NEC

GVT-153324-001-00 1.24

QX-W1000/W1100 シリーズ アクセスポイント

Anchor-AC コマンドマニュアル

改版履歴

版数	日付	改版内容
1.0	2020/11	初版発行
1.1	2020/12	・表紙の「本マニュアルについて」の記載を変更しました。 ・誤記訂正
1.2	2021/02	・「2 章 AP 管理」の下記コマンドにメモを追記しました。 **・ap-model** **・wlan ap** ・「3 章 無線管理の設定」の下記コマンドに説明を追記しました。 **・max-power** ・「4 章 WLAN アクセスの設定」の下記コマンドにメモを追記しました。 **・map-configuration** ・「5 章 WLAN セキュリティ」下記コマンドにメモを追記しました。 **・wpa3** **・pmf** ・「14 章 スペクトル管理」の章を追加しました。 ・「20 章 WLAN メッシュ」の章を追加しました。
1.3	2021/05	・「2 章 AP 管理」の下記コマンドの説明を一部削除しました。 **・reset wlan ap** ・「3 章 無線管理の設定」に下記コマンドを追加しました。 **・bss-color** **・dl-ofdma** **・twt negotiate** **・ul-ofdma** ・「3 章 無線管理の設定」の下記コマンドのデフォルト状態を変更しました。 **・mu-txbf** **・su-txbf** ・「7 章 WLAN QoS の設定」に下記コマンドを追加しました。 **・u-apsd enable**

版数	日付	改版内容
1.4	2021/07	・「2 章 AP 管理」の下記コマンドの注意書きに追記しました。 **・remote-configuration synchronize** ・「3 章 無線管理の設定」の下記コマンドにメモ書きを追加しました。 **・type** ・「12 章 チャネルスキャンの設定」の下記コマンドのデフォルト値を変更しました。 **・scan max-service-time** ・「12 章 チャネルスキャンの設定」の下記コマンドのデフォルト値を変更しました。 **・wlan rrm calibration-channel interval** ・「20 章 WLAN メッシュの設定」の下記コマンドのパラメータの一部を削除しました。 **・display wlan mesh-link ap** ・誤記訂正
1.5	2021/09	・「3 章 無線管理の設定」の下記コマンドのパラメータの設定範囲を追記しました。 **・max-power** ・「4 章 WLAN アクセスの設定」の下記コマンドのパラメータの説明を見直しました。また、使用可能な特殊文字を記載しました。 **・ssid** ・「17 章 WLAN RRM」の下記コマンドの説明を一部見直しました。 **・display wlan rrm-history ap**
1.6	2021/10	・「2 章 AP 管理」の下記コマンドのメモ書きの内容を見直しました。 **・remote-configuration** ・「2 章 AP 管理」に下記コマンドを追加しました。 **・wlan timezone-sync enable** ・「4 章 WLAN アクセスの設定」に下記コマンドを追加しました。 **・display wlan bss** ・「6 章 WLAN 認証の設定」に下記コマンドを追加しました。 **・mac-authentication fast-connect enable** ・「8 章 WLAN QoS の設定」に下記コマンドを追加しました。 **・atf**

版数	日付	改版内容
1.7	2021/11	・「1 章 Anchor-AC の設定」の下記コマンドに注意事項を追加しました。 **・anchor-ap** ・「2 章 AP 管理」の下記コマンドのメモ書きの内容を見直しました。 **・ap-model** **・download file** **・wlan ap** ・「4 章 WLAN アクセスの設定」の下記コマンドのメモ書きの内容を見直しました。 **・map-configuration** ・「6 章 WLAN 認証の設定」に「Web 認証(ポータル認証)設定コマンド」を追加しました。
1.8	2021/12	・「2 章 AP 管理」に下記コマンドを追加しました。 **・display wlan ap files** **・display wlan ap reboot-record** ・「3 章 無線管理の設定」の下記コマンドのデフォルト値を修正しました。 **・type** ・「3 章 無線管理の設定」の下記コマンドのパラメータを修正しました。 **・display wlan ap continuous-mode** **・display wlan ap radio** ・「3 章 無線管理の設定」の下記コマンドを削除しました **・reset wlan ap radio statistics** ・「4 章 WLAN アクセスの設定」の下記コマンドの説明を修正しました。 **・display wlan client**
1.9	2022/02	・「3 章 無線管理の設定」に下記コマンドを追加しました。 **・display wlan statistics ap radio** ・「14 章 WLAN 最適化」に下記コマンドを追加しました。 **・rrop anti-bmc rate-limit** **・rrop anti-bmc rate-limit pps** ・「20 章 WLAN メッシュの設定」に QX-W1100 シリーズでの WLAN メッシュ機能サポートに関するメモ書きを追加しました。

版数	日付	改版内容
1.10	2022/03	・「2 章 AP 管理」に下記コマンドを追加しました。 **・display wlan ap diagnostic-information** ・「2 章 AP 管理」の下記コマンドに、時刻設定に関するメモ書きを追記しました。 **・data-tunnel encryption** ・「3 章 無線管理の設定」の下記コマンドの出力説明に内容を追記しました。 **・display wlan statistics ap radio** ・「4 章 WLAN アクセスの設定」の下記コマンドのパラメータ範囲を修正しました。 **・client max-count** ・「5 章 WLAN 認証」の下記コマンドのデフォルト値と設定範囲の記述を修正しました。 **・dot1x max-user** **・mac-authentication max-user** ・「9 章 WLAN ローミングの設定」に下記コマンドを追加しました。 **・ft enable** **・ft method** **・ft reassociation-timeout** **・bss transition-management disassociation** **・bss transition-management enable** **・sacp anti-sticky** ・「13 章 バンドナビゲーションの設定」の下記コマンドの説明を見直しました。 **・wlan band-navigation balance access-denial** ・「14 章 WLAN 最適化」に下記コマンドを追加しました。 **・rrop anti-bmc network** ・「16 章 WLAN 高可用性の設定」の章を追加しました ・誤記訂正

版数	日付	改版内容
1.11	2022/05	・「2 章 AP 管理」の下記コマンドの出力説明に内容を追記しました。 **・display wlan ap** ・「2 章 AP 管理」の下記コマンドのパラメータ説明に、指定可能な AP モデルの表を追加しました。 **・ap-model** **・wlan ap** ・「3 章 無線管理の設定」に下記コマンドを追加しました。 **・reset wlan statistics ap radio** ・「3 章 無線管理の設定」の下記コマンドの説明に QX-W1110 の情報を追記しました。 **・max-power** **・type** ・「5 章 WLAN セキュリティ」の下記コマンドに QX-W1100 シリーズでの gcmp パラメータのサポートに関するメモ書きを追記しました。 **・cipher-suite** ・「5 章 WLAN セキュリティ」下記コマンドに QX-W1100 シリーズでの WPA3 エンタープライズ 192bit セキュリティモードのサポートに関するメモ書きを追記しました。 **・wpa3** ・「6 章 WLAN 認証」下記コマンドに最大接続数制限の動作に関するメモ書きを追加しました。 **・dot1x max-user** **・mac-authentication max-user** ・「11 章 WLAN 無線リソース計測の設定」の下記コマンドに **spectrum** と **tpc** パラメータを追加しました。 **・measure** ・「17 章 WLAN RRM」に下記コマンドを追加しました。 **・calibrate-bandwidth self-decisive** **・wlan rrm calibration-bandwidth interval** ・誤記訂正

版数	日付	改版内容
1.12	2022/06	・「2 章 AP 管理」の下記コマンドに **apid** のパラメータを追加しました。 **・display wlan ap** ・「3 章 無線管理の設定」　下記コマンドのデフォルト値の記載を変更しました。 **・bss-color** **・dl-ofdma** **・twt negotiate** **・ul-ofdma**・「9 章 WLAN ローミングの設定」に下記コマンドを追加しました。 **・ft mobility-domain-id** ・誤記訂正
1.13	2022/09	・「2 章 AP 管理」の下記コマンドのコマンド出力の表中の「Maximum supported APs」の説明に、QX-W1100 シリーズで QX-W1000 シリーズを管理する際の注意書きを追加しました。 **・display wlan ap** ・「2 章 AP 管理」に下記コマンドを追加しました。 **・wlan ap-image-deploy** **・wlan image-load filepath** ・「3 章 無線管理の設定」に下記コマンドを追加しました。 **・channel-usage threshold** ・「4 章 WLAN アクセスの設定」に下記コマンドを追加しました。 **・display wlan client failure** **・user-profile** **・wlan client failure history aging** **・wlan permit-ssid** ・「6 章 WLAN 認証」の下記コマンドに 802.1X 認証での失敗許可機能に関する説明を追加しました。 **・fail-permit template** ・誤記訂正

版数	日付	改版内容
1.14	2022/12	・「2 章 AP 管理」に以下のコマンドを追加しました。 ・**display wlan ap statistics image-download** ・「4 章 WLAN アクセスの設定」に下記コマンドを追加しました。 ・**access-control acl** ・**display wlan client device-information** ・「5 章 WLAN セキュリティ」に下記コマンドを追加しました。 ・**akm sae pwe** ・「5 章 WLAN セキュリティ」 下記コマンドのデフォルト値を変更しました。 ・**gtk-rekey enable** ・**ptk-rekey enable** ・「5 章 WLAN セキュリティ」 下記コマンドに WEP に関する重要事項を記載しました。 ・**cipher-suite** ・**wep key** ・**wep key-id** ・**wep mode dynamic** ・「8 章 WLAN QoS の設定」に下記コマンドを追加しました。 ・**mu-edca client** ・「14 章スペクトル管理」の章内容は「17 章 WLAN RRM」に含まれているため「14 章スペクトル管理」を削除しました。 ・「16 章 WLAN 高可用性の設定」の 下記コマンドの説明を見直しました。 ・**wlan tunnel-preempt** ・「21 章 コンフィグレーションプロファイル」を追加しました。

版数	日付	改版内容
1.15	2023/04	・「1 章 Anchor-AC の設定」の下記コマンドの view を変更しました。 ・**anchor-ap** ・「3 章 無線管理の設定」　の下記コマンドのデフォルト値を変更しました。 ・**mu-txbf** ・**su-txbf** ・「3 章 無線管理の設定」に下記コマンドを追加しました。 ・**radio-type 2.4g** ・**radio-type 5g** ・「4 章 WLAN アクセスの設定」の下記コマンドは使用出来ない為削除しました。 ・**display wlan statistics** ・「4 章 WLAN アクセスの設定」の下記コマンドは QX-W1100 シリーズで利用できない為、メモ書きにコマンド使用可能機種に関する注意書きを追記しました。 ・**wlan link-test** ・「4 章 WLAN アクセスの設定」に下記コマンドを追加しました。 ・**display wlan statistics client** ・**display wlan statistics connect-history** ・**display wlan statistics service-template** ・**reset wlan statistics service-template** ・誤記訂正
1.16	2023/06	・「3 章 無線管理の設定」の下記コマンドの設定範囲を変更しました。 ・**max-power** ・「3 章 無線管理の設定」　の下記コマンドのデフォルト値を変更しました。 ・**mu-txbf** ・**su-txbf** ・「4 章 WLAN アクセスの設定」下記コマンドの **vlan** パラメータは使用できないため削除しました。 ・**client forwarding-location** ・「21 章 コンフィグレーションプロファイル」の下記コマンドの Syntax に **acl number** *acl-number* の形式を追記しました。 ・「22 章 Web リダイレクトの設定」を追加しました。

版数	日付	改版内容
1.17	2024/01	・「2 章 AP 管理」に下記コマンドを追加しました。 ・**wlan save ap-configuration** ・「2 章 AP 管理」の下記コマンドの led についての説明を追記しました。 ・**display wlan ap** ・「3 章 無線管理の設定」の下記コマンドのレーダ信号検出時の説明を修正しました。 ・**channel** ・「3 章 無線管理の設定」の下記コマンドの説明を追記しました。 ・**power-lock enable** ・「4 章 WLAN アクセスの設定」の以下のコマンドの **vlan** パラメータを削除しました。 ・**client forwarding-location** ・「5 章 WLAN セキュリティ」の下記コマンドの **enterprise-only-mode**、**enterprise-transition-mode** のパラメータをサポートしました。 ・**wpa3** ・誤記訂正
1.18	2024/06	・「3 章 無線管理の設定」に下記のコマンドを追加しました。 ・**radar-channel-switchback disable** ・「4 章 WLAN アクセスの設定」に下記コマンドを追加しました。 ・**display wlan client online-duration** ・「9 章 WLAN ローミングの設定」に下記のコマンドを追加しました。 ・**authentication-mode** ・**display wlan mobility** ・**display wlan mobility group** ・**display wlan mobility roam-track mac-address** ・**group enable** ・**member ip** ・**source ip** ・**tunnel-type** ・**wlan mobility group** ・**wlan mobility-group-isolation enable** ・「23 章 IoT 機能の設定」を追加しました。 ・「24 章 Hotspot 2.0 の設定」を追加しました。

