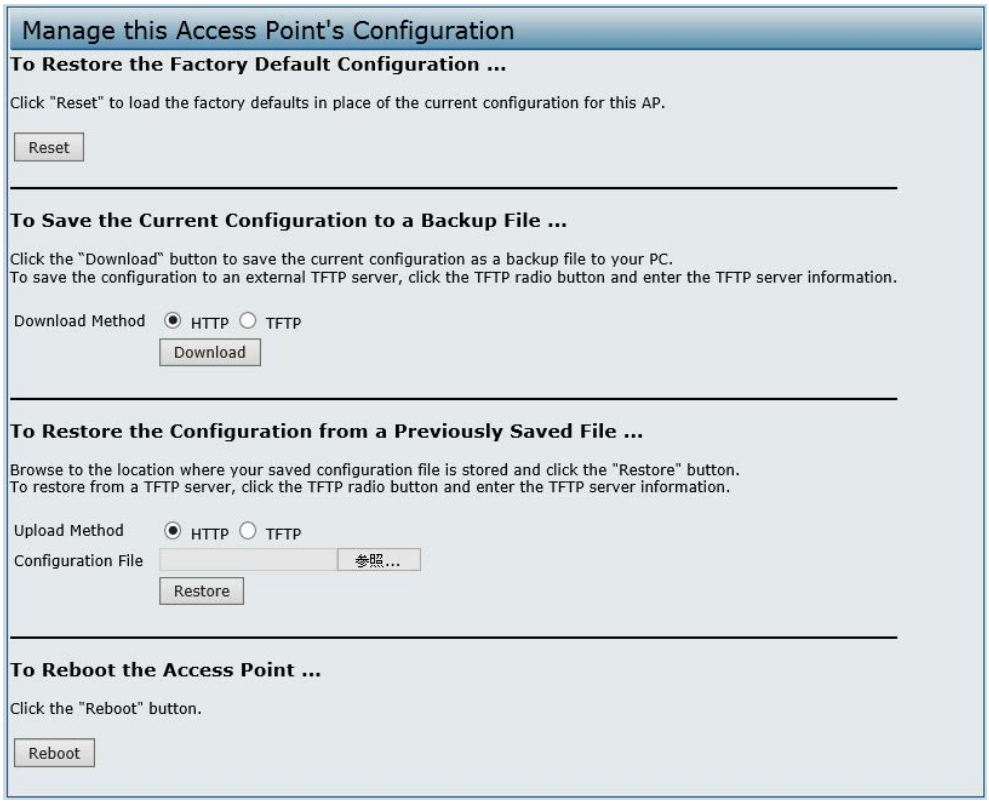
7

コンフィグレーションの保存/リストア、ファームウェアアップグレードなど本製品のメンテナンスを行います。また、本製品のサポート情報をダウンロードして閲覧することも可能です。

Configuration（コンフィグレーションの保存・リストア）

[Maintenance] > [Configuration]

コンフィグレーションファイルの保存、リストアを行います。
方法はHTTP経由またはTFTP経由を選択できます。
コンフィグレーションファイルはXML形式でダウンロードされます。ダウンロード後に編集することも可能です。
また、本画面では設定の初期化やリブートを行うこともできます。

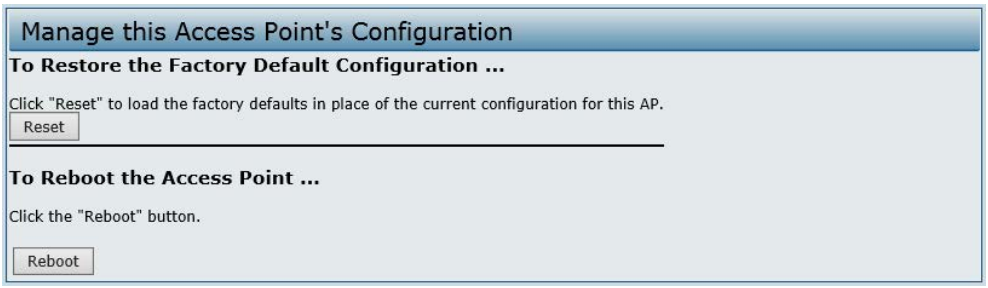


To Restore the Factory Default Configuration.....	
◆ **Reset**	設定を工場出荷時の状態に戻します。 パスワードや無線設定などを含むすべての設定が工場出荷時の設定に戻ります。 本製品の背面にあるリセットボタンを押下して工場出荷時設定にリセットすることもできます。
To Save the Current Configuration to a Backup File	
◆ **Download Method**	現在の設定をコンフィグレーションファイルとしてダウンロードします。 ダウンロード方法は以下から選択してください。 ・[HTTP]: [Download]をクリックし、HTTP経由でダウンロードを行います。 ・[TFTP]: [Configuration File]にファイル名、[Server IP]にTFTPサーバのIPアドレスを入力 →[Download]をクリックします。
To Restore the Configuration from a Previously Saved File	
◆ **Download Method**	保存したコンフィグレーションファイルをリストアします。 リストア方法は以下から選択してください。 ・[HTTP]: [参照]をクリックしてファイルを選択→[Upload]をクリックします。 ・[TFTP]: [Filename]にファイル名、[Server IP]にTFTPサーバのIPアドレスを入力→[Restore]をクリックします。
To Reboot the Access Point.....	
◆ **Reboot**	アクセスポイントを再起動します。

Maintenance（メンテナンス）

[Maintenance] > [Maintenance]

設定の初期化とリブートを行います。



To Restore the Factory Default Configuration.....	
◆ **Reset**	設定を工場出荷時の状態に戻します。 パスワードや無線設定などを含むすべての設定が工場出荷時の設定に戻ります。 本製品の背面にあるリセットボタンを押下して工場出荷時設定にリセットすることもできます。
To Reboot the Access Point.....	
◆ **Reboot**	アクセスポイントを再起動します。

Upgrade（ファームウェアアップグレード）

[Maintenance] > [Upgrade]

ファームウェアのアップグレードを行います。
方法はHTTP経由またはTFTP経由を選択できます。

◆ **Model**	モデル名が表示されます。
◆ **Platform**	プラットフォーム名が表示されます。
◆ **Firmware Version**	現在のファームウェアバージョンが表示されます。
◆ **Upload Method**	ファームウェアアップグレードの方法を以下から選択してください。 • [HTTP]: [参照]をクリックしてファイルを選択→[Upgrade]をクリックします。 • [TFTP]: [Image Filemane]にファイル名、[Server IP]にTFTPサーバのIPアドレスを入力→[Upgrade]をクリックします。

重要

- アップグレード中はWeb GUIに経過画面が表示されます。そのままお待ちください。
- アップグレードには数分かかることがあり、その間本製品は使用できなくなります。
- アップグレードを行っている間は、本製品の電源を切らないでください。アップグレードが終了すると本製品は再起動されます。本製品は、アップグレード前と同じ設定で動作を開始します。

Packet Capture（パケットキャプチャ設定）

[Maintenance] > [Packet Capture]

無線パケットキャプチャは次の2つのモードで動作します

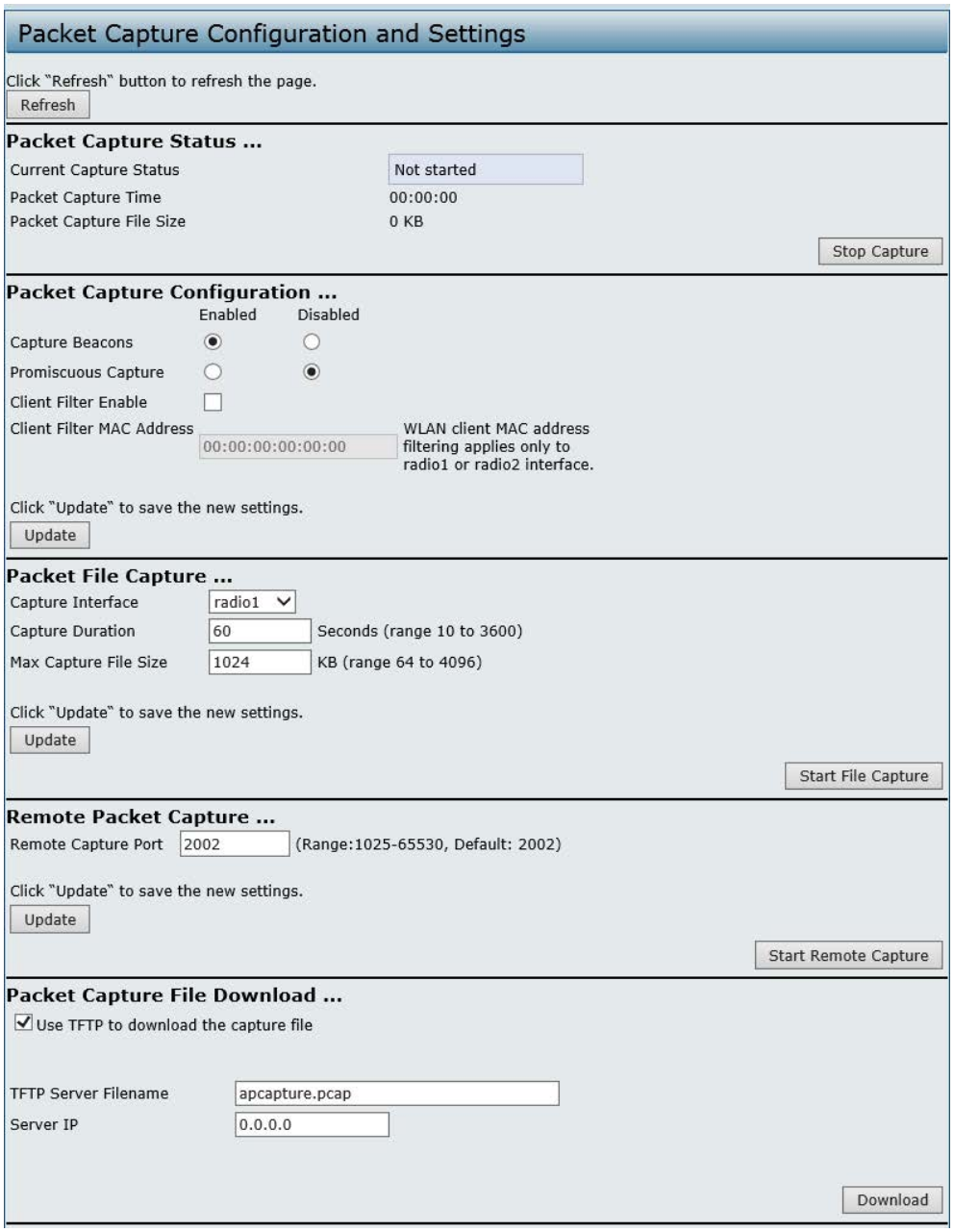
- **キャプチャファイルモード**
  キャプチャされたパケットはファイルとしてアクセスポイントに保存されます。アクセスポイント はファイルをTFTP サーバに送信することが可能です。ファイルはpcap フォーマットで保存されWiresharkや「OmniPeek」といったアプリケーションで使用可能です。
- **リモートキャプチャモード**
  キャプチャされたパケットは「Wireshark®」ツールを起動している外部PC にリアルタイムで排出されます。

アクセスポイントは以下の種類のパケットをキャプチャすることができます。

- 無線インタフェースで送受信された802.11 パケット。無線インタフェースでキャプチャされた802.11 ヘッダを含むパケット。
- イーサネットインタフェースで送受信された802.3 パケット。
- VAPやWDS インタフェースのような内部論理インタフェースで送受信された802.3 パケット。

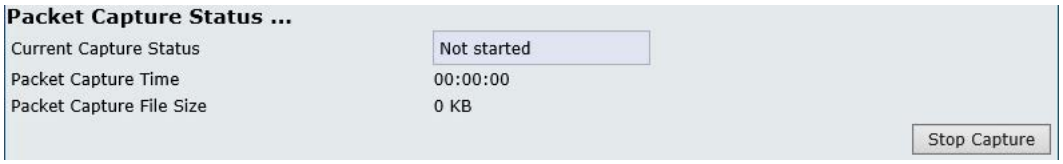
本画面では以下の動作が可能です。

- 現在のパケットキャプチャステータスの確認・変更
- パケットキャプチャ項目の設定
- パケットファイルキャプチャの設定
- リモートキャプチャポートの設定
- パケットキャプチャファイルのダウンロード



■Packet Capture Status

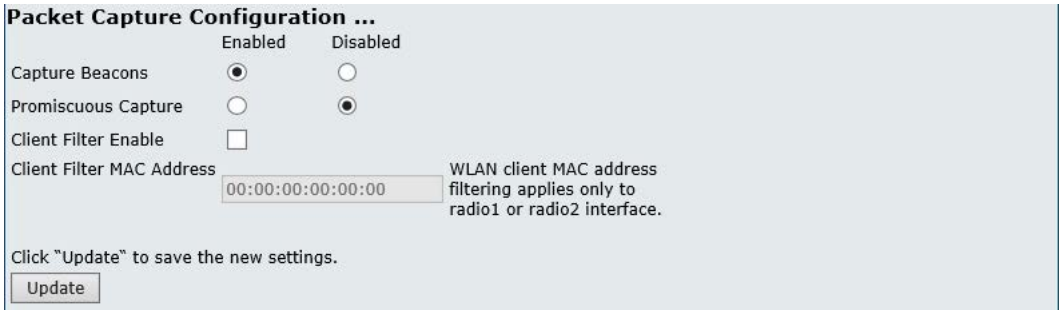
アクセスポイントのパケットキャプチャの状態を表示します。



◆ **Current Capture Status**	現在キャプチャが行われているかどうかが表示されます。
◆ **Packet Capture Time**	パケットをキャプチャした時間が表示されます。
◆ **Packet Capture File Size**	現在のキャプチャファイルのサイズが表示されます。
◆ **Stop Capture**	キャプチャを停止します。

■Packet Capture Configuration

パケットキャプチャの設定を行います。



◆ **Capture Beacons**	無線で送信/ 検出された802.11 ビーコンのキャプチャを[Enabled](有効)または[Disabled](無効)にします。
◆ **Promiscuous Capture**	プロミスキャスモードでのキャプチャを[Enabled](有効)または[Disabled](無効)にします。 有効にすると、アクセスポイント宛ではないトラフィックも含め、チャンネル上のトラフィックすべてを受信します。キャプチャが終了すると、無線の状態はプロミスキャスモードではなくなります。
◆ **Client Filter Enable**	クライアントフィルタを[Enabled](有効)または[Disabled](無効)にします。 有効にすると、WLANクライアントフィルタリングにより、特定のMACアドレスと送受信したトラフィックのみをキャプチャします。
◆ **Client Filter MAC Address**	WLANクライアントフィルタリングで使用するMACアドレスを入力します。
◆ **Update**	設定を適用します。

重要

- パケットキャプチャの設定変更は、パケットキャプチャが再開した時に有効になります。パケットキャプチャセッションが行われている時の変更内容は、現行のパケットキャプチャでは適応されません。
  新しい設定項目を有効にするには、現在のパケットキャプチャセッションを一度止めて再開する必要があります。

■Packet File Capture

パケットキャプチャのインタフェース、期間、最大ファイルサイズを設定し、キャプチャを実行します。
アクセスポイント は、キャプチャしたパケットをシステムのRAM に保存します。
以下の事項が発生するまでパケットキャプチャが続行されます。

- 設定したキャプチャ時間が終了する。
- キャプチャファイルが最大サイズになる。
- 管理者がキャプチャを停止する。

◆ **Capture Interface**	キャプチャを行うインタフェースを以下から選択します。 • [brtrunk]: アクセスポイントのLinuxブリッジインタフェースです。 • [eth0]: イーサネットポートの802.3 トラフィックです。 • [wlan0]: radio 1のVAP0トラフィックです。 • [wlan1]: radio 2のVAP0トラフィックです。 • [radio1]: radio 1の802.11 トラフィックです。 • [radio2]: radio 2の802.11 トラフィックです。
◆ **Capture Duration**	キャプチャを行う期間を設定します。 • 設定可能範囲: 10-3600 (秒)
◆ **Max Capture File Size**	キャプチャファイルの最大サイズを設定します。 • 設定可能範囲: 64-4096 (KB)
◆ **Update**	設定を適用します。
◆ **Start File Capture**	ファイルのキャプチャを開始します。

■Remote Packet Capture

パケットキャプチャの宛先となるリモートポートを指定し、キャプチャを実行します。

本機能はWindows のネットワーク分析ツールのWiresharkとの共同作業となります。パケットキャプチャサーバはアクセスポイントで動作し、TCP 接続を経由してWiresharkツールへキャプチャパケットを送信します。
Wiresharkが起動しているWindows PC でキャプチャされたトラフィックの表示、ログ、分析を行うことが可能です。
リモートキャプチャモードの使用中は、アクセスポイントがファイルシステムにキャプチャデータを保存することはありません。

一度に5 つまでのインタフェースをトレースすることが可能ですが、それぞれのインタフェースで別々のWiresharkセッションを行う必要があります。アクセスポイントとWiresharkを接続するIPポート番号を設定することが可能です。ポート番号の初期値は「 2002」です。システムは連続した5つのポート番号を使用し、パケットキャプチャのセッションを開始します。

Wireshark PC とアクセスポイントの間にファイアウォールが設置されている場合、ポートはファイアウォールを通過できる必要があります。ファイアウォールはまたWireshark PCとアクセスポイントのTCP 接続を許可するように設定されている必要があります。
アクセスポイントをキャプチャパケットの送信元として使用するようにWiresharkを設定するには、「Capture Options」メニューのリモートインタフェースを設定する必要があります。

初期値のIP ポートを使用したradio1のIP アドレス「192.168.1.10」のアクセスポイントのキャプチャパケットの場合、次のようにインタフェースを指定します。

- rpcap://192.168.1.10/radio1

IP ポート「58000」を使用した「radio1」の「VAP0」のAP のイーサネットインタフェースでパケットをキャプチャするためには、Wiresharkセッションを二つ使用し、次のようにインタフェースを指定します。

- rpcap://192.168.1.10:58000/eth0
- rpcap://192.168.1.10:58000/wlan0

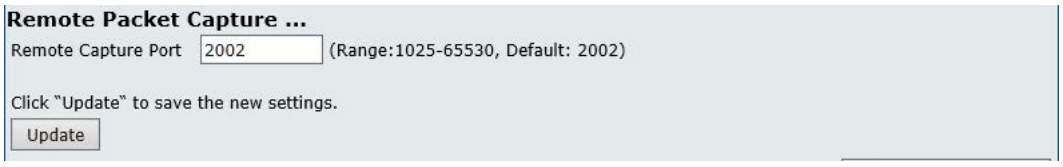
無線インタフェースでトラフィックをキャプチャしている場合、ビーコンキャプチャは無効にできますが、他の802.11 コントロールフレームは Wiresharkへ送信されます。
表示フィルタは以下の通りに設定できます。
・トレース内のデータフレーム
・指定したBSSID のトラフィック
・クライアント間のトラフィック
使用できる表示フィルタの例は以下の通りです。
・除外ビーコンとACK/RTS/CTS フレーム：
・!(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)
・データフレームのみ：
・wlan.fc.type == 2
・指定のBSSID のトラフィック：
・wlan.bssid == 00:02:bc:00:17:d0
・指定クライアントからの全トラフィック：
・wlan.addr == 00:00:e8:4e:5f:8eク

リモートキャプチャモードでは、ネットワークインタフェースの1 つを経由し、Wiresharkを起動しているPC にトラフィックは送信されます。Wiresharkの位置によってはトラフィックはイーサネットインタフェースや無線の1 つに送信されることも可能です。トレースパケットによってトラフィック氾濫が発生するのを避けるために、AP は自動的にWiresharkアプリケーションを宛先にした全パケットをフィルタするキャプチャフィルタをインストールします。
Wireshark IP ポートが「58000」に設定されている場合、アクセスポイントに自動的にインストールされるキャプチャフィルタは次のようになります。
・not portrange 58000-58004.
パケットキャプチャ機能を有効にすると、アクセスポイントのセキュリティ問題が発生する場合があります。(認証されていないクライアントがアクセスポイントに接続しユーザデータをトレースするなど)。アクセスポイントとのWireshark セッションがなくても、アクセスポイントのパフォーマンスへの影響があります。パケットキャプチャが進行している時はパフォーマンスへの影響は広い範囲で発生します。

パフォーマンスとセキュリティ問題によって、パケットキャプチャモードはアクセスポイントのNVRAM に保存されません。アクセスポイントがリセットすると、キャプチャモードは無効になり、トラフィックをキャプチャするには再度有効にする設定を行わなければいけません。パケットキャプチャパラメータはNVRAM に保存されます。
トラフィックキャプチャが進行中にAP へのパフォーマンスへの影響を最小限に抑えるためには、Wiresharkツールに送信するトラフィックに制限をかけるために、キャプチャフィルタをインストールすると有効です。802.11 トラフィックをキャプチャする時、キャプチャされたフレームの大部分はビーコンへとなる傾向にあります。(通常全てのアクセスポイントにより100ms 毎に送信されます。) Wiresharkがビーコンフレーム用に表示フィルタをサポートしていても、Wiresharkツールへのキャプチャされたビーコンパケットの転送からAP を防ぐキャプチャフィルタはサポートしていません。
802.11 ビーコンのキャプチャによるパフォーマンスへの影響を削減するには、キャプチャビーコンモードを無効にすることも可能です。リモートパケットキャプチャ機能はWindows のWireshark ツールに標準搭載されています。

メモ

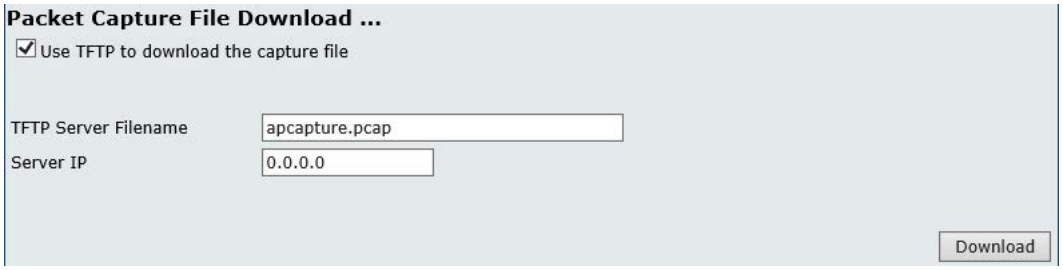
・リモートパケットキャプチャはLinuxバージョンのWiresharkでは標準ではありません。LinuxバージョンはAP で動作しません。
・Wiresharkはオープンソースツールで無料で使用することが可能です。
http://www.wireshark.orgからダウンロードできます。



◆ **Remote Capture Port**	パケットキャプチャの宛先となるリモートポートを指定します。 ・設定可能範囲: 1-65530
◆ **Update**	設定を適用します。
◆ **Start Remote Capture**	リモートキャプチャを開始します。

■Remote Packet Capture

TFTP経由またはHTTP経由でキャプチャファイルをダウンロードします。



◆ **Use TFTP to download the capture file**	チェックをいれた場合、TFTPサーバ経由でキャプチャファイルをダウンロードします。 チェックを外した場合、HTTP経由でキャプチャファイルをダウンロードします。
◆ **TFTP Server Filename**	ダウンロード方法にTFTP経由を選択した場合、ファイル名を指定します。
◆ **Server IP**	ダウンロード方法にTFTP経由を選択した場合、サーバのIPアドレスを入力します。
◆ **Download**	キャプチャファイルのダウンロードを開始します。

Support Information（サポート情報）

[Maintenance] > [Support Information]

アクセスポイントのサポート情報をダウンロードできます。
サポート情報には、本製品のハードウェア/ファームウェアバージョンや、設定内容が記載されています。

◆ **Download**	サポート情報をRTFファイルとしてダウンロードします。

Cluster

8

クラスタの設定方法について説明します。
クラスタを使用することにより、ユーザーアカウントや設定を一括して管理することができます。

Access Points（クラスタによるアクセスポイントの管理）

[Cluster] > [Access Points]

複数の無線アクセスポイントをグループ化したものをクラスタと呼びます。
各クラスタは最大16 個のメンバを持つことができます。1 つの無線ネットワークあたり1 個のクラスタだけがサポートされていますが、ネットワークサブネットは複数のクラスタを持つことができます。クラスタはVAP 設定やQoS キューパラメータなどの様々な設定情報を共有できます。
本クラスタ機能は、情報を共有するための機能であり、耐障害性の機能ではありません。

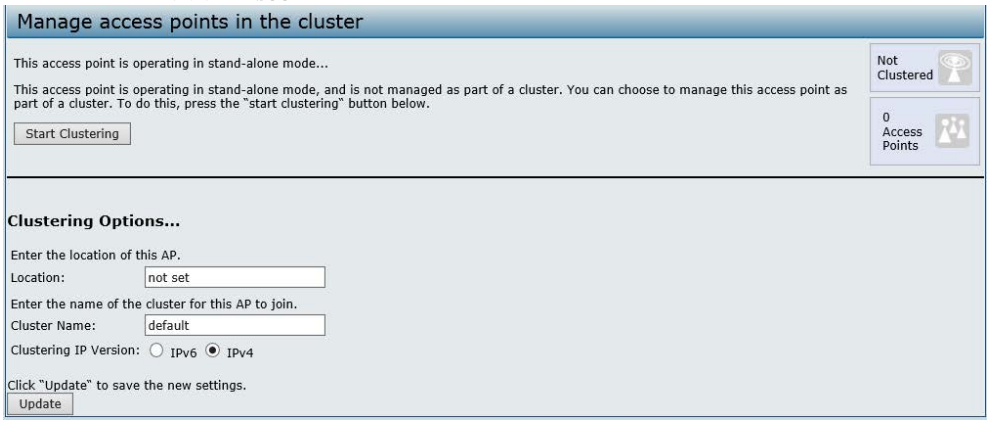
以下の条件が満たされる場合、2 つのアクセスポイント間でクラスタを形成できます。
- アクセスポイントが同一のモデルである
- アクセスポイントが同じブリッジを使用したセグメントで接続されている
- クラスタを接続するアクセスポイントは、同じクラスタ名を持っている
- クラスタリングモードが両方のアクセスポイントで有効になっている

重要

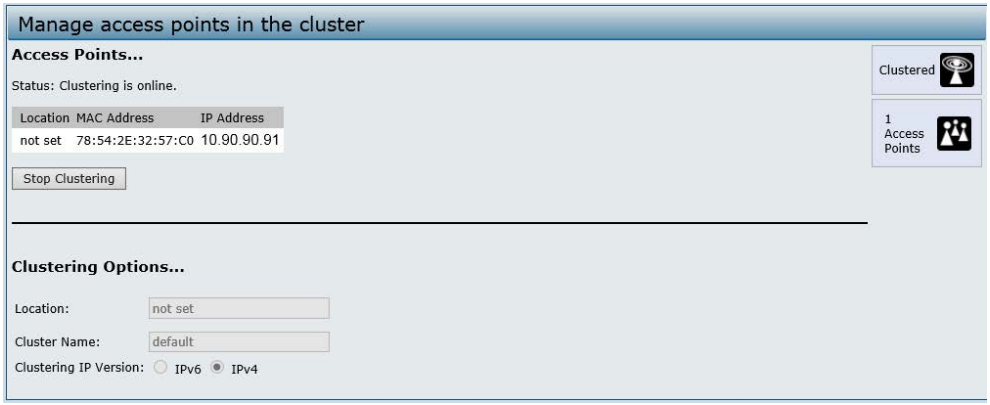
- 2 つのアクセスポイントが同じクラスタに所属するためには、同じ無線インタフェース番号を持つ必要はありませんが、無線帯のサポート機能は同じである必要があります。
- APクラスタ機能は、同一機種間、同一ファームウェアバージョン間のみサポートされます。

本画面では、クラスタリングの開始／停止、クラスタメンバの参照、クラスタメンバのロケーションとクラスタ名の設定を行います。

クラスタリングが無効の場合



クラスタリングが有効の場合



◆ **Status**	クラスタリングが有効になっている場合に表示されます。 • [Location]:アクセスポイントが物理的に位置している場所が表示されます。 • [MAC Address]:アクセスポイントのMACアドレスが表示されます。 • [IP Address]:アクセスポイントのIPアドレスが表示されます。
◆ **Stop Clustering** ◆ **Start Clustering**	クラスタリングの開始／停止を行います。
◆ **Location**	アクセスポイントが物理的に位置している場所に関する説明を入力します。
◆ **Cluster Name**	アクセスポイントが接続するクラスタ名を入力します。クラスタ名はクラスタ内の他のアクセスポイントには送信されません。クラスタのメンバである各アクセスポイントには同じクラスタ名を設定する必要があります。クラスタ名はネットワーク内の各クラスタごとに固有である必要があります。
◆ **Clustering IP Version**	クラスタ内のアクセスポイントが相互に通信するために使用するIP バージョン（IPv6 またはIPv4）を指定します。
◆ **Update**	設定を適用します。

■クラスタからアクセスポイントを削除する

クラスタからアクセスポイントを削除する手順について説明します。

1. クラスタリングしているアクセスポイントの管理 Web マネージャを表示します。
2. [Cluster] > [Access Points] メニューをクリックします。
3. [Stop Clustering] をクリックします。

   アクセスポイントはクラスタのメンバではなくなります。
   ステータスアイコンは以下の通り「Not Clustered」となります。

■クラスタからアクセスポイントを追加する

クラスタからアクセスポイントを削除する手順について説明します。

1. クラスタリングしているアクセスポイントの管理 Web マネージャを表示します。
2. [Cluster] > [Access Points] メニューをクリックします。
3. [Start Clustering] をクリックします。

   アクセスポイントはクラスタのメンバとなります。
   ステータスアイコンは以下の通り「Clustered」となります。

● 特定アクセスポイントの設定情報への移動

Unified APでは、クラスタ内のすべてのアクセスポイントが同じコンフィグレーションを反映するため、クラスタリングしているアクセスポイントの設定を一括で変更できます。管理のために実際にどのアクセスポイントに接続するかは重要ではありません。
各アクセスポイントのクライアント接続またはイベントなどのステータス情報のチェックを行うなど、特定のアクセスポイントに関する情報を参照／管理する場合は、Cluster > Access Points 画面にあるIPアドレスのリンクをクリックすることによって、各アクセスポイントの管理Web インタフェースに移動することができます。
すべてのクラスタリングしているアクセスポイントはCluster > Access Points 画面に表示されます。クラスタリングしているアクセスポイントへ移動するためには、リストに示される特定のクラスタメンバのIP アドレスをクリックします。

● URLにIPアドレス使用してアクセスポイントに移動する

以下の形式でWeb ブラウザのアドレスにそのアクセスポイントのIP アドレスを入力することで特定のアクセスポイントの管理Web画面にリンクできます。

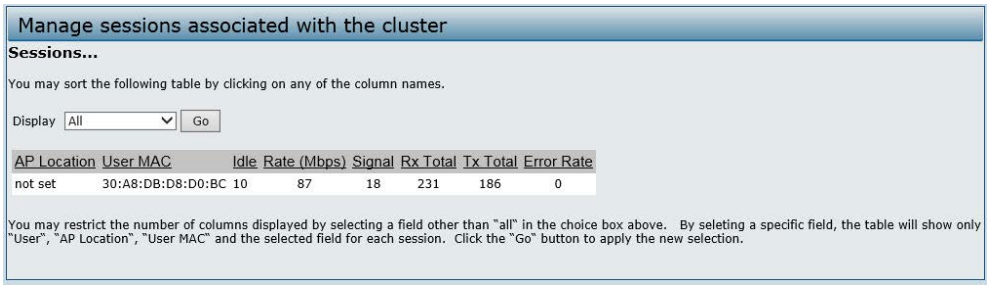
http:// アクセスポイントのIP アドレス

「アクセスポイントのIP アドレス」は、モニタリングまたは設定する特定のアクセスポイントのアドレスです。

Sessions（クラスタセッションの管理）

[Cluster] > [Sessions]

クラスタ内のアクセスポイントに接続するクライアントステーションの情報を表示します。
各クライアントは、現在接続するアクセスポイント（ロケーション）と共にMAC アドレスで識別されます。



◆ **Display**	表示する統計情報を[All][Idle] [Time][Data Rate][Signal][Receive Total][Transmit Total][Error Rate] から選択します。
◆ **AP Location**	アクセスポイントが位置している場所が表示されます。
◆ **User MAC**	ワイヤレスクライアントデバイスのMACアドレスが表示されます。
◆ **Idle**	このステーションが動作していない（アイドル状態）時間が表示されます。 ステーションがデータを送受信していない場合、アイドル状態とみなされます。
◆ **Rate (Mbps)**	このアクセスポイントが指定クライアントにデータを送信する速度（単位：Mbps）が表示されます。この値はアクセスポイントが使用しているモードの速度設定の範囲内になります。 （例：802.11a では6-54Mbps）
◆ **Signal**	クライアントがアクセスポイントから受信する無線周波（RF）信号の強さを示します。 値はReceived Signal Strength Indication（RSSI）によって算出されます。
◆ **Rx Total**	このセッションでクライアントが受信した総パケット数が表示されます。
◆ **Tx Total**	このセッションでクライアントに送信した総パケット数が表示されます。
◆ **Error Rate**	このアクセスポイントにおいて伝送の間に破棄された時間フレームの割合を示します。

● セッション情報のソート

テーブルに示される情報を特定の指示でソートするためには、並べ替える欄のラベルをクリックします。例えば、信号強度で並べたテーブルの行を参照する場合、[Signal]欄のラベルをクリックします。エントリは信号強度によってソートされます。