版数	日付	改版内容
1.19	2024/10	・「2 章 AP 管理」に下記コマンドを追加しました。 ・**display wlan ap group-name** ・「5 章 WLAN セキュリティ」の下記コマンドで、**pass-phrase** の文字列に ”?” の文字の使用をサポートしました。 ・**preshared-key** ・「5 章 WLAN セキュリティ」の下記コマンドの説明を修正しました。 ・**pmf association-comeback** ・「15 章 WLAN IP スヌーピング」に下記コマンドを追加しました。 ・**wlan client ip-conflict-detection enable** ・「23 章 IoT 機能の設定」の下記のメモ欄を削除しました。 ・**filter rssi threshold** ・**filter rssi-fluctuation threshold** ・**filter recent-packet duration** ・**filter highest-rssi** ・誤記訂正
1.20	2025/06	・「9 章 WLAN ローミングの設定」の下記コマンドの説明に **force-logoff** パラメータのサポートに関するメモ書きを追加しました。 ・**sacp anti-sticky** ・「14 章 WLAN 最適化」に下記コマンドを追加しました。 ・**rrop client fast-keep-alive**
1.21	2025/12	・「2 章 AP 管理」の下記コマンドの AP グループに設定可能な最大ルール数の記述を更新しました。 ・**if-match ip** ・「14 章 WLAN 最適化」に下記コマンドを追加しました。 ・**option keep-active** ・「14 章 WLAN 最適化」の下記コマンドに **Interval** のパラメータを追記しました。 ・**rrop client fast-keep-alive** ・誤記訂正

版数	日付	改版内容
1.22	2026/02	・「3 章 無線管理の設定」の下記コマンドのパラメータの説明を更新しました ・**max-power** ・「7 章 WIPS の設定」の下記コマンドの quiet パラメータのデフォルト値を追記しました。 ・**deauthentication-broadcast** ・「WLAN 高可用性の設定」の下記のコマンドの説明を更新しました。 ・**deauthentication-broadcast** ・「16 章 WLAN 高可用性の設定」の下記コマンドの説明を更新しました。 ・**wlan tunnel-preempt** ・「17 章 WLAN RRM」の下記コマンドのデフォルト値の説明を更新しました。 ・**adjacency-factor** ・**calibrate-bandwidth self-decisive** ・**calibrate-channel self-decisive** ・**calibrate-power coverage enable** ・**calibrate-power min** ・**calibrate-power self-decisive** ・**calibrate-power threshold** ・**channel-capability mode** ・**channel-switch-mode** ・**crc-error-threshold** ・**interface-threshold** ・**power-capability mode** ・**power-constraint mode** ・**spectrum-management** ・**tolerance-level** ・「17 章 WLAN RRM」の下記コマンドの説明を更新しました。 ・**calibrate-power 2.4g max** ・**calibrate-power 2.4g coverage rssi-threshold** ・**calibrate-power 5g max** ・**calibrate-power 5g coverage rssi-threshold**

版数	日付	改版内容
1.23	2026/07	・「7 章 WIPS の設定」に、無線通信と WIPS センサの併用に関する説明を追加しました。 ・「9 章 WLAN ローミングの設定」の下記コマンドの説明を修正しました。 **・ft enable** ・「14 章 WLAN 最適化」の下記コマンドのメモを修正しました。 **・rrop client fast-keep-alive**
1.24	2026/11	・「4 章 WLAN アクセスの設定」の下記コマンドのデフォルト値のバージョン差分を記載しました。 **・wlan client idle-timeout** ・「5 章 WLAN セキュリティ」の下記コマンドの **private-psk** パラメータは未サポートであるため削除しました。 **・akm mode**

Copyright © NEC Corporation 2019 - 2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- Anchor モードの本装置は *QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC コマンドマニュアル*と、セクション 2 WLAN を除く *QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC コマンドマニュアル*と、セクション 2 WLAN を除く *QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Anchor モードの Version 7.2.X を含む以降です。

関連マニュアル

次のマニュアルには、QX-W1000/W1100 シリーズアクセスポイントに関する詳細な説明があります

マニュアル	内容
QX-W1000/W1100 シリーズアクセスポイントインスタレーションマニュアル	システムのインストールについて説明しています。
QX-W1000/W1100 シリーズアクセスポイントオペレーションマニュアル	機能の設定について説明しています。
QX-W1000/W1100 シリーズアクセスポイントコマンドマニュアル	機能に関するコマンドについて説明しています。
QX-W1000/W1100 シリーズアクセスポイント Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアル	Anchor-AC として動作させる場合の機能設定について説明しています。
QX-W1000/W1100 シリーズアクセスポイント Anchor-AC コマンドマニュアル	Anchor-AC として動作させる場合の機能に関するコマンドについて説明しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **WLAN**

  Anchor-AC の WLAN 設定について説明します。

  WLAN 以外については QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルを参照してください。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**太字体**を使用します。
イタリック体	コマンドの引数は*イタリック体*を使用します。
[ ]	大カッコに囲まれた項目(キーワード、引数)はオプションです。
{ x | y | ... }	選択する項目は、中カッコに入れて縦線で区切ってあります。1 つを選択します。
[x | y | ...]	オプションの選択項目は､大カッコに入れて縦線で区切ってあります。1 つまたは複数を選択します。
{ x | y | ... }*	選択する項目は、中カッコに入れて縦線で区切ってあります。少なくとも 1 つ選択できます。
[x | y | ...]*	オプションの選択項目は、大カッコに入れて、縦線で区切ってあります。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。例えば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <Alt, A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある重要な情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある重要な情報を示します。
⚠ **重要**	注意を払う必要がある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

VI. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 24 個のセクションで構成されています。

01-Anchor AC の設定

02-AP 管理

03-無線管理の設定

04-WLAN アクセスの設定

05-WLAN セキュリティ

06-WLAN 認証

07-WIPS の設定

08-WLAN QoS の設定

09-WLAN ローミングの設定

10-WLAN ロードバランスの設定

11-WLAN 無線リソースの計測の設定

12-チャネルスキャンの設定

13-バンドナビゲーションの設定

14-WLAN 最適化

15-WLAN IP スヌーピング

16-WLAN の高可用性の設定

17-WLAN RRM

18-WLAN 無線ロードバランス

19-WLAN アップリンク検出の設定

20-WLAN メッシュの設定

21-コンフィグレーションプロファイルの設定

22-Web リダイレクトの設定

23-IoT 機能の設定

24-Hotspot 2.0 の設定

目次

1 章 Anchor AC の設定 1-1
1.1 Anchor AC の設定コマンド 1-1
1.1.1 anchor-ap 1-1
1.1.2 display wlan inside-ap 1-2
1.1.3 save 1-3
1.1.4 wlan anchor-ap persistent-mode ac 1-5

1章 Anchor AC の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

1.1 Anchor ACの設定コマンド

1.1.1 anchor-ap

⚠ **注意：**

- QX-W1100 シリーズのバージョン 7.2.47 を含む以降のソフトウェアでは、QX-W1000 シリーズを管理できますが、QX-W1100 シリーズで QX-W1000 シリーズを管理する際にサポートするモードは FIT モードです。QX-W1000 シリーズに対して AC 選出機能を設定しないでください。
- global configuration view での設定は、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

anchor-ap { **disable** | **enable** }

undo anchor-ap

デフォルト

AP view：ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.59 を含む以前のソフトウェアでは無効です。

ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアでは、global configuration view の設定を使用します。

global configuration view：無効

View

AP view

global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: AC 選出機能を無効にします。

enable: AC 選出機能を有効にします。

説明

anchor-ap disable コマンドは AC 選出機能を無効にします。

anchor-ap enable コマンドは AC 選出機能を有効にします。

undo anchor-ap コマンドはデフォルトに戻します。

動作中の Anchor-AC がオフラインになったとき、本コマンドが AP view に設定された AP が新たな Anchor-AC として起動します。

AP view の設定は、global configuration view の設定よりも優先されます。

例

AP**ap1** に対して AC 選出機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1030

[AC-wlan-ap-ap1] anchor-ap enable

1.1.2 display wlan inside-ap

Syntax

display wlan inside-ap

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan inside-ap コマンドは内部 AP の情報を表示します。

内部 AP とは、Anchor-AC 自身の無線管理のために自動で作成される手動 AP を指します。

内部 AP には、AP 名として MAC アドレスが使用されます。

例

AP**ap1** に対して AC 選出機能を有効にします。

<AC> display wlan inside-ap

```
AP name              : 74ea-c8fd-c180
AP ID                : 1
MAC address          : 74ea-c8fd-c180
```

1.1.3 save

Syntax

save *file-url*

save [**safely**] [**backup** | **main**] [**force**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

file-url: 動作中のコンフィグレーションを指定されたファイルに“.cfg”拡張子で、ファイルを次回起動時のコンフィグレーションファイルとして指定せずに保存します。“.cfg”拡張子を除き、ファイル名は大文字小文字を区別しない 1～255 文字の文字列で、パス情報を含むことができます。有効な文字は、文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

safely: safe モードでコンフィグレーションファイルを保存します。このパラメータを指定しない場合、装置は fast モードでコンフィグレーションファイルを保存します。safe モードは fast モードよりも保存に要する時間が遅くなりますが、安全に行うことができます。

backup: 動作中のコンフィグレーションを指定したファイルに保存し、バックアップの次回に起動するコンフィグレーションファイルとして指定します。**backup** パラメータあるいは **main** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

main: 動作中のコンフィグレーションを指定したファイルに保存し、メインの次回に起動するコンフィグレーションファイルとして指定します。**main** パラメータあるいは **backup** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

force: 動作中のコンフィグレーションを、確認の表示を行わずに保存します。本パラメータを指定しない場合、操作を実行する際に確認メッセージが表示されます。30 秒以内に操作を行わない場合、システムは自動で操作を中止します。30 秒以内に“Y”を入力すると、保存処理を継続し、処理中のターゲットファイル名を変更することができます。

説明

AP を管理した状態で“**save**”コマンドを実行すると、Anchor-AC 本体および、管理下のすべての AP に Anchor-AC の設定が保存されます。これにより、動作中の Anchor-AC がオフラインになったあと、AC 選出機能により新しく選出された Anchor-AC が設定を引き継ぎます。V7.2.27 を含む以降のバージョンでは、管理下の AP への設定保存は **anchor-ap enable** が設定されている AP にのみ行います。AC 選出機能の詳細は QX-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアルの *“Anchor AC の設定”* の *“AC 選出”* を参照してください。

⚠ **注意**：

- *file-url* パラメータを指定した場合、Anchor-AC の設定は管理下の AP には保存されません。
- Anchor-AC の設定を管理下の AP に保存したい場合、*file-url* パラメータを指定しないでください。

🕮 **メモ**：

Anchor-AC の設定は管理下の QX-W1010 および QX-W1020 には保存されません。このとき、設定の保存に失敗したことを示す Fail メッセージが表示されますが、運用に問題はありません。V7.2.27 を含む以降のバージョンでは、誤って QX-W1010 および QX-W1020 の ap view に **anchor-ap enable** が設定されている状態にこの事象が発生します。

save *file-url* コマンドは動作中のコンフィグレーションをコンフィグレーションファイルに保存します。次回に起動するコンフィグレーションファイルとして指定しません。

save [**safely**] [**backup** | **main**] [**force**]コマンドは記憶媒体のルートディレクトリのファイルに動作中のコンフィグレーションを保存します。本コマンドは次回に起動するコンフィグレーションファイルとして自動的に指定します。

本コマンドで指定されたファイルが存在しない場合、設定を保存する前、システムはファイルを作成します。すでにファイルが存在する場合、システムはファイルを上書きするかどうか確認メッセージを表示します。ファイルを上書きしない場合、システムは **save** コマンドの操作を中止します。

コマンドの *file-url* パラメータを指定しない場合、コマンドはテキストファイル“.cfg”と、バイナリファイル “.mdb” に動作中のコンフィグレーションを保存します。2 つのファイルは同一ファイル名です。バイナリファイル “.mdb” はテキストファイル “.cfg” よりも保存に要する時間が短くなります。

safe モードでは、システムは一時ファイルに設定を保存し、保存が完了した後、ターゲットの次回の起動に使用するコンフィグレーションファイルの上書きを開始します。動

作に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルは保持されています。

fast モードでは､装置は直接ターゲットの次回の起動に使用するコンフィグレーションファイルを上書きします。動作中に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルが消失します。

例

AP**ap1** に対して AC 選出機能を有効にします。

<AC> save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to device successfully.
<AC>%Mar 15 03:17:27:903 2019 QX-W1030 CWS/6/CWS_RUN_DOWNLOAD_START: AP 9ce8-9525-f7c0 started to download the file startup.cfg.
%Mar 15 03:17:27:908 2019 QX-W1030 CWS/6/CWS_RUN_DOWNLOAD_START: AP 48bd-3d66-2a00 started to download the file startup.cfg.
%Mar 15 03:17:27:921 2019 QX-W1030 CWS/6/CWS_RUN_DOWNLOAD_FAILED: Failed to download image file startup.cfg for AP 9ce8-9525-f7c0.
%Mar 15 03:17:27:930 2019 QX-W1030 CWS/6/CWS_RUN_DOWNLOAD_COMPLETE: Downloading the file startup.cfg for AP 48bd-3d66-2a00 through the CAPWAP tunnel is complete.
```

1.1.4 wlan anchor-ap persistent-mode ac

🕮 **メモ**：

- このコマンドはソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでサポートしています。
- “**wlan anchor-ap persistent-mode ac**”コマンドは“**save**”コマンドにて管理下の AP には保存されません。“**save**”コマンドの詳細は QX-W1000/W1100 シリーズアクセスポイント Anchor-AC コマンドマニュアルの *“Anchor AC の設定”* を参照してください。

Syntax

wlan anchor-ap persistent-mode ac

undo wlan anchor-ap persistent-mode

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan anchor-ap persistent-mode ac コマンドは AC 維持機能を有効にします。

undo wlan anchor-ap persistent-mode コマンドは AC 維持機能を無効にします。

このコマンドは Anchor-AC として動作中の装置に設定可能です。

このコマンドを設定した場合、ネットワーク内に複数の Anchor-AC が存在する状況が発生した際、AC 維持機能を設定している Anchor-AC のみ MAC アドレスに関わらず Anchor-AC モードを維持できます。

このコマンドを設定しない場合、ネットワーク内に複数の Anchor-AC が存在する状況が発生してしまった際、MAC アドレスが最小の Anchor-AC のみ Anchor-AC モードを維持し、その他は Anchor-FIT モードとして再起動します。

このコマンドは“**save**”コマンドにて、管理下の AP には保存されません。“**save**”コマンドの詳細は、QX-W1000/W1100 シリーズアクセスポイント Anchor-AC コマンドマニュアルの *“Anchor-AC の設定”* を参照してください。

例

Anchor-AC に対して AC 維持機能を有効にします。

<AC> system-view

[AC] wlan anchor-ap persistent-mode ac

関連コマンド

save

目次

2 章 AP 管理 2-1
2.1 AP 管理コマンド 2-1
2.1.1 ap 2-1
2.1.2 ap-model 2-2
2.1.3 bridge-aggregation 2-3
2.1.4 data-tunnel encryption 2-5
2.1.5 delete file 2-6
2.1.6 description (AP group view) 2-7
2.1.7 description (AP view) 2-8
2.1.8 discovery-response 2-9
2.1.9 display wlan ap 2-11
2.1.10 display wlan ap address 2-27
2.1.11 display wlan ap all feature capwap 2-28
2.1.12 display wlan ap connection-record 2-29
2.1.13 display wlan ap diagnostic-information 2-30
2.1.14 display wlan ap files 2-31
2.1.15 display wlan ap group-name 2-33
2.1.16 display wlan ap online-time 2-35
2.1.17 display wlan ap reboot-log 2-35
2.1.18 display wlan ap reboot-record 2-36
2.1.19 display wlan ap running-configuration 2-41
2.1.20 display wlan ap statistics association-failure-record 2-45
2.1.21 display wlan ap statistics image-download 2-46
2.1.22 display wlan ap statistics online-record 2-49
2.1.23 display wlan ap tunnel-down-record 2-50
2.1.24 display wlan ap-distribution 2-52
2.1.25 display wlan ap-distribution ap-name 2-53
2.1.26 display wlan ap-group 2-54
2.1.27 display wlan ap-model 2-56
2.1.28 display wlan ap tunnel latency 2-57
2.1.29 display wlan device role 2-59
2.1.30 download file 2-60
2.1.31 echo-count 2-61
2.1.32 echo-interval 2-62
2.1.33 firmware-upgrade 2-63
2.1.34 fragment-size 2-65
2.1.35 gigabitethernet 2-66

2.1.36 hyprid-remote-ap 2-67
2.1.37 if-match ip 2-68
2.1.38 keepalive-interval 2-69
2.1.39 led-mode 2-71
2.1.40 mac-address(AP group view) 2-73
2.1.41 mac-address(AP view) 2-74
2.1.42 port access vlan 2-74
2.1.43 port hybrid pvid 2-76
2.1.44 port hybrid vlan 2-78
2.1.45 port-isolate enable 2-79
2.1.46 port link-aggregation group 2-81
2.1.47 port link-type 2-83
2.1.48 port trunk permit vlan 2-85
2.1.49 port trunk pvid 2-86
2.1.50 qos priority 2-88
2.1.51 qos trust 2-90
2.1.52 remote-configuration 2-92
2.1.53 remote-configuration synchronize 2-93
2.1.54 reset wlan ap 2-95
2.1.55 reset wlan ap reboot-log 2-95
2.1.56 reset wlan tunnel latency ap 2-96
2.1.57 retransmit-count 2-97
2.1.58 retransmit-interval 2-98
2.1.59 serial-id (AP group view) 2-99
2.1.60 serial-id (AP view) 2-100
2.1.61 snmp-agent trap enable wlan ap 2-101
2.1.62 snmp-agent trap enable wlan capwap 2-102
2.1.63 statistics-interval 2-102
2.1.64 tunnel encryption 2-103
2.1.65 tunnel latency-detect 2-105
2.1.66 usb 2-106
2.1.67 vlan 2-107
2.1.68 wlan ap 2-109
2.1.69 wlan apdb 2-110
2.1.70 wlan apdb file 2-112
2.1.71 wlan ap-group 2-113
2.1.72 wlan ap-image-deploy 2-114
2.1.73 wlan auto-ap enable 2-115
2.1.74 wlan auto-ap persistent 2-115
2.1.75 wlan auto-persistent enable 2-116
2.1.76 wlan capwap discovery-policy unicast 2-117
2.1.77 wlan global-configuration 2-117
2.1.78 wlan image-load filepath 2-118

2.1.79 wlan re-group 2-119
2.1.80 wlan rename-ap..... 2-120
2.1.81 wlan save ap-configuration 2-121
2.1.82 wlan timezone-sync enable..... 2-122

2章 AP 管理

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

2.1 AP管理コマンド

2.1.1 ap

Syntax

ap *ap-name-list*

undo ap *ap-name-list*

デフォルト

AP 名による AP group ルールは作成されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ap-name-list: スペースで区切られた最大 10 の AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別しない 1～64 文字の文字列です。

説明

ap コマンドは AP group ルールを作成します。

undo ap コマンドは AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先順位は、降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group view でこのコマンドを実行することはできません。

例

AP 名で AP group ルールを作成するために、AP **ap1**、**ap2**、**ap3** を AP group **group1** に追加します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap ap1 ap2 ap3

関連コマンド

wlan ap-group

2.1.2 ap-model

Syntax

ap-model *ap-model*

undo ap-model *ap-model*

デフォルト

設定無し

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ap-model: AP モデル名を指定します。

表 2-1 に、装置で指定可能な AP モデル名を示します。

表 2-1 ap-model コマンドで指定可能な AP モデル名

指定可能な AP モデル / Anchor-AC モードの AP モデル	QX-W1010 QX-W1020 QX-W1030	QX-W1110	QX-W1120	QX-W1130
QX-W1030 の場合	指定可能	管理対象外	管理対象外	管理対象外
QX-W1110 の場合	指定可能	指定可能	指定可能	指定可能
QX-W1120 の場合	指定可能 (v7.2.47 以降)	指定可能 (V7.2.55 以降)	指定可能	指定可能
QX-W1130 の場合	指定可能 (v7.2.47 以降)	指定可能 (V7.2.55 以降)	指定可能	指定可能

説明

ap-model コマンドは AP モデルを作成し、その view に移行します。

undo ap-model コマンドは AP モデルとその設定を削除します。

例

#AP グループ group1 に AP モデル QX-W1030 を作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1030

2.1.3 bridge-aggregation

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

bridge-aggregation *interface-number*

undo bridge-aggregation *interface-number*

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、アグリゲートインタフェースは存在しません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。

説明

bridge-aggregation コマンドはアグリゲートインタフェースを作成し、その view あるいは既存のアグリゲートインタフェースの view に移行します。

Undo bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 に対してアグリゲートインタフェース 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] bridge-aggregation 1

[AC-wlan-ap-ap1-bridge-aggregation-1]

AP グループ group1 に対してアグリゲートインタフェース 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-bridge-aggregation-1]

関連コマンド

- **remote-configuration**
- **remote-configuration synchronize**

2.1.4 data-tunnel encryption

Syntax

data-tunnel encryption { **disable** | **enable** }

undo data-tunnel encryption

デフォルト

AP view：AP group view の設定を使用

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: CAPWAP データトンネル暗号化を無効にします。

enable: CAPWAP データトンネル暗号化を有効にします。

説明

🕮 **メモ**：

CAPWAP データトンネル暗号化には独自の証明書をしており、時刻の有効性を確認しています。CAPWAP トンネル暗号化を利用する場合は、事前に装置の時刻が正しく設定されているか確認してください。

data-tunnel encryption enable コマンドは CAPWAP データトンネル暗号化を有効にします。

data-tunnel encryption disable コマンドは CAPWAP データトンネル暗号化を無効にします。

undo data-tunnel encryption コマンドはデフォルトに戻します。

本コマンド適用時、CAPWAP トンネルが再接続されます。

本機能を有効にすると、AP は AC から初めて keepalive パケットを受信したとき、鍵を含む暗号化情報を CAPWAP トンネル経由で AC と交換します。交換後、AC と AP は CAPWAP データトンネル内で転送されたデータパケットを暗号化します。keepalive パケットは暗号化されません。

本機能を有効にする前に、CAPWAP 制御トンネル暗号化が有効になっていることを確認してください。

AP view の設定は AP group view の設定より優先されます。

例

AP **ap1** に対して CAPWAP データトンネル暗号化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] data-tunnel encryption enable

```
This operation will restart the AP. Continue? [Y/N]
```

APgroup **group1** の説明を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] data-tunnel encryption enable

```
This operation will restart member APs that are not enabled with CAPWAP data
tunnel encryption. Continue? [Y/N]
```

関連コマンド

tunnel encryption

2.1.5 delete file

Syntax

delete file *filename*

View

AP view

定義済みユーザロール

network-admin

パラメータ

filename: ファイル名を 1～255 文字の文字列で指定します。

説明

delete file コマンドは AP からファイルを削除します。

このコマンドは、AP がマスタ AC と CAPWAP トンネルを確立した後でのみ有効です。

例

AP **ap1** から **startup.cfg** ファイルを削除します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] delete file startup.cfg

関連コマンド

- **display wlan ap files**
- **download file**

2.1.6 description (AP group view)

Syntax

description *text*

undo description

デフォルト

AP group には説明が設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

text: 1～64 文字で指定します。大文字、小文字を区別します。

説明

description コマンドは AP group の説明を設定します。

undo description コマンドは AP group の説明を削除します。

例

APgroup **group1** の説明を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] description L3-office

関連コマンド

- **display wlan ap-group**
- **wlan ap-group**

2.1.7 description (AP view)

Syntax

description *text*

undo description

デフォルト

AP には説明が設定されていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

text: 1～64 文字で指定します。大文字、小文字を区別します。

説明

description コマンドは AP の説明を設定します。

undo description コマンドは AP の説明を削除します。

例

AP **ap1** の説明を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] description L3-office

関連コマンド

display wlan ap

2.1.8 discovery-response

Syntax

discovery-response wait-time *seconds*

undo discovery-response wait-time

デフォルト

AP view：AP group view の設定を使用

AP group view：2 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

seconds: 2～20 秒の範囲で検出応答タイムアウトタイマを指定します。

説明

discovery-response wait-time コマンドは検出応答タイムアウトタイマを設定します。

undo discovery-response wait-time コマンドはデフォルトに戻します。

検出応答タイムアウトタイマにより、AP が別の検出応答を待つためのタイムアウト時間を指定します。AP が検出応答パケットを受信すると、検出応答タイムアウトタイマが作成もしくは更新されます。タイムアウトタイマが終了すると、AP は最適な AC に対して参加要求を送信します。

ネットワーク品質がプアな場合、検出応答タイムアウトタイマを大きい値に設定してください。

AP view の設定は AP group view の設定より優先されます。

例

AP **ap1** に対して検出応答タイムアウトタイマを 3 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] discovery-response wait-time 3

AP グループ **group1** のすべての AP に対して検出応答タイムアウトタイマを 3 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group group1] discovery-response wait-time 3

2.1.9 display wlan ap

🕮 メモ：

apid のパラメータはソフトウェアバージョン 7.2.56 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap { **all** | **apid** *ap-id* | **name** *ap-name* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

apid *ap-id*: AP を apid で指定します。

name *ap-name*: AP 名指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

verbose: 詳細情報を表示します。

説明

display wlan ap コマンドは AP 情報を表示します。

例

ソフトウェアバージョン 7.2.67 を含む以前のソフトウェアの AP において、すべての AP に関する情報を表示します。

<AC> display wlan ap all