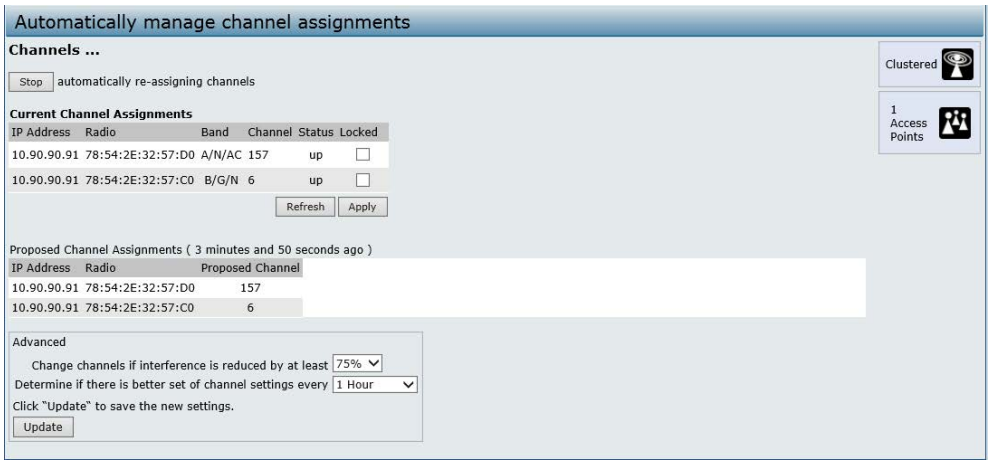
Channel Management（チャンネルの管理）

[Cluster] > [Channel Management]

チャンネル管理が有効な場合、本製品は自動的にクラスタリングしているアクセスポイントが使用する無線チャンネルを割り当てます。自動チャンネル割り当ては、相互干渉（または、クラスタの外側にある他のアクセスポイントとの混信）を抑制し、Wi-Fi 帯域幅を最大にすることで無線ネットワークの通信効率を維持するために役立ちます。

自動チャンネル割り当てを行うためには、チャンネル管理を開始する必要があります。新しいアクセスポイントの初期値は[Disabled]（無効）になっています。

指定した間隔で、チャンネルマネージャがアクセスポイントにチャンネルの使用を割り当て、クラスタ内の干渉レベルを測定します。重要なチャンネル妨害が検出されると、チャンネルマネージャは自動的に効率のよいアルゴリズム（または、自動化されたチャンネルプラン）に従って新しいチャンネルにアクセスポイントのいくつかまたはすべてを再度割り当てます。クラスタリングしているアクセスポイントの過去、現在、および計画されたチャンネル割り当てを表示します。



◆ **Start/Stop**	自動チャンネル割り当てを[Start](開始)または[Stop](停止)します。
Current Channel Assignments	
現在のチャンネル割り当て状況が表示されます。	
◆ **IP Address**	アクセスポイントのIPアドレスが表示されます。
◆ **Radio**	周波数帯のMAC アドレスが表示されます。
◆ **Band**	アクセスポイントがブロードキャストしている帯域が表示されます。
◆ **Channel**	チャンネルが表示されます。
◆ **Status**	ステータスが表示されます。
◆ **Locked**	チェックをいれるとチャンネルの割り当て状況がロックされます。
◆ **Refresh**	表示を更新します。
◆ **Apply**	設定を適用します。
Proposed Channel Assignments　（XX minutes and XX seconds ago）	
最後に提案された変更の設定内容が表示されます。 自動チャンネル割り当てが動作中の場合にのみ表示されます。	
◆ **IP Address**	アクセスポイントのIPアドレスが表示されます。
◆ **Radio**	周波数帯のMAC アドレスが表示されます。
◆ **Proposed Channel Assignments**	チャンネルプランが実行される場合、このアクセスポイントが再割り当てされる無線チャンネルを示します。
Advanced	
チャンネル割り当ての詳細設定を行います。 ・[Change channel if interface is reduced by at least]:ここで設定した割合まで干渉が削減された場合にチャンネル変更を実行します。 ・[Determine if there is better set of channel settings every]:自動更新のスケジュールを選択します。	
◆ **Update**	設定を適用します。

Wireless Neighborhood（無線近接デバイス情報の参照）

[Cluster] > [Wireless Neighborhood]

クラスタ内の全メンバの適用範囲で無線インタフェースごとに最大20 個のアクセスポイントを表示し、どのアクセスポイントがどのクラスタメンバの適用範囲にあるかを表示します。また、クラスタメンバとクラスタメンバでないものを区別します。

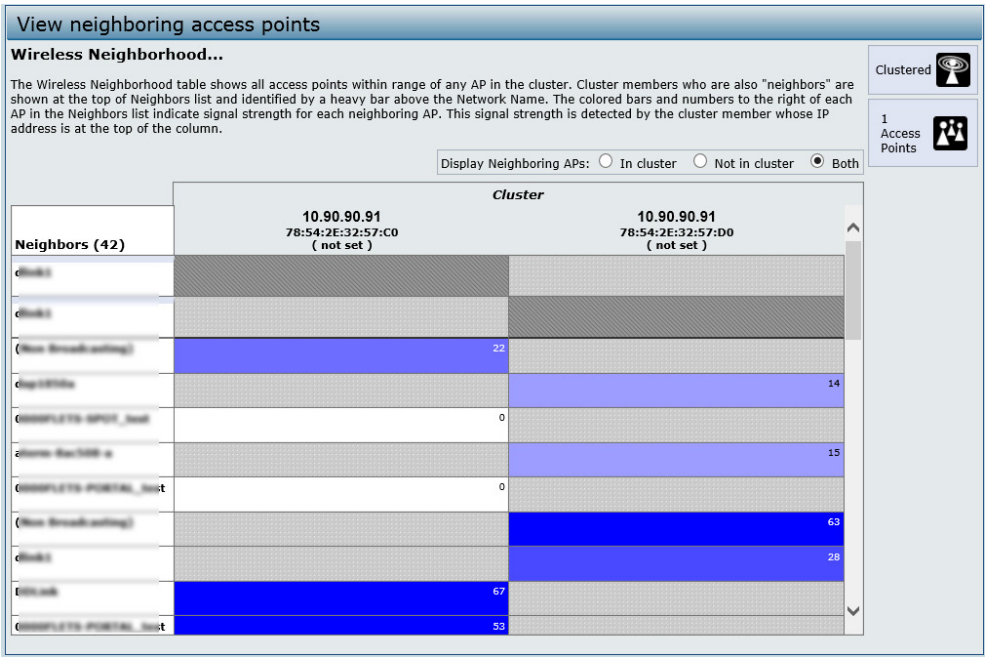
重要

- 無線インタフェースごとに最大20 個のアクセスポイントを表示します。指定のクラスタアクセスポイントで検出されたアクセスポイントのすべてを参照するためには、そのクラスタメンバのWeb インタフェースに移動し、Status > Neighboring Access Points 画面を表示します。

各Neighbor アクセスポイントに対して無線インタフェースの統計情報（信号強度、チャンネル、ビーコン間隔）と共に識別情報（SSID、ネットワーク名、IP アドレス、MAC アドレス）を表示します。アクセスポイントをクリックし、現在選択しているアクセスポイントの無線帯域の範囲内にあるアクセスポイントに関する追加の統計情報を取得します。

Wireless Neighborhoodによって以下の内容を確認することができます。

- 無線ドメイン内で予期しない（不正な）アクセスポイントを検出し、関連するリスクを回避することができます。
- 予測される適用範囲を検証します。アクセスポイントが他のアクセスポイントからの信号強度の大きさを目に見えるもので評価することによって、配置が計画している目標を達成することを確認することができます。
- 故障を検出します。カバレッジパターンの予期しない変更は、カラーコード化テーブルに反映されます。



◆ **Display Neighboring APs**	表示内容を以下から選択します。 • [In cluster]:クラスタのメンバであるNeighbor AP のみを表示します。 • [Not in cluster]:クラスタメンバではないNeighbor AP のみを表示します。 • [Both]:すべてのNeighbor APを表示します。
◆ **Cluster**	クラスタ内の全アクセスポイントのIP アドレスが表示されます。 クラスタに1 つのアクセスポイントしか存在しない場合、1 つのIP アドレス欄のみが表示されます。
◆ **Neighbors**	Neighbor アクセスポイントが表示されます。 クラスタリングしている 1 つ以上のアクセスポイントのNeighbor アクセスポイントは、SSID（ネットワーク名）ごとに表示されます。 クラスタメンバのNeighborとして検出されるアクセスポイントは、クラスタメンバ自身である可能性もあります。クラスタメンバであるNeighbor は上のリストの先頭に常に表示され、ロケーション表示もあります。 カラーバーの色は信号の強さを示しています。 • 濃い青色のバー 濃い青色のバーと高い信号強度番号（例：50）は、IP アドレスが欄の上に表示されているアクセスポイントが参照したNeighbor から検出された良好な信号強度を示します。 • 薄い青色のバー 薄い青色のバーと低い信号強度番号（例：20 以下）は、IP アドレスが欄の上に表示されているアクセスポイントが参照したNeighbor から検出された中間または弱い信号強度を示します。 • 白いバー 白いバーと番号「0」は、クラスタメンバの 1 つが検出したNeighbor AP をIP アドレスが、その欄の上に表示されているアクセスポイントでは検出できないことを示します。 • 薄いグレーのバー 信号強度の表示がグレーのバーは、IP アドレスがその欄の上に表示されているアクセスポイントではなく、他のクラスタメンバによって検出されたNeighbor を示します。 • 濃いグレーのバー 信号強度の表示が濃いグレーのバーは、アクセスポイントが自身を検出する方法を参照するためには適用しないため、IP アドレスがその欄の上に表示されているアクセスポイントであることを示します。

■クラスタメンバに関する詳細情報の参照

クラスタメンバのアクセスポイントに関する詳細情報を参照するためには、画面先頭にあるクラスタメンバのIP アドレスをクリックします。

Neighbor Details

10.90.90.91

SSID	MAC Address	Channel	Rate	Signal	Beacon Interval	Beacon Age
(Non Broadcasting)	02:A0:BB:F2:5C:AE	1	1	87	100	Fri Dec 31 12:00:03 1999
D-Link_Guest	0E:19:8F:F0:A3:2E	1	1	70	100	Fri Dec 31 12:00:03 1999
(Non Broadcasting)	12:A0:BB:F2:5C:3C	1	1	88	100	Fri Dec 31 12:00:03 1999

◆ **SSID**	SSIDが表示されます。
◆ **MAC Address**	MAC アドレスが表示されます。
◆ **Channel**	アクセスポイントが現在ブロードキャストを行っているチャンネルが表示されます。
◆ **Rate**	アクセスポイントの現在の送信速度（Mbit/s）が表示されます。
◆ **Signal**	このアクセスポイントが出力する信号強度（Db）が表示されます。
◆ **Beacon Interval**	このアクセスポイントによって使用されるビーコン間隔が表示されます。
◆ **Beacon Age**	このアクセスポイントが最後のビーコンを受信した日時を表示されます。

Client QoS

9

無線クライアントからアクセスポイントへのトラフィックに作用するQoS の設定方法について説明します。統合アクセスポイントのクライアントQoS 機能を使用して、帯域制限を行い、無線インタフェースにアクセスコントロールリストおよびDiffServ ポリシーを適用することができます。

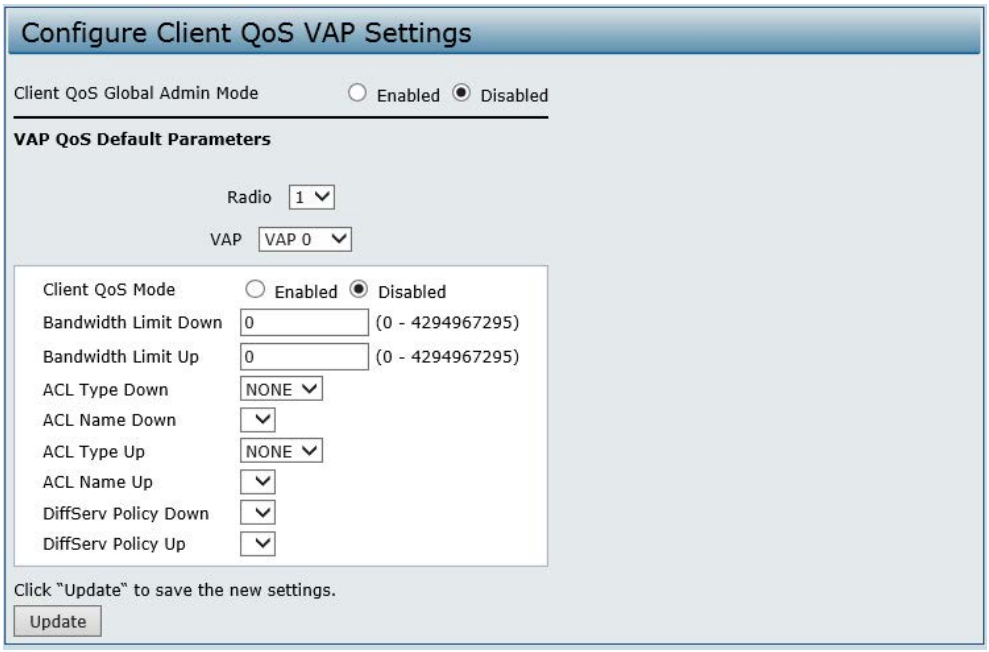
VAP QoS Parameters（VAP QoS パラメータの設定）

[Client QoS] > [VAP QoS Parameters]

クライアントQoS の管理モードを設定し、VAP のQoS 設定を行います。
本製品のクライアントQoS 機能を使用すると、ネットワークに接続する無線クライアントのQoS に対し、個々のクライアントが送受信を許可される帯域幅のコントロールなどのより詳細な制御を行うことができます。
HTTP トラフィックや特定サブネットからのトラフィックなどの一般的なカテゴリのトラフィックを制御するために、アクセスコントロールリストを設定し、1 つ以上のVAP に割り当てることが可能です。

また、クライアントのQoS では、各クライアントがDiffServ による様々なマイクロフロー調整を行うように設定することができます。DiffServ ポリシーは、ネットワーク上でインバウンド／アウトバウンド両方のトラフィックを認証する時に、各無線クライアントに適用する一般的なマイクロフロー定義および特性処理を確立するのに役立つツールです。

クライアントのClient QoS 機能を有効にして、クライアントの帯域制限を指定し、VAP に接続するクライアントがRADIUS サーバによって定義される属性を持たない場合、アクセスコントロールリストおよびDiffServポリシーを選択して初期値として使用します。



◆ **Client QoS Global Admin Mode**	アクセスポイントのクライアントQoS 機能を[Enabled](有効)または[DIsabled](無効)にします。本設定を変更しても、QoS 画面で行ったWMM設定は変更されません。
VAP QoS Default Parameters	
◆ **Radio**	設定する無線インタフェースを[1]または[2]から選択します。
◆ **VAP**	クライアントQoS 設定を行うVAP（VAP 0-15）を指定します。指定したVAP に設定したQoS は、他のVAP 経由でネットワークに接続しているクライアントには適用されません。
◆ **Client QoS Mode**	VAP メニューから選択したVAP のQoS 機能を[Enabled](有効)または[DIsabled](無効)にします。クライアントQoS 設定を無線クライアントに適用するためには、[Client QoS Global Admin Mode]欄でクライアントQoS 機能を有効にし、さらに本欄のVAP を有効にする必要があります。
◆ **Bandwidth Limit Down**	アクセスポイントから無線クライアントへの最大送信速度（bps）を入力します。 ・設定可能範囲:0-4294967295（bps） 0 は、最大帯域幅の制限が実施されないことを意味します。
◆ **Bandwidth Limit Up**	無線クライアントからアクセスポイントへの最大送信速度（bps）を入力します。 ・設定可能範囲:0-4294967295（bps） 0 は、最大帯域幅の制限が実施されないことを意味します。
◆ **ACL Type Down**	アウトバウンドトラフィックに適用するアクセスコントロールリストのタイプを選択します。 ・選択肢：[NONE][IPv4][IPv6][MAC]
◆ **ACL Name Down**	アウトバウンドトラフィックに適用するアクセスコントロールリスト名を選択します。
◆ **ACL Type Up**	インバウンドトラフィックに適用するアクセスコントロールリストのタイプを選択します。 ・選択肢：[NONE][IPv4][IPv6][MAC]
◆ **ACL Name Up**	インバウンドトラフィックに適用するアクセスコントロールリスト名を選択します。
◆ **DiffServ Policy Down**	アウトバウンドトラフィックに適用するDiffServ ポリシー名を選択します。
◆ **DiffServ Policy Up**	インバウンドトラフィックに適用するDiffServ ポリシー名を選択します。
◆ **Apply**	設定を適用します。

Client QoS ACL（クライアントQoS ACL の管理）

[Client QoS] > [Client QoS ACL]

クライアントQoS で使用するアクセスコントロールリストの管理を行います。

アクセスコントロールリストは、許可と拒否の条件をまとめたものであり、特定のリソースにアクセスする非認証のユーザを防ぎ、認証されたユーザに許可を与えて安全性を提供します。

● IPv4/IPv6 アクセスコントロールリスト

IPv4/IPv6アクセスコントロールリストは、レイヤ3 およびレイヤ4 のトラフィックを分類します。各アクセスコントロールリストは最大 10 個のルールの集まりで、無線クライアントから送信されたトラフィックや無線クライアントに送信されるトラフィックに適用されます。各ルールは各欄のコンテンツを使用して、ネットワークへの接続を許可するべきか、拒否するべきかを指定します。ルールはさまざまな基準に基づくことができ、送信元および送信先 IP アドレス、レイヤ4 ポート、あるいは、パケットが運ぶプロトコルなど、パケット内の複数のフィールドに適用することが可能です。

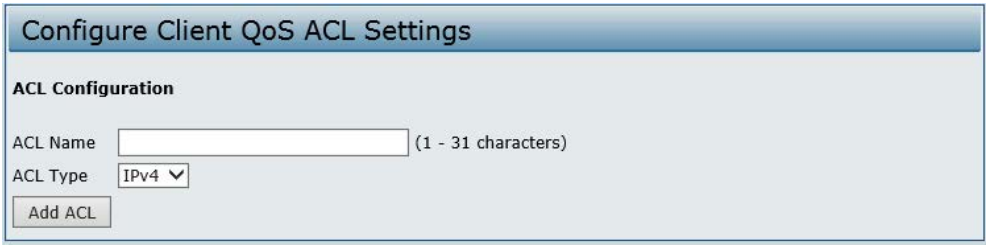
● MAC アクセスコントロールリスト

MAC アクセスコントロールリストはレイヤ2 ACL です。宛先/ 送信元MAC アドレス、VLAN ID、Class of Service 802.1p priority などのフレームの項目検査のルールを設定できます。フレームがAP ポートに入る/ 出る時（ACL が「up」または「down」のどちらかに設定されているかに依存する。）、AP はフレームを検査し、ACL ルールがフレームの内容に違反していないかチェックします。もしルールが1 つでも内容に合致している場合、許可また拒否の動作がフレームに対して行われます。

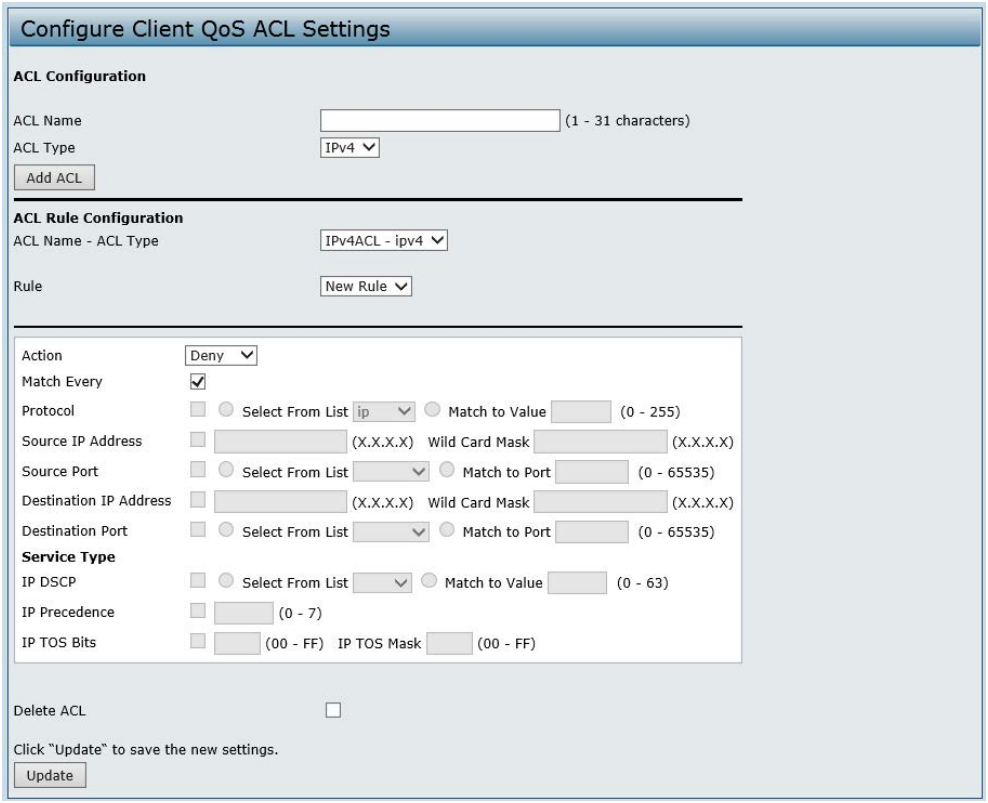
■アクセスコントロールリストの設定手順

アクセスコントロールリストおよびルールの設定を行い（手順1-5）、特定のVAP にルールを適用します（手順6、7）。

1. [Client QoS] > [Client QoS ACL] の順にメニューをクリックし、以下の画面を表示します。



2. [Class Map Name] にクラスマップ名を入力→ [ACL Type] でアクセスコントロールリストのタイプを指定します。
3. [Add ACL] をクリックします。
4. [ACL Name] で設定する ACL を選択→ [ACL Rule Configuration] 欄で ACL ルールの内容を設定します。

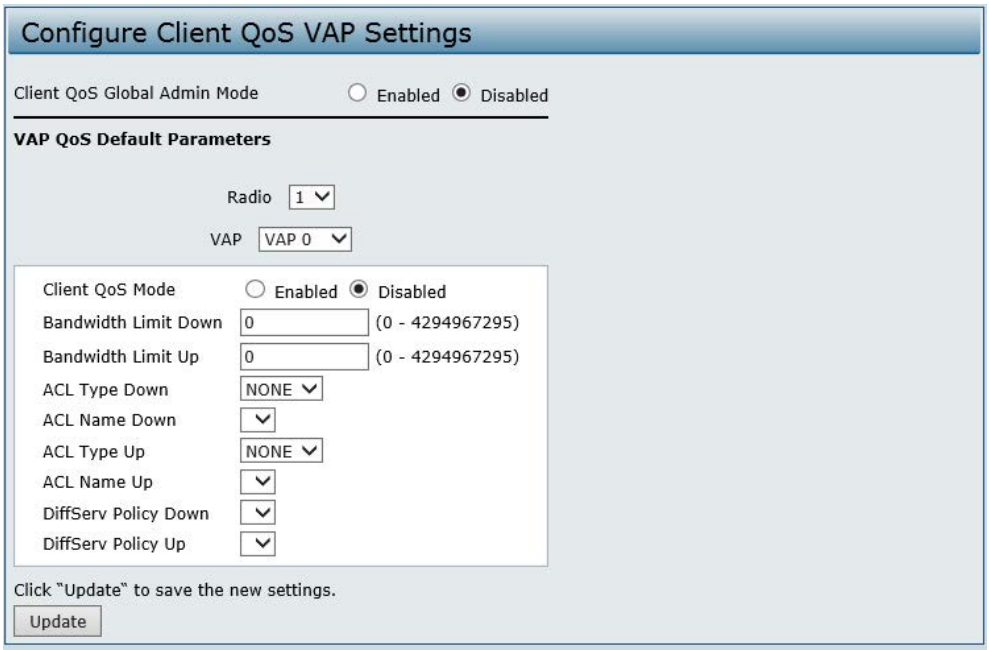


重要

- [ACL Rule Configuration]欄の内容は選択したACLタイプによって異なります。
  詳細は『ACLルールの設定内容：p.99』を参照してください。
- [Delete ACL]にチェックをいれて[Update]をクリックすると、アクセスコントロールリストを削除できます。

5. [Update] をクリックし、設定を適用します。

6. 作成したアクセスコントロールリストを 1 つ以上の VAP に適用します。
   [Client QoS] > [VAP QoS Parameters] の順にメニューをクリックし、以下の画面を表示します。

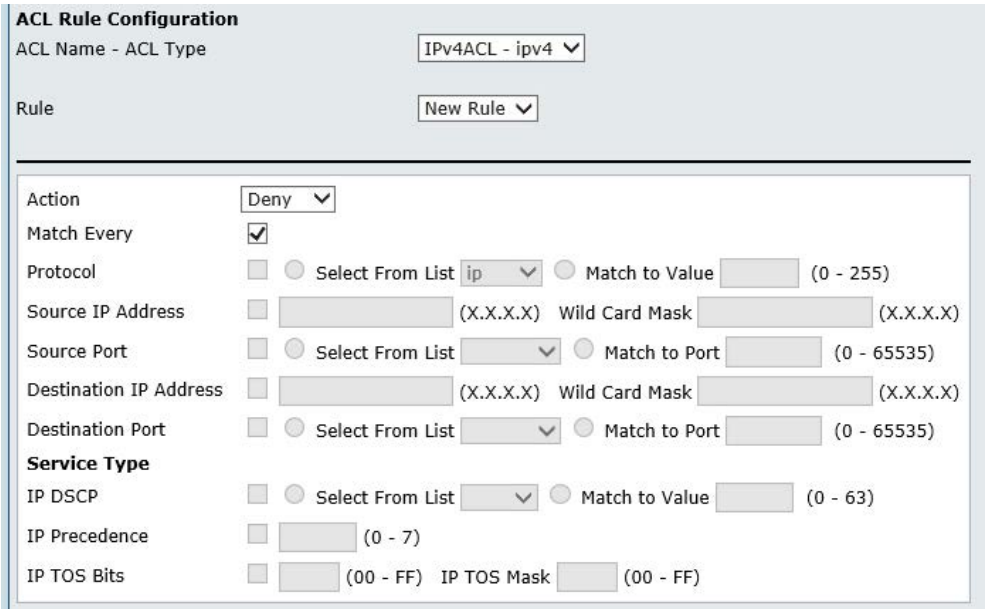


7. [QoS Mode] で [Enabled]、[ACL Type Down] または [ACL Type Up] で [IPv4] を選択後に [ACL Name Down] または [ACL Name Up] で ACL を選択します。

■ACLルールの設定内容

アクセスコントロールリストのタイプによって、ACLルールの設定内容が異なります。
設定した内容に一致しているトラフィックが許可または拒否されます。

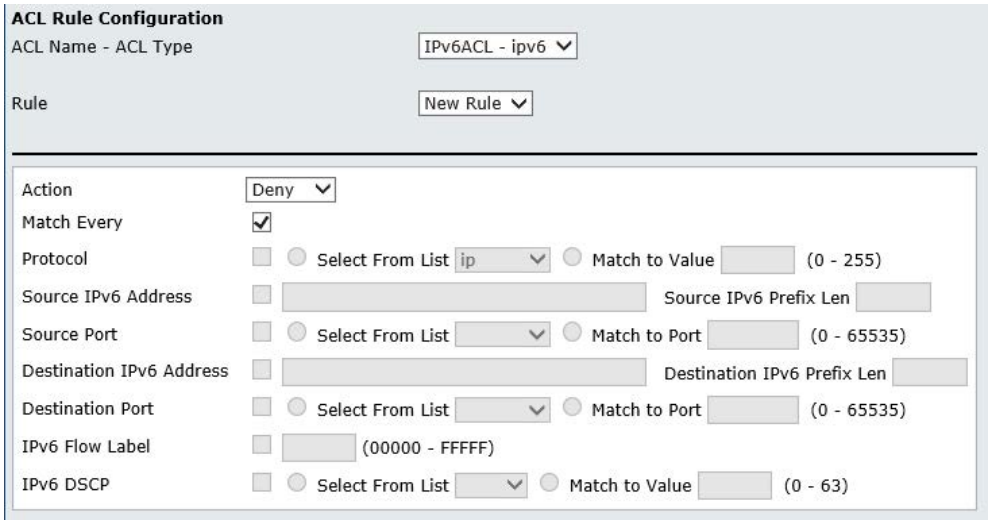
● IPv4アクセスコントロールリスト



◆ **ACL Name - ACL Type**	設定を行うACL名を選択します。
◆ **Rule**	ACLに適用するルールを選択、または[New Rule]を選択して新しいルールを設定します。 ACL 内の複数のルールは、ACL に追加した順番でパケットに適用されます。最終ルールとして、「implicit deny all rule」(暗黙の全否定) があります。
◆ **Action**	ACLルールのアクションを選択します。 • [Permit] アクセスポイントへの送受信の基準に一致するトラフィックはすべて許可されます。 基準に一致しないトラフィックはすべて廃棄されます。 • [Deny] アクセスポイントへの送受信の基準に一致するトラフィックをすべて拒否します。 基準に一致しないトラフィックはすべて送信されますが、最終ルールの場合は異なります。 各ACLの最後には「implicit deny all rule」(暗黙の全否定) という最終ルールがあり、明らかに許可されたトラフィック以外は廃棄されます。
◆ **Match Every**	許可または拒否いずれかのアクションを持つルールを、パケットのコンテンツに関わらず一致させるよう指示します。選択すると、照合基準を追加設定することはできません。 新規のルールには初期値で「Match Every」オプションが選択されています。他の基準を設定する場合は本オプションのチェックを外してください。
◆ **Protocol**	プロトコルを選択します。 • [Select From List]: 以下からプロトコルを選択します。 - [IP][ICMP][IGMP][TCP][UDP] • [Match to Value]:名称でリストアップされないプロトコルに一致させる場合に、プロトコル ID を入力します。プロトコルID は、IANA によって割り当てられたプロトコル番号です。(設定可能範囲:0-255)
◆ **Source IP Address**	送信元IP アドレスを設定します。
◆ **Wild Card Mask**	送信元IP アドレスをワイルドカードマスクに指定します。 ワイルドカードマスクは、一致させるビットと無視するビットを決定するものです。 「255.255.255.255」のワイルドカードマスクは、すべてのビットを無視することを示します。ワイルドカードが「0.0.0.0」の場合は、すべてのビットを一致させることを示します。 本欄は、[Source IP Address]ボックスがチェックされている場合にのみ入力します。 ワイルドカードマスクは、実際にはサブネットマスクを逆にします。 シングルホストアドレスに基準を一致させる場合は、ワイルドカードマスク「0.0.0.0」を使用します。24 ビットのサブネット (例 :192.168.10.0/24) に基準を一致させる場合は、評価基準を合わせるために、「0.0.0.255」のワイルドカードマスクを使用します。

◆ **Source Port**	送信元ポートを設定します。送信元ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信元ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信元ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび/ またはプライベートポート
◆ **Destination IP Address**	送信先IP アドレスを設定します。
◆ **Wild Card Mask**	送信先IP アドレスをワイルドカードマスクに指定します。 ワイルドカードマスクは、一致させるビットと無視するビットを決定するものです。 「255.255.255.255」のワイルドカードマスクは、すべてのビットを無視することを示します。ワイルドカードが「0.0.0.0」の場合は、すべてのビットを一致させることを示します。 本欄は、[Source IP Address]ボックスがチェックされている場合にのみ入力します。 ワイルドカードマスクは、実際にはサブネットマスクを逆にします。 シングルホストアドレスに基準を一致させる場合は、ワイルドカードマスク「0.0.0.0」を使用します。24 ビットのサブネット（例：192.168.10.0/24）に基準を一致させる場合は、評価基準を合わせるために、「0.0.0.255」のワイルドカードマスクを使用します。
◆ **Destination Port**	送信先ポートを設定します。送信先ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信先ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信先ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび/ またはプライベートポート
◆ **IP DSCP**	IP DSCP値を設定します。 • [Select From List]: DSCP タイプを選択します。 • [Match to Value]:照合するDSCP 値（0-63）を入力します。
◆ **IP Precedence**	IP Precedence値を設定します。 IP Precedence値によってIPパケットの優先度が決定されます。値は高い値ほど優先度が高くなります。
◆ **IP TOS Bits**	IP ヘッダのサービスタイプのビット値を入力します。 パケット内のIP TOS フィールドは、IP ヘッダの「Service Type」オクテットの全8 ビットとして定義されます。この値は、00-FF までの2 桁の16 進数です。上位3 ビットはIP 優先度値を表します。上位6 ビットはIP Differentiated Services Code Point（DSCP）値を表します。
◆ **IP TOS Mask**	IP TOS マスク値を入力し、パケットの「IP TOS」フィールドと比較するために使用されるTOS ビット値内のビット位置を指定します。TOS マスク値は、00 ～ ff までの2 桁の16 進数で、逆（ワイルドカード）マスクを表します。「TOSMask」内の「0」の値は、パケットの「IP TOS」フィールドと比較するために使用されるTOS ビット値のビット位置を指定します。例えば、ビット7（ビット7 は非常に重要です。）と5 を設定したIP TOS 値をチェックし、ビット1 をクリアするためには、TOS ビット値「0xA0」とTOS Mask「0xFF」を使用します。