```
Total number of APs: 2
Total number of connected APs: 1
Total number of connected manual APs: 0
Total number of connected auto APs: 0
Total number of connected common APs: 0
Total number of connected WTUs: 0
Total number of inside APs: 1
Maximum supported APs: 100
```

```
Remaining APs: 100
Total AP licenses: 100
Remaining AP licenses: 100

                          AP information
 State : I = Idle,      J  = Join,      JA = JoinAck,    IL = ImageLoad
        C = Config,     DC = DataCheck,  R  = Run   M = Master,  B = Backup

AP name                    APID  State Model          Serial ID
ap1                        1     I     QX-W1020       210235A1BSC123000050
98f1-800d-74e0             1     R/M   QX-W1130       219801A2GH820AE00063
```

ソフトウェアバージョン 7.2.73 を含む以降のソフトウェアの AP において、すべての AP に関する情報を表示します。

<AC> display wlan ap all

```
Total number of APs: 2
Total number of connected APs: 2
Total number of connected manual APs: 0
Total number of connected auto APs: 1
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 1
Maximum supported APs: 50
Remaining APs: 49
Total AP licenses: 50
Local AP licenses: 50
Server AP licenses: 0
Remaining AP licenses: 49
Sync AP licenses: 0

                          AP information
 State : I = Idle,      J  = Join,      JA = JoinAck,    IL = ImageLoad
        C = Config,     DC = DataCheck,  R  = Run   M = Master,  B = Backup

AP name    APID  State Model          Serial ID            Dev-Type  Work-mode
ap1        1     I     QX-W1020       210235A1BSC123000050  COMMON    FitAP
ap2        1     R/M   QX-W1130       219801A2GH820AE00063  COMMON    FitAP
```

表 2-2 コマンド出力

フィールド	説明
Total number of APs	FITまたはAnchor-FIT APの総数です。
Total number of connected APs	接続されたFITまたはAnchor-FIT APの総数です。
Total number of connected manual APs	接続されている手動のFITまたはAnchor-FIT APの総数です。
Total number of connected auto APs	接続されている自動のFITまたはAnchor-FIT APの総数です。
Total number of connected common APs	接続されたFITまたはAnchor-FIT APの総数です。
Total number of connected WTUs	このフィールドは現在のソフトウェアではサポートしていません。
Total number of inside APs	接続されている内部APの総数です。内部APは、Anchor-ACモードでAPが機能するときに自動的に作成される手動APです。
Maximum supported APs	管理できるAPの最大数です。 ⚠ **注意：** QX-W1100 シリーズで QX-W1000 を管理している場合は、管理保証 AP 台数が 51 台(Anchor-AC 自身を含む)までになりますが、100 から変更されません。QX-W1100 シリーズで QX-W1000 シリーズを管理する際は 51 台を超えて接続しないようにご注意ください。
Remaining APs	残りのAP数です。
Total AP licenses	APライセンスの総数です。
Remaining AP licenses	残りのAPライセンス数です。
APID	AC上のAPを一意に識別するためのIDです。

フィールド	説明
Stete	APの現在の状態を以下のように表示します。 ● **I**ーアイドル ● **J**ージョイン ● **JA**ージョイン確認 ● **IL**ーAPがバージョンをダウンロードしています。 ● **C**ーAPが初期設定をダウンロードしています。 ● **DC**ーAPがデータをチェックしています。 ● **R**ーAPが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● **R/M**ーマスタCAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● **R/B**ーバックアップCAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● **M**ーAPはマスタACに接続されています。 ● **B**ーAPはバックアップACに接続されています。
Model	APのモードを表示します。 ● QX-W1010, QX-W1020, QX-W1030 ● QX-W1110, QX-W1120, QX-W1130
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。
Dev-Type	このフィールドには**COMMON**が表示されます。
Work-mode	このフィールドには**FitAP**が表示されます。

AP **ap1** に関する詳細情報を表示します。

<AC> display wlan ap name ap1 verbose

```
AP name                    : ap1
AP ID                      : 1
AP group name               : default-group
State                      : Run
Backup type                 : Master
Online time                 : 0 days 1 hours 25 minutes 12 seconds
System up time              : 0 days 2 hours 22 minutes 12 seconds
Model                      : QX-W1020
Region code                 : JP
Region code lock            : Disable
```

```
Serial ID                 : 219801A0CNC138011454
MAC address               : 0AFB-423B-893C
IP address                : 192.168.1.50
UDP control port number     : 18313
UDP data port number        : N/A
H/W version               : Ver.C
S/W version               : 7.1.0
Boot version              : 1.01
USB state                 : N/A
Power Level               : N/A
PowerInfo                 : N/A
Description               : wtp1
Priority                  : 4
Echo interval              : 10 seconds
Statistics report interval   : 50 seconds
Fragment size (data)        : 1500
Fragment size (control)     : 1450
MAC type                  : Local MAC & Split MAC
Tunnel mode               : Local Bridging & 802.3 Frame & Native Frame
Discovery type             : Static Configuration
Retransmission count        : 3
Retransmission interval     : 5 seconds
Firmware upgrade           : Enabled
Sent control packets        : 1
Received control packets     : 1
Echo requests             : 147
Lost echo responses         : 0
Average echo delay          : 3
Last reboot reason          : User soft reboot
Latest IP address          : 10.1.0.2
Tunnel down reason          : Request wait timer expired
Connection count           : 1
Backup Ipv4               : Not configured
Backup Ipv6               : Not configured
Tunnel encryption          : Disabled
LED mode                  : Normal
Remote configuration        : Enabled
Radio 1:
   Basic BSSID            : 0AFB-42f6-3940
   Admin state            : Up
   Radio type             : 802.11ac
   Antenna type           : internal
   Client dot11ac-only     : Disabled
```

```
Client dot11n-only       : Disabled
Channel band-width       : 20/40/80MHz
Active band-width        : 20/40/80MHz
Secondary channel offset  : SCB
Short GI for 20MHz       : Supported
Short GI for 40MHz       : Supported
Short GI for 80MHz       : Supported
Short GI for 160MHz      : Not supported
A-MSDU                 : Enabled
A-MPDU                 : Enabled
LDPC                   : Not Supported
STBC                   : Supported
Operational VHT-MCS Set:
   Mandatory           : Not configured
   Supported           : NSS1 0,1,2,3,4,5,6,7,8,9
                         NSS2 0,1,2,3,4,5,6,7,8,9
   Multicast           : Not configured
Operational HT MCS Set:
   Mandatory           : Not configured
   Supported           : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                         10, 11, 12, 13, 14, 15
   Multicast           : Not configured
Channel                : 44(auto)
Channel usage(%)         : 15
Max power              : 20 dBm
Operational rate:
   Mandatory           : 6, 12, 24 Mbps
   Multicast           : Auto
   Supported           : 9, 18, 36, 48, 54 Mbps
   Disabled            : Not configured
Distance               : 1 km
ANI                    : Enabled
Fragmentation threshold   : 2346 bytes
Beacon interval         : 100 TU
Protection threshold     : 2346 bytes
Long retry threshold     : 4
Short retry threshold    : 7
Maximum rx duration      : 2000 ms
Noise Floor            : -102 dBm
Smart antenna          : Enabled
Smart antenna policy     : Auto
Protection mode         : rts-cts
Continuous mode         : N/A
```

```
    HT protection mode       : No protection
Radio 2:
    Basic BSSID             : 0AFB-42f6-3950
    Admin state             : Down
    Radio type              : 802.11b
    Antenna type            : internal
    Client dot11n-only       : Disabled
    Channel band-width       : 20MHz
    Active band-width        : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz       : Supported
    Short GI for 40MHz       : Supported
    A-MSDU                  : Enabled
    A-MPDU                  : Enabled
    LDPC                    : Not Supported
    STBC                    : Supported
    Operational HT MCS Set:
       Mandatory            : Not configured
       Supported            : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                              10, 11, 12, 13, 14, 15
       Multicast            : Not configured
    Channel                 : 5(auto)
    Channel usage(%)         : 0
    Max power               : 20 dBm
    Preamble type            : Short
    Operational rate:
       Mandatory            : 1, 2, 5.5, 11 Mbps
       Multicast            : Auto
       Supported            : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
       Disabled             : Not configured
    Distance                : 1 km
    ANI                     : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval          : 100 TU
    Protection threshold     : 2346 bytes
    Long retry threshold     : 4
    Short retry threshold    : 7
    Maximum rx duration      : 2000 ms
    Noise Floor             : 0 dBm
    Smart antenna           : Enabled
    Smart antenna policy     : Auto
    Protection mode          : rts-cts
    Continuous mode          : N/A
```