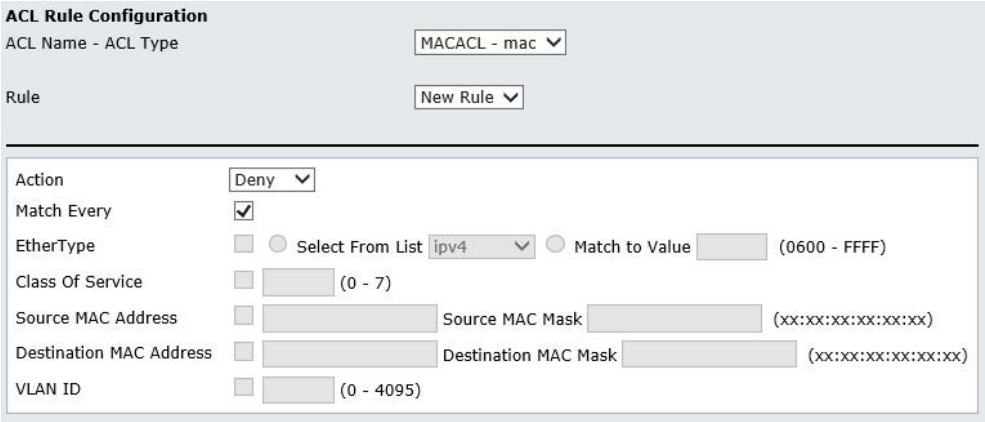
● IPv6アクセスコントロールリスト



◆ **ACL Name - ACL Type**	設定を行うACL名を選択します。
◆ **Rule**	ACLに適用するルールを選択、または[New Rule]を選択して新しいルールを設定します。 ACL 内の複数のルールは、ACL に追加した順番でパケットに適用されます。最終ルールとして、「implicit deny all rule」(暗黙の全否定) があります。
◆ **Action**	ACLルールのアクションを選択します。 • [Permit] アクセスポイントへの送受信の基準に一致するトラフィックはすべて許可されます。 基準に一致しないトラフィックはすべて廃棄されます。 • [Deny] アクセスポイントへの送受信の基準に一致するトラフィックをすべて拒否します。 基準に一致しないトラフィックはすべて送信されますが、最終ルールの場合は異なります。 各ACLの最後には「implicit deny all rule」(暗黙の全否定)という最終ルールがあり、明らかに許可されたトラフィック以外は廃棄されます。
◆ **Match Every**	許可または拒否いずれかのアクションを持つルールを、パケットのコンテンツに関わらず一致させるよう指示します。選択すると、照合基準を追加設定することはできません。 新規のルールには初期値で「Match Every」オプションが選択されています。他の基準を設定する場合は本オプションのチェックを外してください。
◆ **Protocol**	プロトコルを選択します。 • [Select From List]: 以下からプロトコルを選択します。 - [IP][ICMP][IPv6][ICMPv6][IGMP][TCP][UDP] • [Match to Value]:名称でリストアップされないプロトコルに一致させる場合に、プロトコル ID を入力します。プロトコルID は、IANA によって割り当てられたプロトコル番号です。(設定可能範囲:0-255)
◆ **Source IPv6 Address**	送信元IPv6 アドレスを設定します。
◆ **Source IPv6 Prefix Len**	送信元IPv6 アドレスのプリフィクス長を入力します。
◆ **Source Port**	送信元ポートを設定します。送信元ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信元ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信元ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023: 通常のポート - 1024-1518: 登録されたポート - 49152-65535: ダイナミックおよび/ またはプライベートポート

◆ **Destination IPv6 Address**	送信先IPv6アドレスを設定します。
◆ **Destination IPv6 Prefix Len**	送信先IPv6 アドレスのプリフィクス長を入力します。
◆ **Destination Port**	送信先ポートを設定します。送信先ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信先ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信先ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび/ またはプライベートポート
◆ **IPv6 Flow Label**	IPv6フローラベルを設定します フローラベルはIPv6 パケットにとって固有の20 ビットの番号です。ルータ内のQoS に対応するエンドステーションによって使用されます。
◆ **IPv6 DSCP**	IPv6 DSCP値を設定します。 • [Select From List]: DSCP の種類を選択します。 • [Match to Value]: DSCP 値を入力します。

● MACアクセスコントロールリスト



◆ **ACL Name - ACL Type**	設定を行うACL名を選択します。
◆ **Rule**	ACLに適用するルールを選択、または[New Rule]を選択して新しいルールを設定します。 ACL 内の複数のルールは、ACL に追加した順番でパケットに適用されます。最終ルールとして、「implicit deny all rule」(暗黙の全否定) があります。
◆ **Action**	ACLルールのアクションを選択します。 • [Permit] アクセスポイントへの送受信の基準に一致するトラフィックはすべて許可されます。 基準に一致しないトラフィックはすべて廃棄されます。 • [Deny] アクセスポイントへの送受信の基準に一致するトラフィックをすべて拒否します。 基準に一致しないトラフィックはすべて送信されますが、最終ルールの場合は異なります。 各ACLの最後には「implicit deny all rule」(暗黙の全否定)という最終ルールがあり、明らかに許可されたトラフィック以外は廃棄されます。
◆ **Match Every**	許可または拒否いずれかのアクションを持つルールを、パケットのコンテンツに関わらず一致させるよう指示します。選択すると、照合基準を追加設定することはできません。 新規のルールには初期値で「Match Every」オプションが選択されています。他の基準を設定する場合は本オプションのチェックを外してください。
◆ **Ether Type**	Ether Typeを設定します。 • [Select From List]: 以下からプロトコルのタイプを選択します。 - [ipv4][appletalk][arp][ipv6][ipx] [netbios][pppoe] • [Match to Value]: パケットに一致するカスタムプロトコルを16 進数の4 文字で入力します。 （入力可能範囲：0600 – FFFF）

◆ **Class of Service**	CoS 802.1p ユーザ優先度の値を入力します。
◆ **Source MAC Address**	送信元MAC アドレスを入力します。
◆ **Source MAC Mask**	送信元MAC アドレスマスクを入力します。
◆ **Destication MAC Address**	送信先MACアドレスを入力します。
◆ **Destication MAC Mask**	送信先MAC アドレスマスクを入力します。
◆ **VLAN ID**	VLAN ID を入力します。(入力可能範囲:0-4095)

Class Map（Diffservクラスマップの作成）

[Client QoS] > [Class Map]

Diffservクラスマップの作成を行います。

クライアントQoS はDifferentiated Services (DiffServ) をサポートしています。
DiffServ は、パケットを様々な要素で分類し、グループごとに優先制御を定義し、その定義に従ってパケットの転送を実施する機能です。

トラフィックを分類し、トラフィッククラスを処理する方法を定義するポリシーを作成することによって、音声などのトラフィックに他のトラフィックより高い優先度を与えることができます。

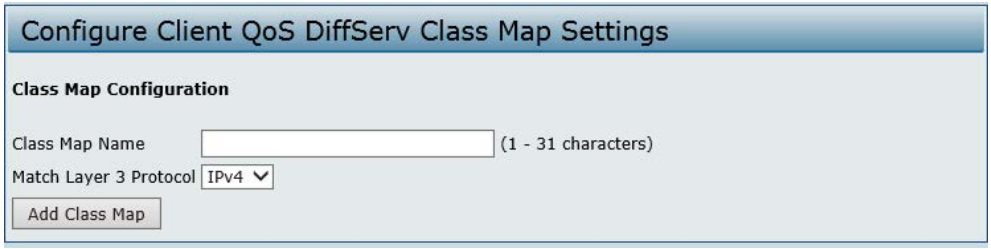
● Diffserv クラスマップの定義
クライアントQoS にDiffServ を使用するためには、[Class Map]と[Policy Map]画面を使用して以下のカテゴリと基準を定義します。

- クラス: クラスを作成し、クラスの基準を定義します。
- ポリシー: ポリシーを作成し、ポリシーにクラスを関連付けてポリシーのステートメントを定義します。

クラスを定義して、ポリシーに関連付けたら、[Client QoS] > [VAP QoS Parameters]画面で指定したVAP にポリシーを適用します。
パケットは、定義した基準に基づいて分類され、処理されます。
分類の基準はクラスによって定義され、その処理はポリシーの属性によって定義されます。
ポリシーの属性はクラスごとにインスタンスベースで定義し、これらの属性は一致する場合に適用されます。ポリシーには、複数のクラスを含めることができます。ポリシーがアクティブな場合は、パケットがどのクラスに一致するかによって、アクションを行います。

■Diffservクラスマップの設定手順

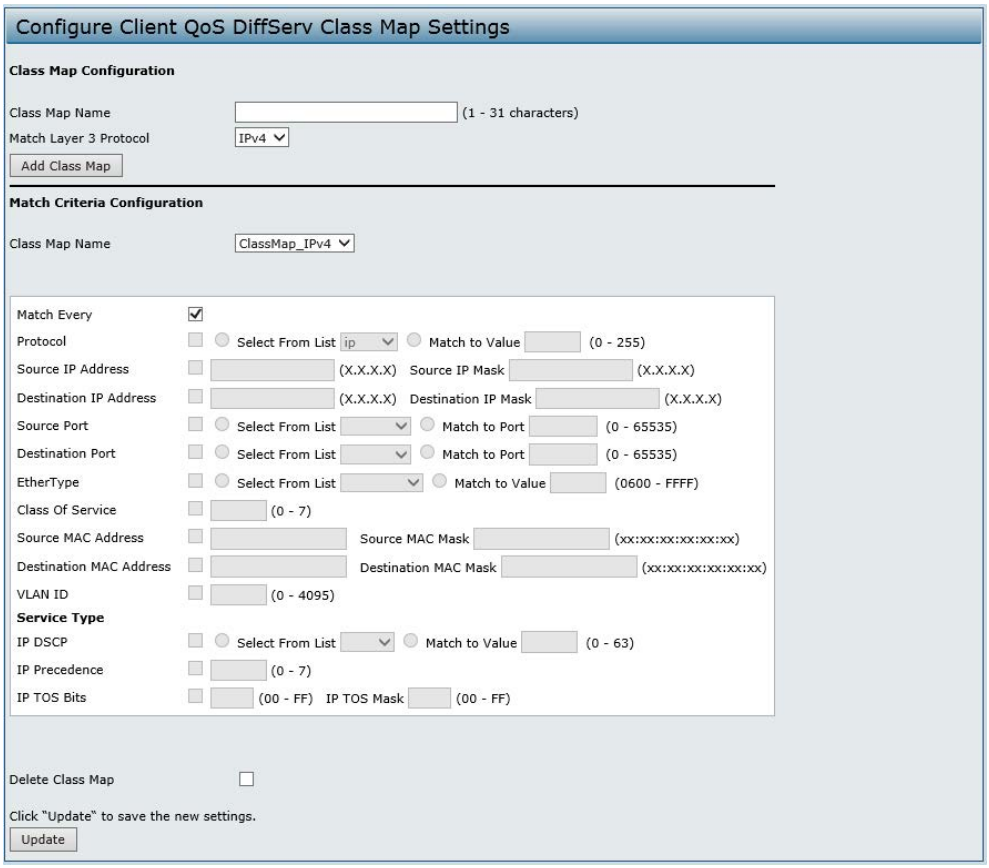
1. [Client QoS] > [Class Map] の順にメニューをクリックし、以下の画面を表示します。



2. [Class Map Name] にクラスマップ名を入力→ [Match Layer 3 Protocol] でプロトコルを指定します。

3. [Add Class Map] をクリックします。

4. [Class Map Name] で設定するクラスマップを選択→ [Match Criteria Configuration] 欄で ACL ルールの内容を設定します。



重要

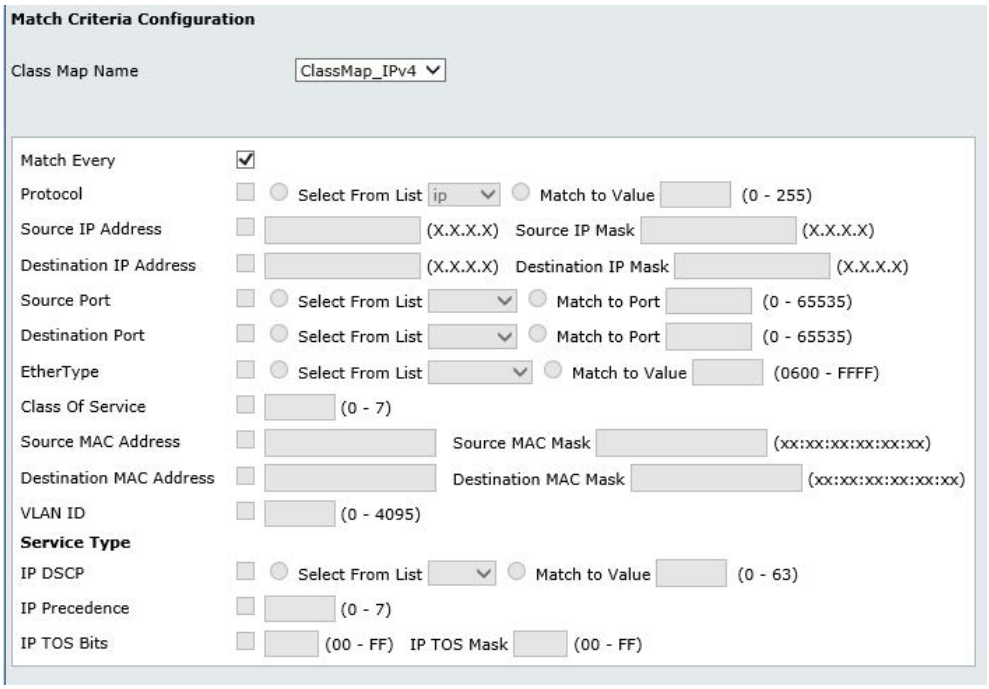
- [Match Criteria Configuration]欄の内容は選択したクラスマップによって異なります。
  詳細は『クラスマップの設定内容：p.105 』を参照してください。
- [Delete Class Map]にチェックをいれて[Update]をクリックすると、クラスマップを削除できます。

5. [Update] をクリックし、設定を適用します。

■クラスマップの設定内容

クラスマップのプロトコル（IPv4またはIPv6）によって、設定内容が異なります。

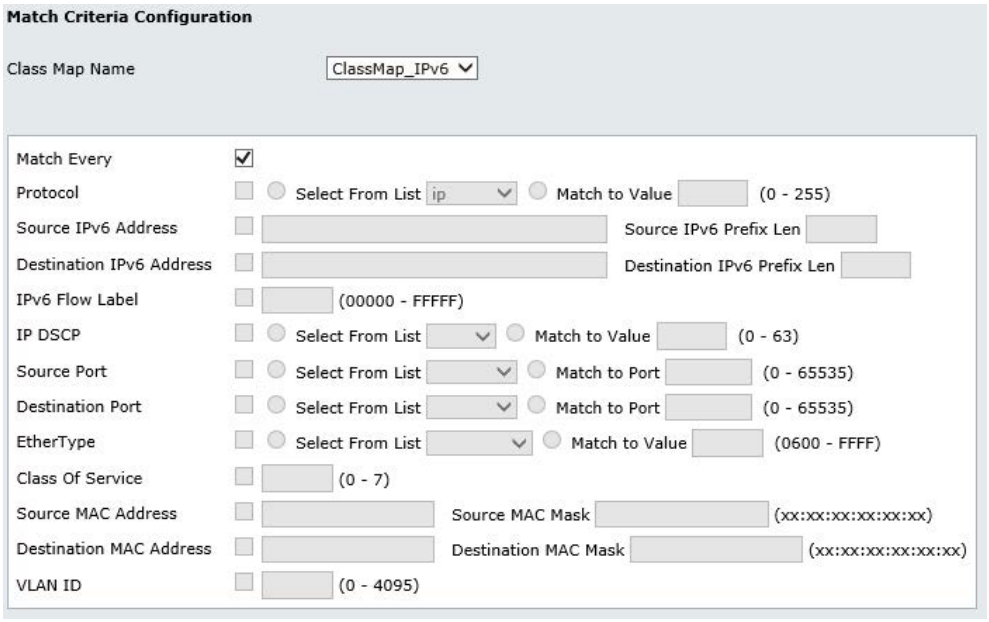
● IPv4クラスマップ



◆ **Class Map Name**	設定を行うクラスマップ名を選択します。
◆ **Match Every**	照合条件がL3パケットのすべてのパラメータと一致するよう設定します。
◆ **Protocol**	プロトコルを選択します。 ・[Select From List]: 以下からプロトコルを選択します。 - [IP][ICMP][IGMP][TCP][UDP] ・[Match to Value]:名称でリストアップされないプロトコルに一致させる場合に、プロトコルID を入力します。プロトコルID は、IANA によって割り当てられたプロトコル番号です。 （設定可能範囲：0-255）
◆ **Source IP Address**	送信元IP アドレスを設定します。
◆ **Source IP Mask**	送信元IP アドレスのマスクを設定します。 DiffServ のマスクは、パケットコンテンツとの照合に使用する送信先IP アドレスの部分を指定する「.」（ドット）で区切った10 進数形式のネットワーク型ビットマスクです。「255.255.255.255」の DiffServ マスクは、すべてのビットが重要で、「0.0.0.0」のマスクは、どのビットも重要でないことを示します。逆の場合はACL ワイルドカードマスクに一致します。例えば、シングルホストアドレスに基準を一致させる場合は、「255.255.255.255」マスクを使用します。24 ビットのサブネット（例:192.168.10.0/24）に基準を一致させる時は、「255.255.255.0」のマスクを使用します。
◆ **Destination IP Address**	送信先IP アドレスを設定します。
◆ **Destination IP Mask**	送信先IP アドレスマスクを入力します。 DiffServ のマスクは、パケットコンテンツとの照合に使用する送信先IP アドレスの部分を指定する「.」（ドット）で区切った10 進数形式のネットワーク型ビットマスクです。「255.255.255.255」のDiffServ マスクは、すべてのビットが重要で、「0.0.0.0」のマスクは、どのビットも重要でないことを示します。 逆の場合はACL ワイルドカードマスクに一致します。例えば、シングルホストアドレスに基準を一致させる場合は、「255.255.255.255」マスクを使用します。24 ビットのサブネット（例:192.168.10.0/24）に基準を一致させる時は「255.255.255.0」のマスクを使用します。

◆ **Source Port**	送信元ポートを設定します。送信元ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信元ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信元ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび/ またはプライベートポート
◆ **Destination Port**	送信先ポートを設定します。送信先ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信先ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信先ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび/ またはプライベートポート
◆ **Ether Type**	Ether Typeを設定します。 • [Select From List]: 以下からプロトコルのタイプを選択します。 - [ipv4][appletalk][arp][ipv6][ipx] [netbios][pppoe] • [Match to Value]: パケットに一致するカスタムプロトコルを16 進数の4 文字で入力します。（入力可能範囲：0600 – FFFF）
◆ **Class Of Service**	CoS 802.1p ユーザ優先度の値を入力します。
◆ **Source MAC Address**	送信元MAC アドレスを入力します。
◆ **Source MAC Mask**	送信元MAC アドレスマスクを入力します。
◆ **Destication MAC Address**	送信先MACアドレスを入力します。
◆ **Destication MAC Mask**	送信先MAC アドレスマスクを入力します。
◆ **VLAN ID**	VLAN ID を入力します。（入力可能範囲：0-4095）

● IPv6クラスマップ



◆ **Class Map Name**	設定を行うクラスマップ名を選択します。
◆ **Match Every**	照合条件がL3パケットのすべてのパラメータと一致するよう設定します。
◆ **Protocol**	プロトコルを選択します。 • [Select From List]: 以下からプロトコルを選択します。 - [IP][ICMP][IPv6][ICMPv6][IGMP][TCP][UDP] • [Match to Value]:名称でリストアップされないプロトコルに一致させる場合に、プロトコルID を入力します。プロトコルID は、IANA によって割り当てられたプロトコル番号です。(設定可能範囲:0-255)
◆ **Source IPv6 Address**	送信元IPv6 アドレスを設定します。
◆ **Source IPv6 Prefix Len**	送信元IPv6 アドレスのプリフィクス長を入力します。
◆ **Destination IPv6 Address**	送信先IPv6アドレスを設定します。
◆ **Destination IPv6 Prefix Len**	送信先IPv6 アドレスのプリフィクス長を入力します。
◆ **IPv6 Flow Label**	IPv6フローラベルを設定します フローラベルはIPv6 パケットにとって固有の20 ビットの番号です。ルータ内のQoS に対応するエンドステーションによって使用されます。
◆ **IPv6 DSCP**	IPv6 DSCP値を設定します。 • [Select From List]: DSCP の種類を選択します。 • [Match to Value]: DSCP 値を入力します。
◆ **Source Port**	送信元ポートを設定します。送信元ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信元ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信元ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023: 通常のポート - 1024-1518: 登録されたポート - 49152-65535: ダイナミックおよび/ またはプライベートポート

◆ **Destination Port**	送信先ポートを設定します。送信先ポートはデータグラムヘッダで識別されます。ポート名を指定するか、またはポート番号を入力します。 • [Select From List]: 以下から送信先ポートに関連するキーワードを選択します。 各キーワードは相当するポート番号に変換されます。 - [ftp][ftpdata][http][smtp][snmp][telnet][tftp][www] • [Match to Port]: データグラムヘッダで識別される送信先ポートに一致させるIANA ポート番号を入力します。ポート範囲は0-65535 で、以下の3 つの異なるポートタイプを含みます。 - 0-1023：通常のポート - 1024-1518：登録されたポート - 49152-65535：ダイナミックおよび/ またはプライベートポート
◆ **Ether Type**	Ether Typeを設定します。 • [Select From List]: 以下からプロトコルのタイプを選択します。 - [ipv4][appletalk][arp][ipv6][ipx] [netbios][pppoe] • [Match to Value]: パケットに一致するカスタムプロトコルを16 進数の4 文字で入力します。（入力可能範囲：0600 – FFFF）
◆ **Class Of Service**	CoS 802.1p ユーザ優先度の値を入力します。
◆ **Source MAC Address**	送信元MAC アドレスを入力します。
◆ **Source MAC Mask**	送信元MAC アドレスマスクを入力します。
◆ **Destication MAC Address**	送信先MACアドレスを入力します。
◆ **Destication MAC Mask**	送信先MAC アドレスマスクを入力します。
◆ **IP DSCP**	IP DSCP値を設定します。 • [Select From List]: DSCP タイプを選択します。 • [Match to Value]:照合するDSCP 値 (0-63) を入力します。
◆ **IP Precedence**	IP Precedence値を設定します。 IP Precedence値によってIPパケットの優先度が決定されます。値は高い値ほど優先度が高くなります。
◆ **IP TOS Bits**	一致基準として使用するパケットのIP ヘッダのサービスタイプのビット値を入力します。TOS ビット値の範囲は00-FF です。上位3 ビットはIP 優先度値を表します。上位6 ビットはIP Differentiated Services Code Point (DSCP) 値を表します。
◆ **IP TOS Mask**	IP TOS マスク値を入力し、パケットのヘッダ内にあり、本ルールで入力したTOS と照合されるTOS フィールドとのブーリアン型論理和を実行します。パケットのIP ヘッダ内のTOS フィールドからの指定されたビット (Precedence/Type of Service) を本ルールで入力したTOS と比較するためにTOS マスクを使用することができます。(00-FF)。

Policy Map（Diffservポリシーマップの作成）

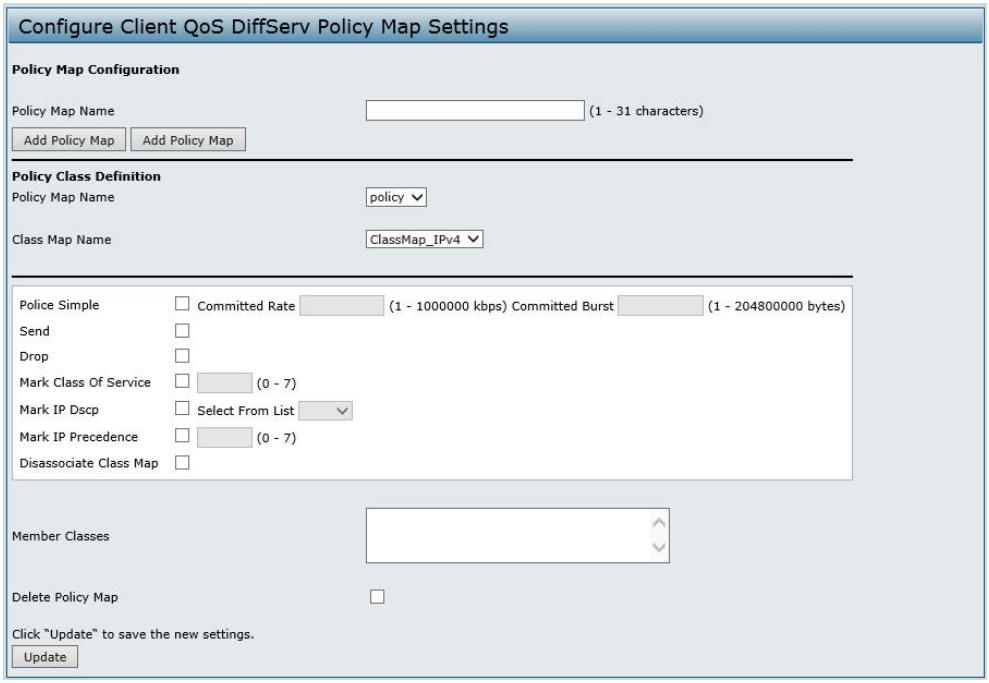
[Client QoS] > [Policy Map]

Diffservポリシーマップの作成を行います。

■Diffservポリシーマップの設定手順

1. [Client QoS] > [Class Map] の順にメニューをクリックし、以下の画面を表示します。

2. [Policy Map Name] にポリシーマップ名を入力します。
3. [Add Policy Map] をクリックします。
4. 以下の画面でポリシーの設定を行います。



重要

・[Delete Policy Map]にチェックをいれて[Update]をクリックすると、ポリシーマップを削除できます。

5. [Update] をクリックし、設定を適用します。

■ポリシーマップの設定内容

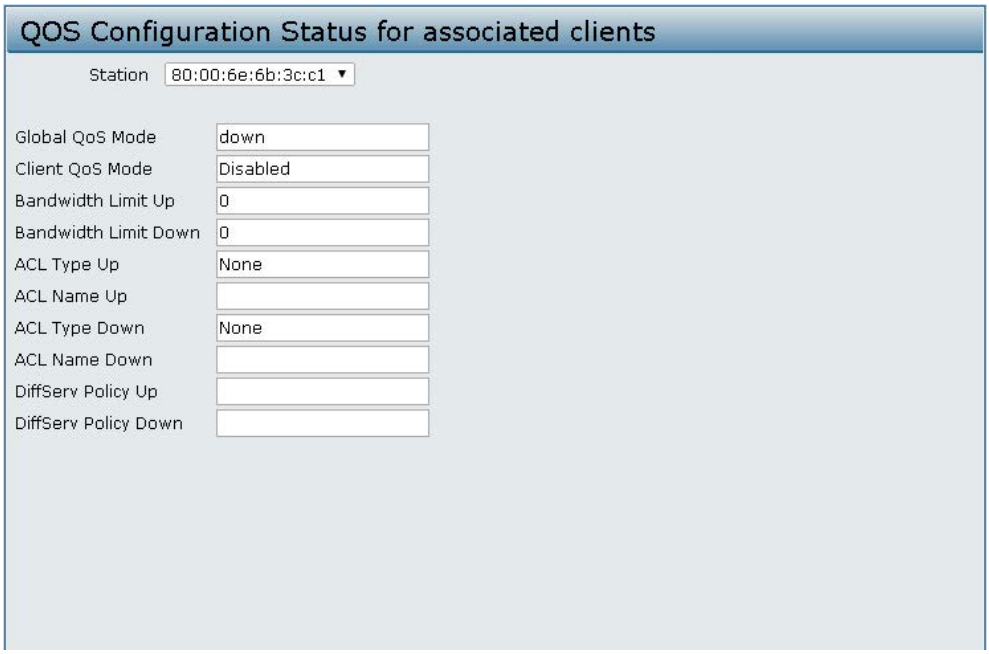
[Policy Class Definition]の設定内容について説明します。

◆ **Policy Map Name**	設定を行うポリシーマップ名を選択します。
◆ **Class Map Name**	設定を行うクラスマップ名を選択します。
◆ **Police Simple**	クラスにトラフィックポリシングスタイルを設定します。 シングルデータレートとバーストサイズを使用し、適合と違反の2 つの結果がもたらされます。 • [Committed Rate]: トラフィックが適合する必要のあるレート（単位:Kbps）を入力します。 • [Committed Burst]:トラフィックが適合する必要のあるバーストサイズ（単位: bytes）を入力します。
◆ **Send**	クラスマップ基準が満たされる場合に、関連トラフィックストリームのすべてのパケットが転送されることを指定します。
◆ **Drop**	ラスマップ基準が満たされる場合に関連トラフィックストリームのすべてのパケットが破棄されることを指定します。
◆ **Mark Class Of Service**	802.1p ヘッダの優先度フィールドに指定したサービスクラスに関連するトラフィックストリームに対するパケットのすべてにマークを付けます。パケットがまだこのヘッダを持っていない場合、1 つ挿入されます。CoS値は0-7 の整数です。
◆ **Mark IP Dscp**	リストから選択した、または入力したIP DSCP 値に関連するトラフィックストリームに対するパケットのすべてをマークします。 • [Select From List]: DSCP タイプを選択します。
◆ **Mark IP Precedence**	指定したIP Precedence 値に関連するトラフィックストリームに対するパケットのすべてをマークします。IP Precedence 値は0-7 の整数です。
◆ **Disassociate Class Map**	本オプションを選択し、[Apply]ボタンをクリックして[Policy Map Name]で選択したポリシーから[Class Map Name]で選択したクラスを削除します。
◆ **Member Classes**	現在定義されているすべてのDiffServ クラスを選択されたポリシーのメンバとして表示します。ポリシーと関連するクラスがない場合、本欄は空白です。
◆ **Delete Policy Map**	[Policy Map Name]で選択したポリシーマップを削除します。

Client Configuration（クライアント設定）

[Client QoS] > [Client Configuration]

アクセスポイントに接続しているクライアントのQoS 設定を表示します。



◆ **Station**	アクセスポイントに接続しているステーションを選択できます。
◆ **Global QoS Mode**	QoS モードが有効または無効であるかが表示されます。
◆ **Client QoS Mode**	クライアントのQoS モードが有効または無効であるかを表示します。
◆ **Bandwidth Limit Up**	クライアントがアクセスポイントからトラフィックを受信する最大レート（bps）を表示します。
◆ **Bandwidth Limit Down**	クライアントがアクセスポイントにトラフィックを送信する最大レート（bps）を表示します。
◆ **ACL Type Up**	インバウンドトラフィックに適用されるACL のタイプが表示されます。
◆ **ACL Name Up**	インバウンドトラフィックに適用されるACL の名称が表示されます。
◆ **ACL Type Down**	アウトバウンドトラフィックに適用されるACL のタイプが表示されます。
◆ **ACL Name Down**	アウトバウンドトラフィックに適用されるACL の名称が表示されます。
◆ **DiffServ Policy Up**	インバウンドトラフィックに適用されるDiffServポリシーの名称が表示されます。
◆ **DiffServ Policy Down**	アウトバウンドトラフィックに適用されるDiffServポリシーの名称が表示されます。

メモ

・QoS モードをクライアントに対して有効にするためには、アクセスポイントのQoS モードを有効にし、クライアントが接続するVAP でも有効にします。
[Client QoS] > [VAP QoS Parameters] を使用し、[Client QoS Global Admin Mode]とVAP ごとの[Client QoS Mode]を有効にします。

付録 10

設定例

本製品で利用可能ないくつかの機能を設定する方法について説明します。
設定方法はWeb GUIを使用した場合とCLIを使用した場合の両方を記載します。

◎ VAP の設定

◎ 無線設定

◎ WDS の設定

◎ アクセスポイントのクラスタリング設定

◎ クライアントQoS の設定

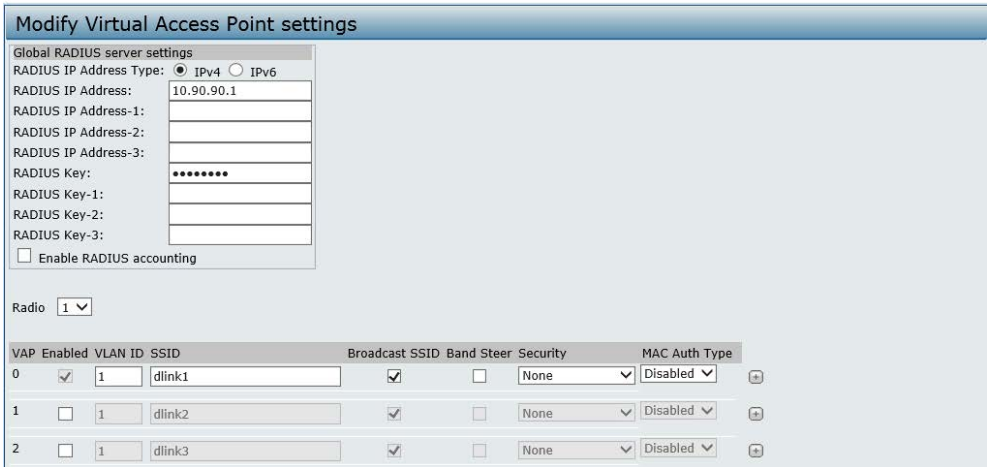
■VAPの設定

VAP 1 の設定を以下のとおりに設定します。

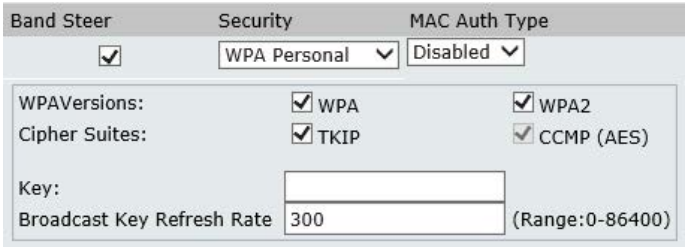
- VLAN ID : 2
- SSID : Marketing
- Security : WPA Personal using WPA2 with CCMP (AES)

● Web GUIからのVAP設定

1. [Manage] > [VAP] の順にメニューをクリックします。



2. VAP 1 の [Enabled] 欄のチェックボックスをチェックします。
3. [VLAN ID] 欄に [2] を入力します。
4. [SSID] 欄で既存の SSID を削除して [Marketing] と入力します。
5. [Security] 欄のプルダウンメニューから [WPA Personal] を選択します。
   以下の画面が表示されます。



6. [WPA2] と [CCMP（AES）] のチェックボックスをチェックし、[WPA] と [TKIP] のチェックを外します。
7. [Key] 欄に WPA 暗号キーを入力します。
   暗号キーには、半角英数字および記号を使用することができます。
   暗号キーは、大文字小文字を区別し、8 ～ 63 文字です。
8. [Update] をクリックし、設定を適用します。