```
HT protection mode       : No protection
```

表 2-3 コマンド出力

フィールド	説明
Stete	APの現在の状態を以下のように表示します。 ● **Idle**－アイドル ● **Join**－ジョイン ● **JoinAck**－ジョイン確認 ● **Image**－APがバージョンをダウンロードしています。 ● **Config**－APが初期設定をダウンロードしています。 ● **Data Check**－APがデータをチェックしています。 ● **Run**－APが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● **R/M**－マスタCAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● **R/B**－バックアップCAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● **M**－APはマスタACに接続されています。 ● **B**－APはバックアップACに接続されています。
Backup type	CAPWAPトンネルタイプです。 ● **Idle**－APはACとCAPWAPトンネルを確立していません。 ● **Master**－APとマスタAC間に確立されたCAPWAPトンネルです。 ● **Backup**－APとバックアップAC間に確立されたCAPWAPトンネルです。
Region code lock	● Enable ● Disable
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。
MAC address	APのMACアドレスです。MACアドレスが設定されていない場合、このフィールドには**Not configured**が表示されます。
UDP control port number	CAPWAPコントロールトンネルを確立するためにAPによって使用されるポート番号です。
UDP data port number	CAPWAPデータトンネルを確立するためにAPによって使用されるポート番号です。
H/W version	APのハードウェアバージョンです。

フィールド	説明
S/W version	APのソフトウェアバージョンです。
USB state	USB状態: ● Enabled. ● Disabled. USB状態の情報がない場合、このフィールドには**N/A**が表示されます。
Power Level	このフィールドは現在のソフトウェアバージョンではサポートされていません。 電力レベル: ● Low. ● Middle. ● High. 電力レベルが不明の場合、このフィールドには**N/A**が表示されます。
PowerInfo	電源情報
PoE status	このフィールドは現在のソフトウェアバージョンではサポートされていません。 各PIのPoE電源状態: ● Enabled. ● Disabled.
Description	APの説明です。説明が設定されていない場合、このフィールドには**Not configured**が表示されます。
Priority	ACに対するAP接続優先度です。
Fragment size (data)	CAPWAPデータパケットの最大フラグメントサイズです。
Fragment size (control)	CAPWAP制御パケットの最大フラグメントサイズです。
MAC type	AP-AC接続のMACタイプです。 ● **Local MAC**－APはACにフレームを送信する前に802.3形式でカプセル化します。 ● **Split MAC**－APはACにフレームを送信する前に802.11形式でカプセル化します。 ● **Local & Split MAC**－APをACはフレームに送信する前に、フレームを802.3形式または802.11形式でカプセル化します。

フィールド	説明
Tunnel mode	サポートされているAPのトンネルモードです。 ● **Local Bridging**－APはローカルブリッジングをサポートし、データをACに転送しません。 ● **802.3 Frame**－APはフレームを802.3形式でカプセル化してACに送信します。 ● **Native Frame**－APはフレームを802.11形式でカプセル化してACに送信します。 ● **Local Bridging & 802.3 Frame**－APは、ローカルブリッジングモードと802.3フレームモードをサポートしています。 ● **802.3 Frame & Native Frame**－APは、802.3フレームモードとネイティブフレームモードをサポートしています。 ● **Local Bridging & Native Frame**－APはローカルブリッジモードとネイティブフレームモードをサポートしています。
Discovery type	APの検出タイプです。 ● **Static Configuration**－APは手動で設定されたACのIPv4アドレスを使用します。 ● **DHCP**－APはDHCPを介してACのIPアドレスを取得します。 ● **DNS**－APはDNSを介してACのIPアドレスを取得します。 ● **Unknown.**
Retransmission count	AC要求の再伝送試行回数です。
Retransmission interval	AC要求を再伝送する間隔です。
Firmware upgrade	APソフトウェアアップグレードです。 ● Enable ● Disable
Sent control packet	ACが**Run**状態となった後に送信されたパケットの数です。**Change State Event Response**パケットが含まれています。
Received control Packets	ACが**Run**状態となった後に受信したパケット数です。**Change State Event Response**パケットが含まれています。
Echo requests	実行状態でAPによって送信されたエコー要求の数です。
Lost echo responses	実行状態でAPによって受信されなかったエコー応答の数です。
Average echo delay	平均エコー遅延（ミリ秒）です。

フィールド	説明
Last reboot reason	APの最後の再起動理由： ● 電源投入 ● ハードリブート ● ウォッチドッグによる再起動 ● 不明な再起動 ● ユーザによるソフトリブート ● カーネル例外ソフトリブート ● カーネルデッドループソフトリブート ● 自動アップデートによるソフトリブート ● 不明なソフトリブート ● メモリ枯渇 ● その他
Latest IP address	APによって最近使用されたIPアドレスです。

フィールド	説明
Tunnel down reason	CAPWAPトンネルがダウンする原因: ● タイマの作成に失敗しました。 ● 隣接デッドタイマが切れました。 ● 要求待ちタイマの有効期限が切れました。 ● データチェックタイマーの有効期限が切れました。 ● データチャネルキープアライブメッセージの処理に失敗しました。 ● 要求を処理できませんでした。 ● APがリセットされました。 ● APが削除されました。 ● オンラインにできませんでした。 ● シリアル番号が変更されました。 ● MACアドレスが変更されました。 ● APの数が上限を超えました。 ● 実行状態中に結合要求されました。 ● APコンテキストの作成に失敗しました。 ● 失敗結果コードを受信しました。 ● メッセージの再送信に失敗しました。 ● 画像ファイルのダウンロードに失敗しました。 ● イメージファイルが正常にダウンロードされました。 ● ファイル操作タイマの有効期限が切れました。 ● トンネルを追加できませんでした。 ● APからWTPトンネルダウンイベントを受信しました。 ● バックアップACがバックアップトンネルを閉じました。 ● マスタとバックアップトンネルの切り替えです。 ● 設定を継承できませんでした。 ● AP認証に失敗しました。 CAPWAPトンネルがダウンしなかった場合、このフィールドには**N/A**が表示されます。
Connection count	APがACに接続した回数です。次のいずれかの場合にクリアされます。 ● ACの再起動 ● APのシリアルIDの変更 **reset wlan ap**コマンドでは、接続した回数はクリアされません。

フィールド	説明
Backup Ipv4	バックアップACのIPv4アドレスです。バックアップACが指定されていない場合、このフィールドには**Not configured**が表示されます。
Backup ipv6	バックアップACのIPv6アドレスです。バックアップACが指定されていない場合、このフィールドには**Not configured**が表示されます。
Tunnel encryption	• Enable • Disable
LED mode	LED点灯モードです。 • **quiet**－LEDが常に消灯するモードです。 • **always-on**－LEDが常に緑点灯するモードです。 • **awake**－LEDが1秒緑点灯、60秒間消灯を繰り返すモードです。 • **normal**－APの動作状況ごとにLEDの点灯・点滅パターンが変更するモードです。
Remote configuration	• Enabled. • Disabled.
Basic BSSID	無線のMACアドレスです。APがACとのCAPWAPトンネルを確立していない場合、このフィールドにはN/Aが表示されます。
Admin state	無線の状態です。 • Up • Down

Radio type	ワイヤレスモードです。
	• 2.4 GHz
	  • 802.11b
	  • 802.11g
	  • 802.11n(2.4GHz)
	• 5 GHz
	  • 802.11a
	  • 802.11n(5GHz)
	  • 802.11ac
	  • 802.11ax

Client dot11ac-only	• **Enable**－802.11a/b/g/n/acクライアントを無線と関連付けることができます。 • **Disable**－802.11acクライアントだけを無線に関連付けることができます。

フィールド	説明
Client dot11n-only	• **Enable**－802.11a/b/g/n/ac/axクライアントを無線と関連付けることができます。 • **Disable**－802.11nまたは802.11ac/axクライアントだけを無線に関連付けることができます。
Client dot11ax-only	• **Enable**－802.11a/b/g/n/axクライアントを無線と関連付けることができます。 • **Disable**－802.11axクライアントだけを無線に関連付けることができます。
Channel band-width	チャネル帯域幅です。 • 20 MHz • 20 or 40 MHz • 20/40/80/160 MHz
Active band-width	実行中の無線帯域幅です。
Secondary channel offset	802.11nおよび802.11ac/ax無線モードのセカンダリチャネル情報です。 • **SCA(Second Channel Above)**－APは40MHz帯域幅モードで動作し、セカンダリチャネルはプライマリチャネルよりも上にあります。 • **SCB(Second Channel Below)**－APは40MHz帯域幅モードで動作し、セカンダリチャネルはプライマリチャネルよりも下にあります。 • **SCN**－APは40MHz帯域幅モードでは動作しません。
Short GI for 20MHz	20MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
Short GI for 40MHz	40MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
Short GI for 80MHz	80MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
Short GI for 160MHz	160MHzモードで動作するときに無線がShort GIをサポートするかどうかを示します。
A-MSDU	• Enable • Disable
A-MPDU	• Enable • Disable
LDPC	• Supported • Not Supported

フィールド	説明
STBC	• Supported • Not Supported
Operational VHT MCS Set	• **Supported**－サポートVHT MCSセット • **Mandatory**－必須VHT MCSセット • **Multicast**－マルチキャストVHT MCSセット
Operational HT MCS Set	• **Supported**－サポートMCSセット • **Mandatory**－必須MCSセット • **Multicast**－マルチキャストMCSセット
Operational HE MCS Set	• **Supported**－サポートHE MCSセット • **Mandatory**－必須HE MCSセット • **Multicast**－マルチキャストHE MCSセット
Channel	• 現在のチャネルがAPによって自動的に選択された最適なチャネルである場合、このフィールドには*Number*<auto>が表示されます。 • 現在のチャネルが手動で設定されている場合、このフィールドには*Number*が表示されます。 • 現在のチャネルがレーダー信号を避けるためにAPによって自動的に選択されたチャネルである場合、このフィールドには*Number*<avoid radar>と表示されます。
Max power	無線の最大送信電力です。
Preamble type	プリアンブルタイプです。 • Short • Long
Operational rate	• Mandatory • Supported • Multicast • Disable • Not configured
Distance	無線信号が到達できる最大距離です。
ANI	• Enable • Disable
Protection threshold	保護メカニズムを起動するために必要なフレーム長のしきい値です。
Long retry threshold	長さがRTSしきい値を超えたフレームの最大再送信試行回数です。

フィールド	説明
Short retry threshold	長さがRTSしきい値を超えないフレームの最大再送試行回数です。
Maximum rx duration	フレームの最大バッファ持続時間です。
Smart antenna	• Enable • Disable
Smart antenna policy	• Auto • High availability • High throughput
Protection mode	競合回避モード: • cts-to-self. • rts-cts.
Continuous mode	連続モード設定： • Transmission rate. • MCS index. • NSS index. • VHT-MCS index. 連続モードが設定されていない場合、このフィールドには**N/A**が表示されます。

フィールド	説明
HT protection mode	802.11n保護モード: ● No protection • APに関連付けられたクライアントと近接の無線装置は802.11nモードで動作しています。APに関連付けられたクライアントは40MHz帯で動作しています。 • APに関連付けられたクライアントは802.11nモードで動作しています。APに関連付けられたクライアントは40MHz帯で動作しています。 ● Non-member protection すべてのAPに関連付けられたクライアントは802.11nモードで動作しています。近接の無線装置は非802.11nモードで動作しています。 ● 20 MHz protection APの無線は40MHz帯を使用します。APに関連付けられたクライアントと近接の無線装置は802.11nモードで動作しています。20MHzの帯域幅を持つ最低 1 つのクライアントがAPの無線と関連付けられています。 ● Non-HT mixed 上記のいずれのモードにもあてはまらないときに使用するモードです。
MU-TxBF	● Enabled. ● Disabled. このフィールドのサポートは、APモデルによって異なります。
SU-TxBF	● Enabled. ● Disabled. このフィールドのサポートは、APモデルによって異なります。

2.1.10 display wlan ap address

Syntax

display wlan ap { **all** | **name** *ap-name* } **address**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap address コマンドは AP アドレス情報を表示します。

例

すべての AP のアドレス情報を表示します。

<AC> display wlan ap all address

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of inside APs: 0
AP name                      IP address                MAC address
ap1                          1.1.1.5                   0afb-428f-fc6a
```

表 2-4 コマンド出力

フィールド	説明
AP name	APの名前です。
IP address	APのIPアドレスです。 オフラインAPの場合、このフィールドには**N/A**が表示されます。
MAC address	APのMACアドレスです。 オフラインAPの場合、このフィールドには**N/A**が表示されます。

2.1.11 display wlan ap all feature capwap

Syntax

display wlan ap all feature capwap

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap all feature capwap コマンドは CAPWAP 機能の設定状態を表示します。

例

CAPWAP 機能の設定状態を表示します。

<AC> display wlan ap all feature capwap

```
AP name                  Upgrade   Encryption  Control-address   Switch-back
ap1                      Disabled Both         Disabled          Horizontal
```

表 2-5 コマンド出力

フィールド	説明
Upgrade	APソフトウェアアップグレードです。 ● Enabled ● Disabled
Encryption	CAPWAPトンネルの暗号化です。 ● **Control**—制御トンネルの暗号化が有効です。 ● **Data**—データトンネルの暗号化が有効です。 ● **Both**—制御、データの両方のトンネルの暗号化が有効です。 ● **Disabled**—制御、データの両方のトンネルの暗号化が無効です。
Control-address	AC の再検出です。 ● Enabled. ● Disabled.

2.1.12 display wlan ap connection-record

Syntax

display wlan ap { **all** | **name** *ap-name* } **connection-record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap connection-record コマンドは AC 上に AP 接続レコードを表示します。

例

AC 上のすべての AP 接続レコードを表示します。

<AC> display wlan ap connection-record

```
AP name                      IP address    State     Time
ap1                          2001::3       Run       05-06 09:47:44
ap2                          2001::5       Run       05-06 09:50:38
```

表 2-6 コマンド出力

フィールド	説明
State	APの現在の状態: • Idle－アイドル状態です。 • Run－CAPWAPトンネルが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。
Time	APがACとCAPWAPトンネルを確立した直近の時間です。

2.1.13 display wlan ap diagnostic-information

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.52 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap name *ap-name* **diagnostic-information**

View

すべての view

定義済みユーザロール

network-admin

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap diagnostic-information コマンドは、AC で管理している AP の診断情報を取得します。

取得した診断情報のファイルは、”apdiag_(apname).tar.gz”として、”apdiag”ディレクトリに保存されます。このコマンドを複数回実行した場合、”apdiag”ディレクトリ内の診断情報ファイルは、最後に実行した際のファイルに上書きされます。

例

AP **ap1** のダイアグ情報を取得します。

<AC> display wlan ap name ap1 diagnostic-information

```
begin to collect apdiag_ap1.tar.gz
save to flash:/apdiag/apdiag_ap1.tar.gz successfully.
```

2.1.14 display wlan ap files

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.49 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap name *ap-name* **files**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap files コマンドは AP 上のファイルおよびファイルフォルダに関する情報を表示します。

例

AP **ap1** のファイルとファイルフォルダに関する情報を表示します。

<AC> display wlan ap name ap1 files

```
Directory of flash:
   0   13638656  wa4300-system.bin
   1   2573312   wa4300-boot.bin
131072 KB total (114208 KB free)
```

表 2-7 コマンド出力

フィールド	説明
0 13638656 xx.xx	ファイルまたはファイルのフォルダ情報: • 0ーシリアル番号です。システムによって自動的に割り当てられます。 • 13638656ーファイルサイズ（バイト）です。ハイフン（ - ）はファイルフォルダを示します。 • xx.xx–ファイルまたはファイルフォルダの名前です。

関連コマンド

- **delete file**
- **download file**

2.1.15 display wlan ap group-name

> 🕮 メモ：
> このコマンドは、ソフトウェアバージョン 7.2.79 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap group-name *ap-group-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap-group-name: AP グループ名を指定します。

説明

display wlan ap group-name コマンドは AP グループ内の AP に関する情報を表示を表示します。

例

AP グループ **group1** のすべての AP に関する情報を表示します。

<AC> display wlan ap group-name default-group

```
Total number of APs: 2
Total number of online APs: 2

                          AP information
 State : I = Idle,     J  = Join,      JA = JoinAck,    IL = ImageLoad
        C = Config,    DC = DataCheck,  R  = Run,   M = Master,  B = Backup
 Online time : Day:Hour:Minute:Second

AP name  APID State  Model    Serial ID           Group name      Online time
Clients Mode  IP address
ap1      1    R/M    QX-W1110 219801A3DG8221E13131 default-group  0:15:31:36
  0      Fit   1.1.1.1
ap2      1    R/M    QX-W1120 219801A2EJ8218E01234 default-group  0:15:50:36
  0      Fit   1.1.1.2
```