● CLIからのVAP設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。
2. VAP 1 を有効にします。

```
set vap vap1 status up
```

3. VLAN ID を [2] に設定します。

```
set vap vap1 vlan-id 2
```

上記のコマンドでは、両方の無線デバイスの [VAP 1] の [VLAN ID] を [2] に設定します。Radio 1 における [VAP 1] の [VLAN ID] だけを設定する場合は、次のコマンドを使用します。

```
set vap 1 with radio wlan0 to vlan-id 2
```

4. SSID を [Marketing] に設定します。

```
set interface wlan0vap1 ssid Marketing
```

5. セキュリティモードを [WPA Personal] に設定します。

```
set interface wlan0vap1 security wpa-personal
```

6. 本製品への接続を WPA2 クライアントに許可し、WPA クライアントを拒否します。

```
set bss wlan0bssvap1 wpa-allowed off
set bss wlan0bssvap1 wpa2-allowed on
```

7. Cipher Suite（暗号スイート）を [CCMP（AES）] のみに設定します。

```
set bss wlan0bssvap1 wpa-cipher-tkip off
set bss wlan0bssvap1 wpa-cipher-ccmp on
```

8. 事前共有鍵を設定します。

```
set interface wlan0vap1 wpa-personal-key JuPXkC7GvY$moQiUttp2
```

事前共有鍵にスペースが含まれている場合は、キーの前後に ["] を入力します。

9. 次のコマンドを使用して設定の参照と確認を行います。

```
get interface wlan0vap1 detail
```

```
get vap vap1 detail
```

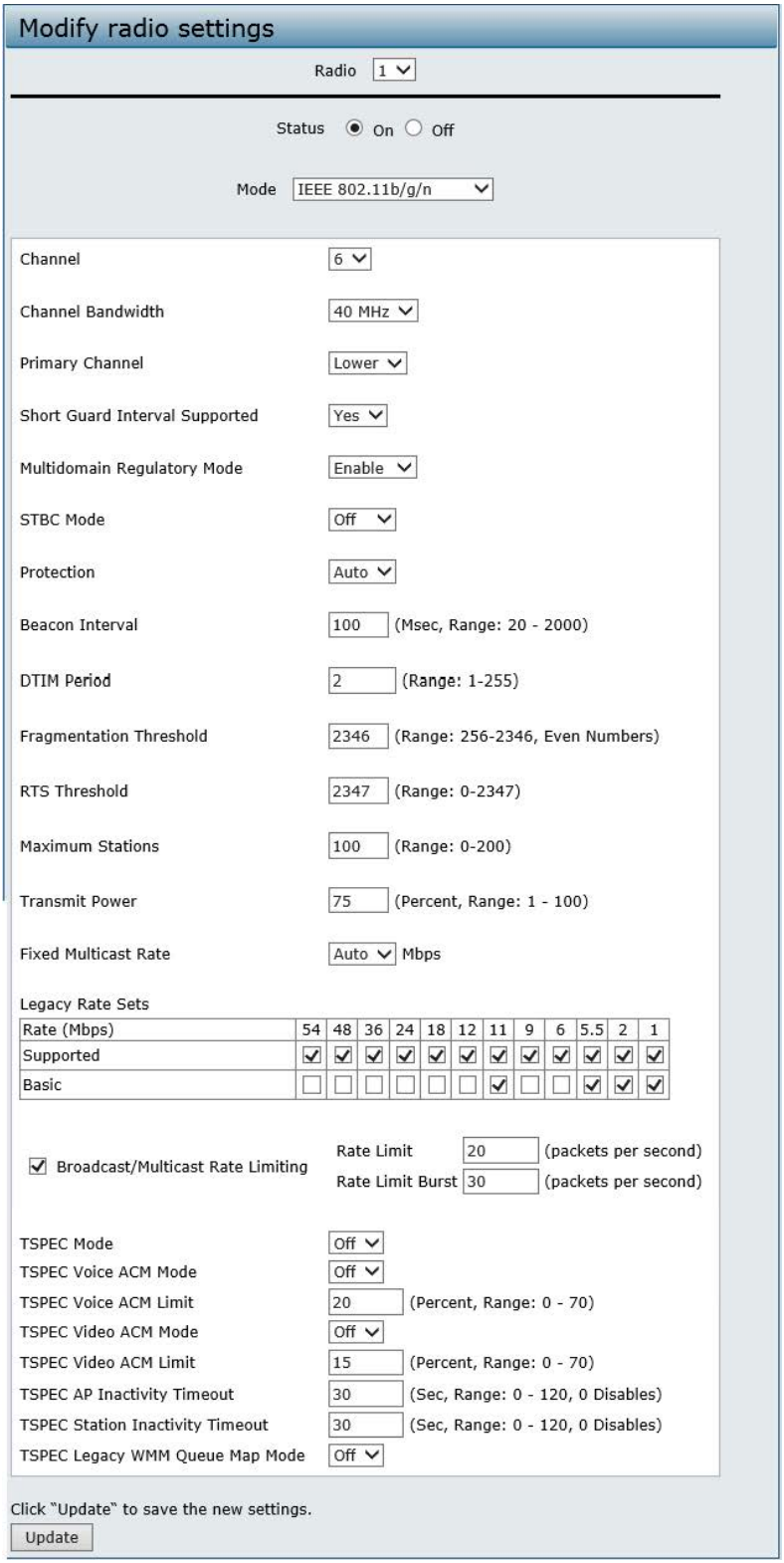
■無線インタフェースの設定

Radio 1 を以下のとおりに設定します。

- モード - IEEE 802.11b/g/n
- チャンネル - 6
- チャンネル帯域幅 - 40MHz
- 最小ステーション - 100
- 送信電力 - 75%

● Web GUIからの無線インタフェース設定

1. [Manage] > [Radio] の順にメニューをクリックします。



2. 番号 [1] が [Radio] 欄に表示され、ステータスが [On] であることを確認します。
3. [Mode] メニューから [IEEE 802.11b/g/n] を選択します。
4. [Channel] 欄から [6] を選択します。
5. [Channel Bandwidth] 欄から [40MHz] を選択します。
6. [Maximum Station] 欄の値を [100] に変更します。
7. [Transmit Power] 欄の値を [75] に変更します。
8. [Update] をクリックし、設定を適用します。

● CLIからの無線インタフェース設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。
2. ステータスが現在 up でない場合、Radio 1 を有効にします。

```
set radio wlan0 status up
```

3. モードを IEEE 802.11a/n に設定します。

```
set radio wlan0 mode bg-n
```

4. チャンネルを 36 に設定します。

```
set radio wlan0 channel-policy static
set radio wlan0 static-channel 6
```

5. チャンネル帯域幅を 40MHz に設定します。

```
set radio wlan0 n-bandwidth 40
```

6. 一度に最大 100 個のステーションをアクセスポイントに接続させます。

```
set radio wlan0 max-stations 100
```

7. 送信電力を 75% に設定します。

```
set radio wlan0 tx-power 75
```

8. 無線設定に関する情報を参照します。

```
get radio wlan0 detail
```

■WDSの設定

2 つのアクセスポイント間にWDS リンクを設定する方法について説明します。
ローカルなアクセスポイントは[MyAP1]で、リモートアクセスポイントは[MyAP2]とします。
WDS リンクには、以下の設定があり、両方のアクセスポイントに設定される必要があります。

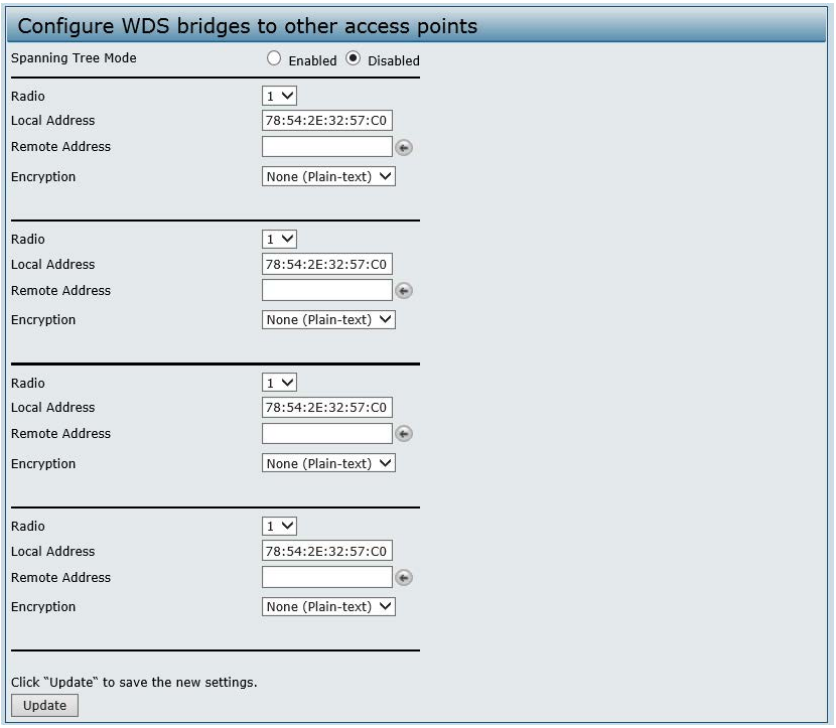
- 暗号化 - WPA(PSK)
- SSID - wds-link
- Key - abcdefghijk

重要

- 異機種間、異なるファームウェアバージョン間でWDS モードを使用することはできません。

● Web GUIからのWDS設定

1. MyAP1 にログインし、[Manage] > [WDS] の順にメニューをクリックします。



2. [Remote Address] 欄に MyAp2 の MAC アドレスを入力するか、欄の横にある矢印をクリックして表示されるメニューから MyAp2 の MAC アドレスを選択します。

3. [Encryption] メニューから [WPA(PSK)] を選択します。

   [Radio 1]におけるVAP0 がWPA (PSK) を使用する場合にだけ、WPA(PSK) オプションはセキュリティ方式として利用可能です。VAP0 がWPA Personal または WPA Enterprise に設定されない場合、None (Plain-text) またはWDS link encryption のどちらかを選択する必要があります。

4. [SSID] に [wds-link]、[Key] に [abcdefghijk] と入力します。

5. [Update] をクリックしてアクセスポイントに WDS 設定を適用します。

6. [MyAP2] にログインし、手順 1-5 を繰り返します。

   ただし、[Remote Address]欄には[MyAP1]のMAC アドレスを使用することに注意します。
   MyAP1 とMyAP2 は同じIEEE 802.11 モードで、同じチャンネルで送信するように設定される必要があります。

● CLIからのWDS設定

1. Telnet、SSH、またはシリアル接続を使用して「MyAP1」に接続します。
2. 「MyAP2」のリモート MAC アドレスを設定します。

```
set interface wlan0wds0 status up remote-mac 00:30:AB:00:00:B0
```

3. リンクの暗号化タイプとして「WPA(PSK)」を設定します。

```
set interface wlan0wds0 wds-security-policy wpa-personal
```

4. WDS リンクにおける SSID を設定します。

```
set interface wlan0wds0 wds-ssid wds-link
```

5. 暗号化キーを設定します。

```
set interface wlan0wds0 wds-wpa-psk-key abcdefghijk
```

6. WDS リンクを管理上有効にします。

```
set interface wlan0wds0 status up
```

7. 同じ設定手順を MyAP2 にも実行します。

■アクセスポイントのクラスタリング設定

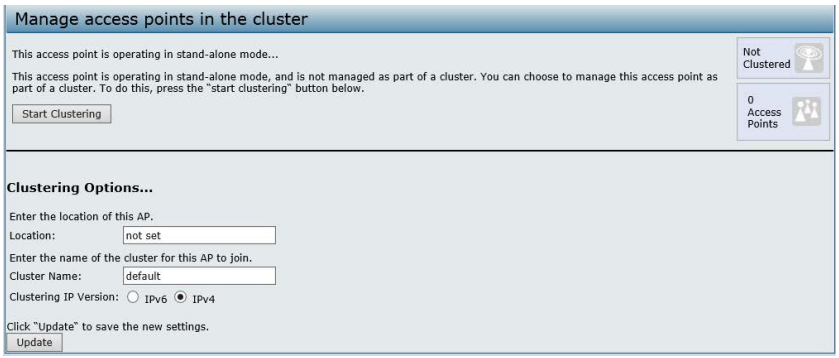
アクセスポイント間にクラスタを設定し、自動チャンネル再割り当てを有効にする方法を示しています。ローカルなアクセスポイントのロケーションは「Room214」で、クラスタ名は「MyCluster」であるものとします。

重要

APクラスタ機能は、同一機種間、同一ファームウェアバージョン間のみサポートされます。

● Web GUIからのクラスタリング設定

1. [Cluster] > [Access Points] の順にメニューをクリックします。



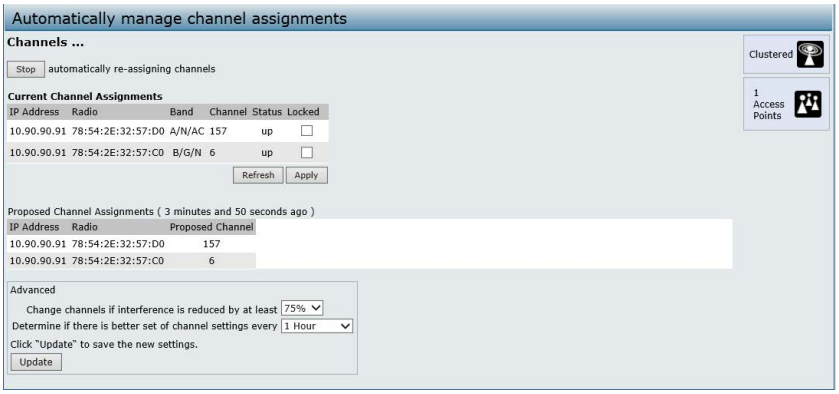
2. [Location] にアクセスポイントが接続するロケーション、[Cluster Name] に参加するクラスタの名称を入力します。

3. [Update] をクリックして設定を適用します。

画面の更新後、同じブリッジセグメントにあり、同じ操作モードの無線帯域を持ち、クラスタリングが有効で、同じクラスタ名を持つ他のアクセスポイントがアクセスポイントテーブルに表示されます。

4. [Channel Management] 画面を表示してチャンネル割り当てを参照します。

現在のチャンネル割り当てと提案されたチャンネル割り当てを表示します。「Advanced」セクションの間隔設定では、提案された変更を適用する間隔を決定します。



● CLIからのクラスタリング設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。
2. アクセスポイントのロケーションを設定します。

```
set cluster location "Room 214"
```

クラスタ名かクラスタロケーションがスペースを持つ場合、CLI でテキストを入力する際に「"」マークでテキストを囲む必要があります。Web GUI を使用してテキストを入力する場合には、「"」マークを使用する必要はありません。

3. クラスタ名を設定します。

```
set cluster cluster-name MyCluster
```

4. クラスタリングを開始します。

```
set cluster clustered 1
```

5. アクセスポイントのクラスタリング設定に関する情報を参照します。

```
DLINK-WLAN-AP# get cluster detail
Property            Value
------------------------------------------
clustered           1
location            Room 214
cluster-name        MyCluster
ipversion           ipv4
member-count        1
clustering-allowed  true
compat              BROADCOM_V02_bcm953012er

operational-mode    1
```

6. 自動チャンネルプランを開始します。

```
set channel-planner status up
```

7. 自動チャンネルプランの設定を参照します。

```
DLINK-WLAN-AP# get channel-planner detail
Property          Value
----------------------
status            up
change-threshold  75
interval          60
locked-ips
DLINK-WLAN-AP#
```

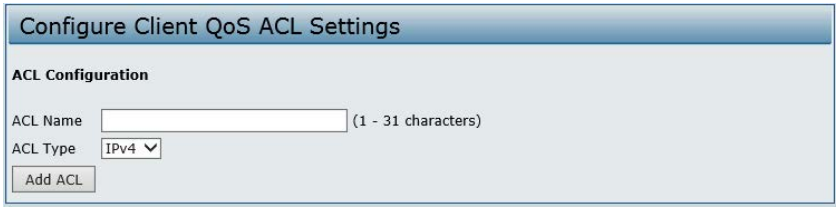
■クライアントQoS の設定

この例ではクライアントQoS を有効にする方法、アクセスポイントにACL とDiffServ ポリシーを設定する方法、VAP0 に接続するクライアントから送信されるトラフィックおよびアクセスポイントが受信するトラフィックにACL とポリシーを適用する方法について示します。
IPv4 ACL は「acl1」という名称で、2 つのルールを含むものとします。最初のルールは、「192.168.1.0」サブネットからのHTTP トラフィックを許可します。2 番目のルールは管理ステーション「192.168.1.23」からの全IP トラフィックを許可します。他のすべてのトラフィックは、ACL リストの最後にある暗黙の「deny all」(すべて拒否) のルールで拒否されます。ACL は、アクセスポイントが接続するクライアントからトラフィックを受信する場合にパケットがチェックされるように、アクセスポイントの内向きインタフェースに適用されます。
この例のDiffServ ポリシーは、RADIUS サーバを通じてDiffServ ポリシー名を取得しないVAP に接続するクライアントに対して初期値で行うDiffServ の動作を示します。宛先アドレス (192.168.2.200) としてVoIP サーバを持つ「192.168.1.0」サブネットがクライアントから受信した音声トラフィック (UDP パケット) は、他のトラフィックより優先するように「EF」(完全優先転送) のIP DSCP 値でマークされます。

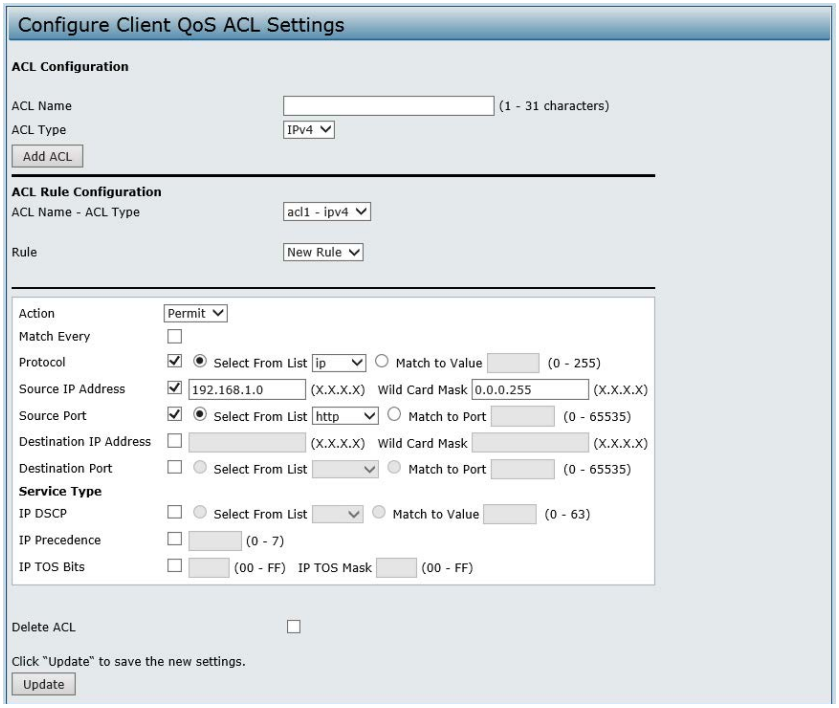
● Web GUIからのQoS設定

ACLの設定

1. [Client QoS] > [Client QoS ACL] の順にメニューをクリックします。



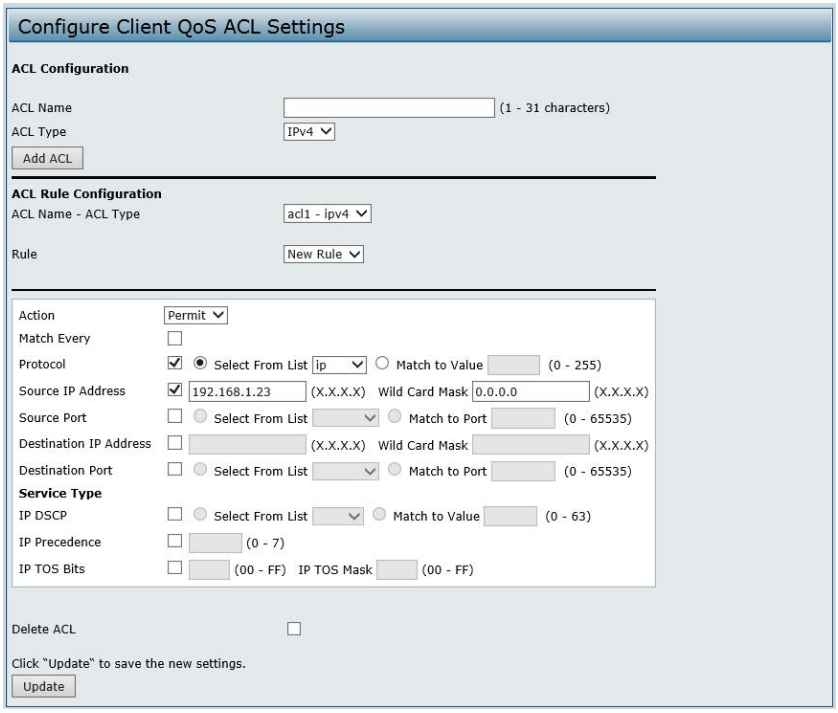
2. [ACL Name] に「acl1」を入力し、[Add ACL] をクリックします。
3. [Action] から [Permit] を選択します。
4. [Match Every] オプションをクリアします。
5. [Protocol] オプションを選択→ [Select From List] で [ip] を選択します。
6. 残りの設定を行います。



- Source IP Address : 192.168.1.0
- Wild Card Mask : 0.0.0.255
- Source Port : オプションを選択します。
- Select From List (Source Port) : http

7. [Update] をクリックしてルールを保存します。

8. [Rule] メニューから [New Rule] を選択し、以下の設定を持つ別のルールを作成します。



- Action : Permit
- Match Every : オプションをクリアします。
- Protocol - Select From List : ip
- Address : 192.168.1.23
- Wild Card Mask : 0.0.0.0

9. [Update] をクリックしてルールを保存します。

10. [Client QoS] > [VAP QoS Parameters] 画面を表示します。

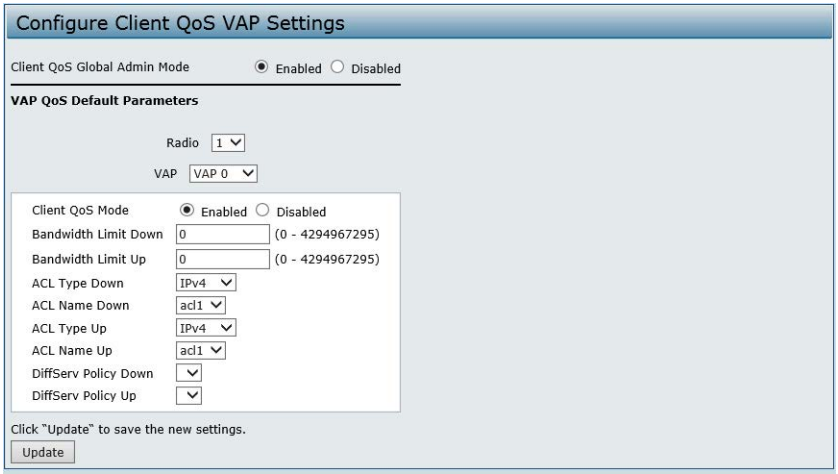
11. [Client QoS Global Admin Mode] で [Enabled] を選択します。

12. [VAP] で [VAP 0] を選択します。

13. [Client QoS Mode] で [Enabled] を選択します。

14. [ACL Type Up] で [IPv4] を選択します。

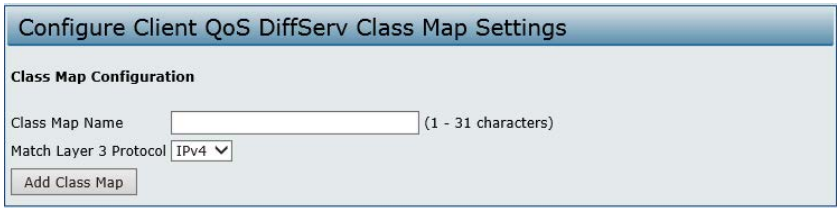
15. [ACL Name Up] で [acl1] を選択します。



16. [Update] をクリックして設定を適用します。

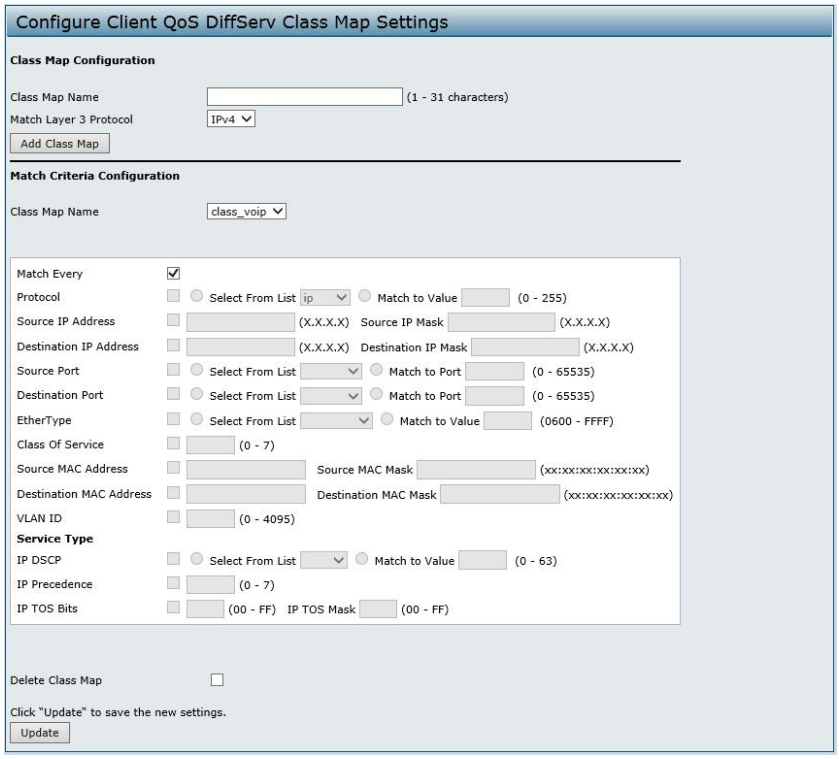
Diffserv 設定

1. [Client QoS] > [Class Map] の順にメニューをクリックします。



2. [Class Map Name] に「class_voip」を入力し、[Add Class Map] をクリックします。

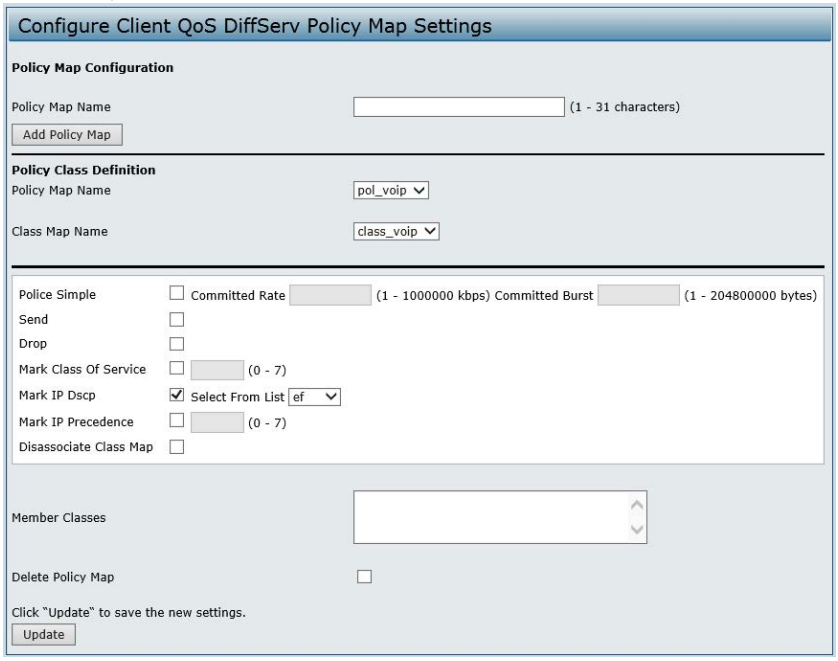
画面が更新され、以下の項目が表示されます。



3. [Match Every] オプションをクリアします。
4. [Protocol] オプションを選択→ [Select From List] で [udp] を選択します。
5. [Source IP Address] を選択し、以下の情報を入力します。
   - Address : 192.168.1.0
   - Source IP Mask : 255.255.255.0
6. [Destination IP Address] を選択し、以下の情報を入力します。
   - Address : 192.168.2.200
   - Destination IP Mask : 255.255.255.255
7. [Update] をクリックし、設定を保存します。
8. [Client QoS] > [Policy Map] の順にメニューをクリックします。

9. [Policy Map Name] に「pol_voip」を入力し、[Add Policy Map] をクリックします。

10. [Mark IP Dscp] を選択し、[Select From List] で [ef] を選択します。
「class_voip」クラスに定義された基準を満たすトラフィックは、EF (完全優先転送) のDSCP 値でマークされます。

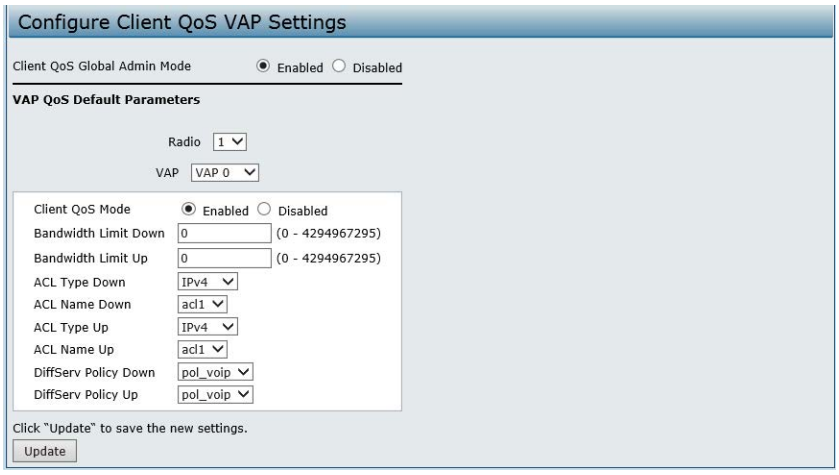


11. [Update] をクリックして設定を適用します。

12. [Client QoS] > [VAP QoS Parameters] の順にメニューをクリックします。

13. [VAP] で [VAP 0] を選択します。

14. [Client QoS Global Admin Mode] と [QoS Mode] が共に [Enabled]（有効）であることを確認し、以下の情報を入力します。



- ACL Type Down : IPv4
- ACL Name Down : acl1
- ACL Type Up : IPv4
- ACL Name Up : IPv4
- DiffServ Policy Down : pol_voip
- DiffServ Policy Up : pol_voip

15. [Update] をクリックして設定を適用します。

● CLIからのQoS設定

ACL設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。
2. 「acl1」という名称の ACL を作成します。

```
add acl acl1 acl-type ipv4
```

3. 「acl1」に 192.168.1.0 サブネットからの HTTP トラフィックを許可するルールを追加します。

```
add rule acl-name acl1 acl-type ipv4 action permit protocol ip src-ip 192.168.1.0
src-ip-mask 0.0.0.255 src-port http
```

4. 「acl1」に IP アドレス 192.168.1.23 を持つホストからの全トラフィックを許可する別のルールを追加します。

```
add rule acl-name acl1 acl-type ipv4 action permit protocol ip src-ip
192.168.1.23 src-ip-mask 0.0.0.0
```

5. アクセスポイントのクライアント QoS を有効にします。

```
set client-qos mode up
```

6. VAP0 に ACL のタイプを指定します。

```
set vap vap0 def-acltype-down ipv4
set vap vap0 def-acltype-up ipv4
```

7. 「acl1」を VAP0 のアクセスコントロールリストに適用します。

```
set vap vap0 def-acl-up acl1
set vap vap0 def-acl-down acl1
```

8. VAP0 でクライアント QoS を有効にします。

```
set vap vap0 qos-mode up
```

Diffserv 設定

1. Telnet、SSH、またはシリアル接続を使用してアクセスポイントに接続します。

2. 「class_voip」という名称のクラスマップを作成し、「192.168.2.200」（VoIP サーバ）の宛先 IP アドレスを持つ「192.168.1.0」ネットワークからのすべての UDP パケットに一致するように設定します。

```
add class-map class_voip l3-protocol ipv4 every yes protocol udp src-ip
192.168.1.0 src-ip-mask 255.255.255.0 dst-ip 192.168.2.200 dst-ip-mask
255.255.255.255
```

3. 「pol_voip」という名称のポリシーマップを追加します。

```
add policy-map pol_voip
```

4. 「class_voip」クラスマップを追加し、「class_voip」基準に一致するパケットを EF（完全優先転送) の DSCP 値でマークすることを指定することで「pol_voip」ポリシーマップを定義します。

```
add policy-attr policy-map-name pol_voip class-map-name class_voip mark-ip-dscp
ef police-simple no
```

5. pol_voip を VAP0 に適用します。

```
set vap vap0 def-policy-up pol_voip
set vap vap0 def-policy-down pol_voip
```

6. アクセスポイントのクライアント QoS を有効にします。

```
set vap vap0 qos-mode up
```

工場出荷時設定に戻す

本製品の設定を工場出荷時の状態に戻す方法について説明します。

■リセットボタンで設定リセット行う

1. 本体の電源をいれた状態で、本体側面のリセットボタンを 10 秒以上押します。

2. ボタンを離すと、本体が再起動します。そのままお待ちください。

■Web GUIから設定リセットを行う

1. Web GUI 上部にある管理メニューの [System] をクリックします。
2. [Reset] をクリックします。
3. 本体が再起動します。そのままお待ちください。