表 2-8 コマンド出力

フィールド	説明
Total number of APs	FITまたはAnchor-FIT APの総数です。
Total number of online APs	オンラインのFITまたはAnchor-FIT APの合計数です。
APID	AC上のAPを一意に識別するためのIDです。
AP name	AP名です。
State	APの現在の状態を以下のように表示します。 ● Iーアイドル ● Jージョイン ● JAージョイン確認 ● ILーAPがバージョンをダウンロードしています。 ● CーAPが初期設定をダウンロードしています。 ● DCーAPがデータをチェックしています。 ● RーAPが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● R/Mーマスタ CAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● R/Bーバックアップ CAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● MーAPはマスタACに接続されています。 ● BーAPはバックアップACに接続されています。
Serial ID	APのシリアルIDです。APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。
Group Name	APグループ名です。
Online Time	APのオンライン期間です。
Clients	クライアント数です。
Mode	APモードです。
IP address	APのIPアドレスです。

2.1.16 display wlan ap online-time

Syntax

display wlan ap { **all** | **name** *ap-name* } **online-time**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap online-time コマンドは AP のオンライン期間を表示します。

例

すべての AP のオンライン期間を表示します。

<AC> display wlan ap online-time all

```
AP name          IP address            Time
ap1              1.1.1.2               0 days 0 hours 2 minutes 6 seconds
ap2              1.1.1.1               0 days 0 hours 5 minutes 6 seconds
ap3              1.1.1.6               0 days 0 hours 2 minutes 1 seconds
```

表 2-9 コマンド出力

フィールド	説明
IP address	APのIPアドレスです。
Time	APがオンラインになってからのAPのリアルタイムアソシエーション期間です。

2.1.17 display wlan ap reboot-log

Syntax

display wlan ap name *ap-name* **reboot-log**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap reboot-log コマンドは管理している AP の再起動ログを表示します。

管理している AP でシステムクラッシュが発生した場合、このコマンドを使用してクラッシュに関する詳細情報を表示できます。

このコマンドを使用するには、指定した AP が **Run** 状態であることを確認してください。

例

AP ap1 の再起動のログを表示します。

<AC> display wlan ap name ap1 reboot-log

```
Debugging information is not available on the AC.
Downloading debugging data from AP. Continue? [Y/N]:y
Downloading debugging data. Please wait...
Please enter the same command again to view the log messages.
```

関連コマンド

reset wlan ap reboot-log

2.1.18 display wlan ap reboot-record

メモ:

このコマンドはソフトウェアバージョン 7.2.49 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan ap { **all** | **name** *ap-name* } **reboot-record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap reboot-record コマンドは管理している AP の再起動履歴を表示します。

このコマンドは、オンライン状態の AP から再起動履歴を取得し、AC 上で表示できます。オンライン状態の AP から再起動履歴を取得するには、数分かかります。再起動履歴を再度表示するには、AC が AP から再起動履歴を取得し終えるのを待ってから、再度 **display wlan ap reboot-record** コマンドを実行してください。

AP の再起動履歴は、直近で最大 10 件まで表示されます。

AP が AC から切断されると、AC は AP の再起動履歴を削除します。

このコマンドを使用するには、指定した AP が **Run** 状態であることを確認してください。

例

AP ap1 の再起動履歴を表示します。

<AC> dis wlan ap name ap1 reboot-record

```
******************************************************************************
AP Name : ap1
PowerOn BootTimes   : 76
Watchdog BootTimes  : 0
Software BootTimes  : 4781
Hardware BootTimes  : 1
MotherBoard BootTimes: 0
Backup BootTimes    : 0
SlotOut BootTimes   : 0
Current Boot Type   : Software-boot
Current Running Time: 120(s)
Running Time        : 77(d)12(h)
*** Boot History(Startup Time and Reason) ***
2021-12-08 15:36:46 User soft reboot
2021-01-10 06:22:04 User soft reboot(Stayed in idle state for a long time)
```

```
2021-01-10 06:12:00 User soft reboot(Stayed in idle state for a long time)
2021-01-10 06:01:56 User soft reboot(Stayed in idle state for a long time)
```

全ての AP の再起動履歴を表示します。

<AC> display wlan ap all reboot-record

```
**************************************************************************
Number of Online APs Supporting Displaying Reboot Records: 2
Number of APs from Which Reboot Records Have Been Obtained: 2
**************************************************************************
AP Name   : ap1
PowerOn BootTimes   : 70
Watchdog BootTimes  : 7
Software BootTimes   : 2939
Hardware BootTimes  : 0
MotherBoard BootTimes   : 0
Backup BootTimes  : 0
SlotOut BootTimes   : 0
Current Boot Type  : Poweron-boot
Current Running Time   : 480(s)
Running Time  : 90(d)7(h)
*** Boot History(Startup Time and Reason) ***
2021-09-10 20:46:36 Power on
2021-09-10 20:46:30 Power on
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
**************************************************************************
AP Name   : ap2
PowerOn BootTimes   : 140
Watchdog BootTimes  : 6
Software BootTimes   : 2039
Hardware BootTimes  : 0
MotherBoard BootTimes   : 0
Backup BootTimes  : 0
SlotOut BootTimes   : 0
Current Boot Type  : Poweron-boot
Current Running Time   : 240(s)
Running Time  : 70(d)5(h)
```

```
*** Boot History(Startup Time and Reason) ***
2021-09-10 20:46:36 Power on
2021-09-10 20:46:30 Power on
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 Power on
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
2021-09-10 20:46:51 User soft reboot(Stayed in idle state for a long time)
```

表 2-10 コマンド出力

フィールド	説明
Number of Online APs Supporting Displaying Reboot Records	再起動履歴の表示をサポートしているオンラインのAPの数です。
Number of APs from Which Reboot Records Have Been Obtained	再起動履歴の取得を終えたAPの数です。
AP Name	再起動履歴を取得したAP名です。
PowerOn BootTimes	Power onが原因で再起動した合計回数です。
Watchdog BootTimes	Watchdog rebootが原因で再起動した合計回数です。
Software BootTimes	soft rebootが原因で再起動した合計回数です。
Hardware BootTimes	Hard rebootが原因で再起動した合計回数です。
MotherBoard BootTimes	Master slotの合計再起動回数です。
Backup BootTimes	Standby slotの合計再起動回数です。
SlotOut BootTimes	Stanby slotが外れた合計回数です。
Current Boot Type	現在のBootタイプ。 ● Unknown ● Poweron-boot ● Software-boot ● Watchdog-boot ● Hardware-boot ● MotherBoard-boot ● ExtendWatchdog-boot ● Backup-boot ● ExtendedModuleRemoved-boot
Current Running Time	直近のBootの動作時間です。

フィールド	説明
Running Time	合計の動作時間です。
Boot History	下記が表示されます。 原因： ● Power on ● Hard reboot ● Watchdog reboot ● User soft reboot ● Kernel exception soft reboot ● Kernel deadloop soft reboot ● DevHandShake soft reboot ● Lic overTime soft reboot ● Slave switch soft reboot ● IRF mergesoft reboot ● Auto update soft reboot ● Memory-exhausted reboot ● -Crypto self-test failed reboot サブカテゴリ： ● Reset by admin ● Image was downloaded successfully ● Stayed in idle state for a long time ● WTU reboot because of offline WT ● AP reset from Cloud ● Anomaly detected ● Inconsistent BSS states on AC and AP ● Inconsistent BSS states on AP and in drive

フィールド	説明
	• Inconsistent radio states on AC and AP • Inconsistent radio modes on AC and AP • Inconsistent radio rates on AC and AP • Inconsistent radio channels on AC and AP • Inconsistent radio bandwidth on AC and AP • Inconsistent radio interface states on AC and AP • Inconsistent radio states on AP and in drive • Inconsistent radio modes on AP and in drive • Inconsistent radio channels on AP and in drive • Inconsistent radio bandwidth on AP and in drive • Anchor AC detected another anchor AC with smaller MAC address and switched its role to AP • Anchor AC received a discovery response and switched its role to AP • Anchor AP failed to detect other anchor ACs or ACs and switched its role to AC • Anchor AC detected another anchor AC with higher priority and switched its role to AP • Configure the anchor device as an AC • Configure the anchor device as an AP • Manually configure the AP to act as a fit AP • Manually configure the AP to act as a fat AP • Manually configure the inside AP to act as a fat AP • Local AC image download • Device role changed from common to local • Device role changed from local to common • Device role changed from common to central • Device role changed from central to common • WT version changed • Cannot process subslot insert event • Cannot send subslot insert event to next step for processing

2.1.19 display wlan ap running-configuration

Syntax

display wlan ap { **all** | **name** *ap-name* } **running-configuration** [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

verbose: 詳細情報を表示します。

説明

display wlan ap running-configuration コマンドは指定した AP またはすべての AP のランニングコンフィグレーションを表示します。

例

#すべての AP の詳細なランニングコンフィグレーションを表示します。

<AC> display wlan ap running-configuration all verbose

```
(i) -- Inherited from AP group
(g) -- Inherited from AP global-configuration

#
wlan ap ap1 model QX-W1020 id 5
  ap group name 1
  serial-id 210235A1BSC123000050
  region code JP (g)
  echo interval 10 (i)
  retransmission count 3 (i)
  retransmission interval 5 (i)
  statistics interval 50 (i)
  jumbo frame 1500 (i)
  firmware update 1
  priority 4 (i)
...

  radio 1
    radio type 802.11ac (i)
    radio disable (i)
```

```
    channel auto<64> (i)
    channel unlock (i)
    max-power 11 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
…

  radio 2
    radio type 802.11n(2.4GHz) (i)
    radio disable (i)
    channel auto<11> (i)
    channel unlock (i)
    max-power 15 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
…

#
wlan ap ap2 model QX-W1020 id 6
  ap group name 2
  serialid
  region code JP (g)
  echo interval 10 (i)
  retransmission count 3 (i)
  retransmission interval 5 (i)
  statistics interval 50 (i)
  jumbo frame 1500 (i)
  firmware update 1
  priority 4 (i)
…

  radio 1
    radio type 802.11ac (i)
    radio disable (i)
    channel auto<60> (i)
    channel unlock (i)
    max-power 11 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
…
```

```
  radio 2
    radio type 802.11n(2.4GHz) (i)
    radio disable (i)
    channel auto<13> (i)
    channel unlock (i)
    max-power 15 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
...
```

2.1.20 display wlan ap statistics association-failure-record

Syntax

display wlan ap statistics association-failure-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap statistics association-failure-record コマンドは AP の関連付けに失敗した記録を表示します。

例

AP の関連付けに失敗した記録を表示します。

<AC> display wlan ap statistics association-failure-record

```
MAC address     AP ID   failed at           Reason
9a48-45ed-0300  12312   07-07/15:56:25      AP authentication failed
```

表 2-11 コマンド出力

フィールド	説明
MAC address	APのMACアドレスです。
AP ID	AC上のAPを一意的に識別するAPのIDです。
Last failure at	APがACと関連付けられた最後の時間です。フォーマットは date/hh:mm:ssです。

フィールド	説明
Reason	関連づけに失敗した理由です。 • メモリが十分でありません。 • APが存在しません。 • APのライセンスが足りません。 • MACアドレスが使用されています。 • APLBの追加に失敗しました。 • APが別のACを選択しました。 • ACでAPの最大数に到達しました。 • Run状態の加入要求を受信しました。 • APLBチェックに失敗しました。 • HA smoothのAPアクセスに拒否されました。 • AP認証に失敗しました。 • Auto APの作成に失敗しました。 • 手動APオンラインinfoチェックに失敗しました。 • インデックスの追加に失敗しました。 • APとACのバージョンがあっていません。 • 待ち要求タイマが終了しました。 • 失敗リザルトコードを受信しました。 • トンネルの追加に失敗しました。 • APの設定が見つかりません。 • AP IDが一致していません。 • APの基本ランニングデータの追加に失敗しました。

2.1.21 display wlan ap statistics image-download

Syntax

display wlan ap statistics image-download [failed | in-progress | succeeded]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

failed: イメージのダウンロードに失敗した AP を表示します。

in-progress: イメージをダウンロード中の AP を表示します。

succeeded: イメージのダウンロードが成功した AP を表示します。

説明

display wlan ap statistics image-download コマンドは AP イメージのダウンロード情報を表示します。

パラメータを指定しない場合、AP イメージのダウンロードに関する簡易情報を表示します。

例

#AP イメージのダウンロードに関する簡易情報を表示します。

<AC> display wlan ap statistics image-download

```
Completed : 50%
Time consumed : xxd hh:mm:ss
AP count:
 Total to download : 300
 Succeeded : 152
 In-progress : 140
 Failed : 8
```

表 2-12 コマンド出力

フィールド	説明
Completed	イメージのダウンロードが完了したAPの割合です。
Time consumed	イメージのダウンロードにかかった時間です。
Total to download	ソフトウェアを更新する必要があるAPの合計数です。
Succeeded	イメージのダウンロードに成功したAPの数です。
In-progress	イメージをダウンロード中のAPの数です。
Failed	イメージのダウンロードに失敗したAPの数。

#AP イメージをダウンロード中の AP を表示します。

<AC> display wlan ap statistics image-download in-progress

```
AP name                    Time consumed
ap6                            xxd 00:45:11
ap7                            N/A
ap8                            xxd 00:14:05
ap9                            xxd 01:16:09
....
------More----
```

表 2-13 コマンド出力

フィールド	説明
Time consumed	イメージのダウンロードにかかった時間です。 イメージをダウンロードしていない場合、このフィールドにはN/Aと表示されます。

#AP イメージのダウンロードに失敗した AP を表示します。

<AC> display wlan ap statistics image-download in-progress

```
AP name                  Failure reason
ap1                      Tunnel down
ap2                      AP memory not enough
ap3                      Image file does not exist
ap5                      Others
....
------More----
```

表 2-14 コマンド出力

フィールド	説明
Failure reason	イメージのダウンロードに失敗した理由: ● トンネルがダウンしました。 ● APのメモリが不足しています。 ● イメージファイルが存在しません。 ● 再送信に失敗しました。 ● その他。

#AP イメージのダウンロードが成功した AP を表示します。

<AC> display wlan ap statistics image-download succeeded

```
AP name                  Version              Download at
ap1                      7.2.59               11-25 01:10:15
ap2                      7.2.59               11-25 01:12:34
ap3                      7.2.59               11-25 01:14:21
ap5                      7.2.59               11-25 01:16:45
....
------More----
```

表 2-15 コマンド出力

フィールド	説明
Version	APイメージのソフトウェアバージョンです。

フィールド	説明
Download at	APイメージのダウンロードが成功した日時です。

2.1.22 display wlan ap statistics online-record

Syntax

display wlan ap statistics online-record [**time** *date time*] [**count** *count*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time *date time*: オンライン AP を記録する時間を指定します。*date* パラメータは YYYY/MM/DD あるいは MM/DD/YYYY のフォーマットです。YYYY パラメータの設定範囲は 2000～2035 です。MM パラメータの設定範囲は 1～12 です。DD パラメータは月を記載します。time パラメータは hh:mm のフォーマットです。hh パラメータの設定範囲は 0～23 です。mm パラメータの設定範囲は 0～59 です。パラメータを指定しない場合、降順で最近の 7 日のオンライン AP 数についての統計情報を表示します。

count *count*: オンライン AP 数を指定します。設定範囲は 1～256 です。指定しない場合、10 のオンライン AP 数の記録を表示します。

説明

display wlan ap statistics online-record コマンドはオンライン AP 数の記録を表示します。

オンライン AP 数の記録は 1 分の間隔で 1 つずつ表示されます。コマンドは最近の 7 日で生成された記録を表示します。*time* パラメータを指定した場合、指定した時間から生成された記録を表示します。

例

2017/10/11 10:25 後に生成されたオンライン AP 数の記録を 11 表示します。

<AC> display wlan ap statistics online-record time 2017/10/11 10:16:11 count 11

```
Time                 Manual APs      Auto APs       Total       Total delta
2017-10-11 10:16:00    20              10            30          -2
2017-10-11 10:17:00    22              10            32          +6
2017-10-11 10:18:00    16              10            26          0
2017-10-11 10:19:00    16              10            26          0
```

```
2017-10-11 10:20:00    16            10            26          0
2017-10-11 10:21:00    16            10            26          0
2017-10-11 10:22:00    16            10            26          0
2017-10-11 10:23:00    16            10            26          0
2017-10-11 10:24:00    16            10            26          0
2017-10-11 10:25:00    16            10            26          0
2017-10-11 10:26:00    16            10            26          0
```

表 2-16 コマンド出力

フィールド	説明
Time	記録が生成された日時です。
Manual APs	オンライン手動AP数です。
Auto APs	オンラインauto AP数です。
Total	オンラインAPの総数です。
Total delta	最後の1分での数の差分です。

2.1.23 display wlan ap tunnel-down-record

Syntax

display wlan ap tunnel-down-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap tunnel-down-record コマンドは CAPWAP トンネルダウンレコードを表示します。

例

CAPWAP トンネルダウンレコードを表示します。

<AC> display wlan ap tunnel-down-record

```
AP ID   AP name        Tunnel down at       Tunnel down reason
12321   9a48-45ed-0300    2017-07-07/15:56:25    Processed join request in Run
state
```

表 2-17 コマンド出力

フィールド	説明
AP ID	AC上のAPを一意的に識別するAPのIDです。
AP name	APの名前です。
Tunnel down at	APとAC間のCAPWAPトンネルがダウンした時刻です。形式は、date / hh：mm：ssです。
Tunnel down reason	CAPWAPトンネルダウン理由: ● タイマの作成に失敗しました。 ● 近隣デッドタイマが期限切れになりました。 ● 要求待ちタイマの有効期限が切れました。 ● データチェックタイマーの有効期限が切れました。 ● キープアライブメッセージの処理に失敗しました。 ● 要求の処理に失敗しました。 ● APはadminによってリセットされました。 ● APはCloudTunnelによってリセットされました。 ● APが削除されました。 ● オンラインにできませんでした。 ● シリアル番号が変更されました。 ● MACアドレスが変更されました。 ● AC最大能力を超過しました。 ● 実行状態中に結合要求されました。 ● APコンテキストの作成に失敗しました。 ● 失敗結果コードを受信しました。 ● メッセージの再送信に失敗しました。 ● イメージファイルのダウンロードに失敗しました。 ● イメージファイルが正常にダウンロードされました。 ● ファイル操作タイマの有効期限が切れました。 ● トンネルの追加に失敗しました。 ● APからのWTPトンネルダウンイベントを受信しました。 ● バックアップACがバックアップトンネルを閉じました。 ● マスタとバックアップトンネルの切り替えです。 ● 設定を継承できませんでした。 ● AP認証に失敗しました。 ● バックアップAPのアップグレードに失敗しました。 ● ボードはアクティブではありません。 ● APライセンスの欠如です。

2.1.24 display wlan ap-distribution

Syntax

display wlan ap-distribution all

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap-distribution コマンドは AC 用に接続された AP の配信情報を表示します。

例

AP の配信情報を表示します。

<AC> display wlan ap-distribution

```
Total number of APs: 1
                          AP information
 State : I = Idle,     J  = Join,      JA = JoinAck,    IL = ImageLoad
 C = Config,    DC = DataCheck,   R = Run,   M = Master,   B = Backup

AP name           APID   State   Model          Serial ID
722a-d561-0300      4     R/M    QX-W1020       210235A1BSC123000050
```

表 2-18 コマンド出力

フィールド	説明
APID	AC上のAPを一意的に識別するためのAPのIDです。

フィールド	説明
State	APの現在の状態: ● **I**－Idle ● **J**－Join ● **JA**－Join acknowledge ● IL－APがソフトウェアイメージバージョンをダウンロードしています。 ● C－APが初期設定をダウンロードしています。 ● DC－APがデータをチェックしています。 ● R－CAPWAPトンネルが動作しています。 これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● R / M－マスタCAPWAPトンネルが動作しています。 これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● R / B－バックアップCAPWAPトンネルが動作しています。 これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● M－APがマスタACに接続されています。 ● B－APがバックアップACに接続されています。
Model	APモデル情報です。
Serial ID	APのシリアルIDです。 APのシリアルIDが設定されていない場合、このフィールドには**Not configured**が表示されます。

2.1.25 display wlan ap-distribution ap-name

Syntax

display wlan ap-distribution ap-name *ap-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap-name: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap-distribution ap-name コマンドは AP の接続位置を表示します。

例

AP **ap1** の接続位置の場所を表示します。

<AC> display wlan ap-distribution ap-name ap1

```
The AP is not in run state.
```

2.1.26 display wlan ap-group

Syntax

display wlan ap-group [**brief** | **name** *group-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief: すべての AP group に関する簡易情報を表示します。

name *group-name*: 指定した AP group に関する詳細情報を表示します。*group-name* 引数は、1～31 文字の大文字小文字を区別しない AP group の名前を表します。

説明

display wlan ap-group コマンドはすべての AP group または指定した AP group に関する情報を表示します。

パラメータを指定しない場合、このコマンドはすべての AP group に関する詳細情報を表示します。

例

すべての AP group に関する詳細情報を表示します。

[AC] display wlan ap-group

```
Total number of AP groups: 2
AP group name      : default-group
Description        : Not configured
AP model           : Not configured
APs               : Not configured

AP group name      : group1
Description        : abcd
AP model           : QX-W1020
AP grouping rules:
  AP name          : ap1, ap2
  Serial ID        : 219801A0CNC138011454
  MAC address      : 0AFB-423B-893C
  IPv4 address     : Not configured
  IPv6 address     : Not configured
APs               : ap1 (AP name)
```

AP group **group1** に関する詳細情報を表示します。

[AC] display wlan ap-group group1

```
AP group name      : group1
Description        : Not configured
AP model           : QX-W1020
AP grouping rules:
  AP name          : ap1, ap2
  Serial ID        : 219801A0CNC138011454
  MAC address      : 0AFB-423B-893C
  IPv4 address     : Not configured
  IPv6 address     : Not configured
APs               : ap1 (AP name)
```

すべての AP group に関する簡易情報を表示します。

<AC> display wlan ap-group brief

```
Total number of AP groups: 4
AP group name              Group ID  Member APs   Online APs
default-group              1         1            0
group1                     2         2006         1986
group2                     3         10           10
group3                     4         4            4
```

関連コマンド

wlan ap-group

2.1.27 display wlan ap-model

Syntax

display wlan ap-model { **all** | **name** *model-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP モデルを指定します。

name *model-name*: AP モデルの名前を指定します。

説明

display wlan ap-model コマンドは AP モデル情報を表示します。

例

AP モデル **QX-W1020** に関する情報を表示します。

<AC> display wlan ap-model name QX-W1020

```
AP model       : QX-W1020
Alias          : QX-W1020
Vendor name    : NEC
Vendor ID      : 25506
License weight  : 100
Radio count    : 2
 Radio 1:
  Mode         : 802.11a, 802.11an, 802.11ac
  Default mode  : 802.11ac
  BSS count    : 16
 Radio 2:
  Mode         : 802.11b, 802.11g, 802.11gn
  Default mode  : 802.11gn
  BSS count    : 16
Version Support List :
 Hardware Version Ver.A:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.B:
```

```
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.C:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.D:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
 Hardware Version Ver.E:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
Hardware Version Ver.F:
  Software Version        : 7.1.0
  Default Software Version : 7.1.0
  Image Name              : qx-w1000-fit.ipe
```

表 2-19 コマンド出力

フィールド	説明
AP model	APモデル名です。
Alias	APモデルのエイリアスです。
License weight	APライセンスを使用したAPモデルの重み（パーセンテージ）です。
Radio count	無線の数です。
Mode	サポートされている無線タイプです。
Default mode	デフォルトの無線タイプです。
BSS count	無線がサポートするBSSの最大数です。
Software Version	APによって報告されたソフトウェアバージョンと比較するために使用されるAPのソフトウェアバージョンです。
Default Software Version	デフォルト値は、APDBに格納されているAPソフトウェアのバージョンです。
Image Name	APDBに格納されているAPソフトウェアのバージョンです。

2.1.28 display wlan ap tunnel latency

Syntax

display wlan ap name *ap-name* **tunnel latency**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap-name: AP 名を指定します。AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap name tunnel latency コマンドは AP のトンネル待ち時間情報を表示します。

このコマンドを実行する前に、CAPWAP トンネル待ち時間検出が開始されていることを確認してください。

例

AP **ap1** のトンネル待ち時間情報を表示します。

<AC> display wlan tunnel latency ap name ap1

```
AP name                          : ap1
Tunnel latency                    : Enabled
Control link delay:
  Current delay                   : 1ms
  Maximum delay                   : 1ms
  Minimum delay                   : 1ms
Data link delay:
  Current delay                   : 1ms
  Maximum delay                   : 1ms
  Minimum delay                   : 1ms
```

表 2-20 コマンド出力

フィールド	説明
Tunnel latency	• Disable • Enable
Current delay	最新の遅延です。

関連コマンド

- **reset wlan tunnel latency ap**
- **tunnel latency-detect**

2.1.29 display wlan device role

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.26 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan device role

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan device role コマンドは装置の動作モード情報を表示します。

Anchor-AC モードで動作している場合、「Anchor AC」と表示されます。

Anchor-FIT モードで動作している場合、「Anchor AP」と表示されます。

FAT モードで動作している場合、「FAT AP」と表示されます。

FIT モードで動作している場合、「FIT AP」と表示されます。

表 2-21 に、装置の動作モードと出力を示します。

表 2-21 装置の動作モードとコマンド出力

動作モード / AP モデル	FAT モード	Anchor-AC モード	Anchor-FIT モード	FIT モード
QX-W1000 シリーズ	FAT	Anchor AC	Anchor AP	FIT
QX-W1100 シリーズ (v7.2.27a を含む以前)	未サポート	未サポート	未サポート	FIT
QX-W1100 シリーズ (v7.2.30 を含む以降)	FAT	Anchor-AC	Anchor AP ※Anchor-FIT モードと FIT モードを統合	

例

装置の動作モード情報を表示します。

<AC> display wlan device role

```
Current running mode: Anchor AC.
```

2.1.30 download file

Syntax

download file *filename*

View

AP view

定義済みユーザロール

network-admin

パラメータ

filename: イメージファイル名を 1～255 文字で指定します。

説明

download file コマンドはイメージファイルを AP にダウンロードします。

🕮 **メモ：**

転送するファイルと同じ名称のファイルが AP にすでに存在する場合、ファイルの転送に失敗します。

例

#イメージファイル **main.ipe** を AP **ap1** にダウンロードします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan‑ap-ap1] download file main.ipe

2.1.31 echo-count

Syntax

echo-count *count*

undo echo-count

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、エコー要求の送信試行の最大回数は 3 回です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

count: エコー要求の送信試行の最大回数を 3～60 の範囲で指定します。

説明

echo-count コマンドはエコー要求の送信試行の最大回数を設定します。

undo echo-interval コマンドはデフォルトに戻します。

AP は、指定されたエコーインターバルでエコー要求を AC に送信し、CAPWAP 制御トンネルが正しく動作しているかどうかを識別します。AC は、エコー応答を送信することによって応答します。AP がキープアライブ時間内にエコー応答を受信しない場合、AP は接続を終了します。AC がキープアライブ時間内にエコー要求を受信しない場合、AC

は接続を終了します。キープアライブ時間は、エコー間隔にエコー要求の送信試行の最大回数を掛けたものです。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** のエコー要求送信試行の最大回数を 5 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] echo-count 5

AP group **group1** のエコー要求送信試行の最大回数を 5 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] echo-count 5

2.1.32 echo-interval

Syntax

echo-interval *interval*

undo echo-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view では、エコー要求を送信する間隔は 10 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: エコー要求を送信する間隔を 5～80 秒の範囲で指定します。

説明

echo-interval コマンドは AP が AC にエコー要求を送信する間隔を設定します。

undo echo-interval コマンドはデフォルトに戻します。

AP は、指定されたエコー間隔でエコー要求を AC に送信し、CAPWAP 制御トンネルが正しく動作しているかどうかを識別します。AC は、エコー応答を送信することによって応答します。AP から keepalive 時間内にエコー要求を受信しない場合、AC は接続を終了します。AP が keepalive 時間内にエコー応答を受信しない場合、AP は接続を終了します。keepalive 時間は、echo 間隔に **echo-count** *count* コマンドを使用して設定されたエコー要求送信の最大回数を掛けたエコー間隔です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** のエコー間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] echo-interval 15

AP group **group1** の AP のエコー間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] echo-interval 15

2.1.33 firmware-upgrade

Syntax

firmware-upgrade { **disable** | **enable** }

undo firmware-upgrade

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、global configuration view の設定を使用します。

global configuration view は、ソフトウェア更新機能が有効になっています。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: ソフトウェア更新機能を無効にします。

enable: ソフトウェア更新機能を有効にします。

説明

firmware-upgrade enable コマンドはソフトウェア更新機能を有効にします。

firmware-upgrade disable コマンドはソフトウェア更新機能を無効にします。

undo firmware-upgrade コマンドはデフォルトに戻します。

この機能により、AC は、AP のソフトウェアバージョンが、CAPWAP トンネル確立中に AC に格納されているハードウェアバージョンおよびソフトウェアバージョンマッピングと一致するかどうかを調べることができます。

- 一致が見つかった場合、AC は AP との CAPWAP トンネルを確立します。
- 一致するものが見つからない場合、CAPWAP トンネルの設定は次のように行われます。

a) ACはAPにソフトウェアのバージョンの不一致を通知します。

b) 通知を受信した後、APはソフトウェアバージョンをACから要求し、次にソフトウェアをアップグレードしてACとCAPWAPトンネルを確立します。

この機能が無効の場合、AC は AP のソフトウェアバージョンを調べず、AP と CAPWAP トンネルを直接確立します。

AP view の設定は、AP group view の設定よりも優先されます。AP group view の設定は、global configuration view の設定よりも優先されます。

例

AP **ap3** のソフトウェア更新機能を有効にします。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] firmware-upgrade enable

AP group **group1** の AP のソフトウェア更新機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] firmware-upgrade enable

#ソフトウェア更新機能をグローバルに有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] firmware-upgrade enable

関連コマンド

wlan apdb

2.1.34 fragment-size

Syntax

fragment-size { **control** *control-size* | **data** *data-size* }

undo fragment-size { **control** | **data** }

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、CAPWAP 制御パケットとデータパケットの最大フラグメントサイズは、それぞれ 1450 バイトと 1500 バイトです。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

control *control-size*: CAPWAP 制御パケットの最大フラグメントサイズをバイト単位で指定します。*control-size* 引数の値の範囲は 1000～1450 です。

data *data-size*: CAPWAP データパケットの最大フラグメントサイズをバイト単位で指定します。*control-size* 引数の値の範囲は 1000～1748 です。

説明

fragment-size コマンドは CAPWAP 制御またはデータパケットの最大フラグメントサイズを設定します。

undo fragment-size コマンドは設定を削除します。

このコマンドは、AP がインターネット経由で AC に接続する場合、中間装置が AC と AP 間でパケットをドロップすることを防ぎます。

フラグメントサイズの最大変更は、オンライン AP で直ちに有効になります。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **AP1** の CAPWAP データパケットの最大フラグメントサイズを 1500 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] fragment-size data 1500

AP group **group1** の CAPWAP データパケットの最大フラグメントサイズを 1500 バイトに設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] fragment-size data 1500

2.1.35 gigabitethernet

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

gigabitethernet *interface-number*

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

interface-number: インタフェース番号を指定します。値の範囲は、AP モデルによって異なります。

説明

gigabitethernet コマンドは AP の GigabitEthernet interface view に移行します。

例

AP view から GigabitEthernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1]

AP group1 の AP モデル view から GigabitEthernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-gigabitethernet-1]

2.1.36 hyprid-remote-ap

Syntax

hybrid-remote-ap { **disable** | **enable** }

undo hybrid-remote-ap

デフォルト

AP view は、AP group view の設定を使用します。

AP group view では、リモート AP は無効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: リモート AP 機能を無効にします。

enable: リモート AP 機能を有効にします。

説明

hybrid-remote-ap enable コマンドはリモート AP 機能を有効にします。

hybrid-remote-ap disable コマンドはリモート AP 機能を無効にします。

undo hybrid-remote-ap コマンドはデフォルトに戻します。

デフォルトでは、AP と AC 間のトンネルが切断された場合、AP はサービスの提供を停止します。この機能を有効にすると、AP はリモート AP として機能し、引き続きサービスを提供できます。

このコマンドは、ローカル転送モードで動作する AP でのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のリモート AP を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] hybrid-remote-ap enable

AP group **group1** 内の AP に対してリモート AP を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] hybrid-remote-ap enable

2.1.37 if-match ip

Syntax

if-match ip *ip-address* { *mask-length* | *mask* }

undo if-match ip [*ip-address* { *mask-length* | *mask* }]

デフォルト

IP アドレスによる AP グループルールは設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドット付き 10 進表記で IPv4 アドレスを指定します。

mask-length: マスクの長さを 1～31 の範囲で指定します。

mask: ドット付き 10 進表記でマスクを指定します。

説明

if-match ip コマンドは IPv4 アドレスによる AP グループルールを作成します。

undo if-match ip コマンドは IPv4 アドレスによる AP グループルールを削除します。

デフォルトの AP group view でこのコマンドを実行することはできません。

AP グループまたは異なる AP グループの IPv4 アドレスによる AP グループ化ルールは、互いに重複することはできません。

AP グループに設定できる IPv4 アドレスによる AP グループルールの設定可能数は、使用する Anchor-AC の AP モデル、ソフトウェアバージョンにより異なります。

- QX-W1030 Anchor-AC は、AP グループに設定できる IPv4 アドレスによる AP グループルールの設定可能数は最大 32 個です。
- QX-W1100 シリーズの Anchor-AC は、ソフトウェアバージョンにより AP グループに設定できる IPv4 アドレスによる AP グループルールの設定可能数が異なります。
  - □ ソフトウェアバージョン 7.2.85a を含む以前のソフトウェアでは、AP グループに最大 32 個ルールを設定できます。
  - □ ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアでは、AP グループに最大 64 個のルールを設定できます。

AP 名、シリアル ID、MAC アドレス、IPv4 アドレスによる AP グループルールの優先度は降順になっています。AP グループルールと一致しない AP は、デフォルトの AP グループに追加されます。

undo if-match ip コマンドを IPv4 アドレス未指定で実行すると、AP グループに設定されている IPv4 アドレスによる AP グルーピングルールをすべて削除します。

例

IP アドレスが **192.168.0.0/16** に属する AP を AP group **group1** に追加します。

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] if-match ip 192.168.0.0 16

2.1.38 keepalive-interval

Syntax

keepalive-interval *interval*

undo keepalive-interval

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、データトンネルキープアライブ間隔は 10 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: AP が CAPWAP データトンネルを介してキープアライブパケットを送信する間隔を指定します。値の範囲は 1～255 秒です。

説明

keepalive-interval コマンドはデータトンネルキープアライブ間隔を設定します。

undo keepalive-interval コマンドはデフォルトに戻します。

例

AP **ap1** のデータトンネルキープアライブ間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] keepalive-interval 15

AP group **1** のデータトンネルキープアライブ間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-ap-group-1] keepalive-interval 15

2.1.39 led-mode

Syntax

led-mode { **always-on** | **awake** | **normal** | **quiet** }

undo led-mode

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、LED 点灯モードは **normal** です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

always-on: LED が常に緑点灯するモードです。

awake: LED が 1 秒緑点灯、60 秒間消灯を繰り返すモードです。

normal: AP の動作状況ごとに LED の点灯・点滅パターンが変更するモードです。

quiet: LED が常に消灯するモードです。

🕮 **メモ**:

led-mode コマンドで設定できるのは、コンフィグが読み込まれた後の運用中の LED の点灯・点滅パターンです。起動中の LED の点灯・点滅パターンや、LED の色についてはインスタレーションマニュアルをご確認ください。

説明

led-mode コマンドは LED 点灯・点滅パターンを設定します。

undo led-mode コマンドはデフォルトの状態に戻します。デフォルトは normal です。

AP group view で LED 点灯モードを awake または always-on に設定すると、指定された LED 点灯モードをサポートするメンバ AP に対してのみ設定が有効になります。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の LED 点灯モードを **normal** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] led-mode normal

AP group **g1** の AP に対して LED 点灯モードを **awake** に設定します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] led-mode awake

2.1.40 mac-address(AP group view)

Syntax

mac-address *mac-address*

undo mac-address *mac-address*

デフォルト

MAC アドレスによる AP group ルールは設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを指定します。

説明

mac-address コマンドは MAC アドレスによる AP group ルールを作成します。

undo mac-address コマンドは MAC アドレスによる AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

複数の AP group ルールを MAC アドレスで設定できます。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先度は降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group の view でこのコマンドを実行することはできません。

例

AP group **group1** の MAC アドレスで AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] mac-address 0AC1-F9B2-B1C2

関連コマンド

wlan ap-group

2.1.41 mac-address(AP view)

Syntax

mac-address *mac-address*

undo mac-address

デフォルト

AP には MAC アドレスは指定されていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドは AP の MAC アドレスを指定します。

undo mac-address コマンドはデフォルトに戻します。

AP が AC と CAPWAP トンネルを確立している場合、AP の MAC アドレスを変更または削除すると CAPWAP トンネルが終了します。その後、AP は AC と CAPWAP トンネルを再確立します。

例

AP **ap1** の MAC アドレスを **0001-0000-0000** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] mac-address 0001-0000-0000

2.1.42 port access vlan

🕮 **メモ**:

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

AP の Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、AP 上のすべての access ポートが VLAN 1 に属します。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port access vlan コマンドは AP 上の access ポートを指定された VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

access ポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP **ap1** の Layer 2 Ethernet interface view で GigabitEthernet 1 を VLAN 3 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap3-gigabitethernet-1] port access vlan 3

AP グループ 1 のモデル **QX-W1020** の AP の Ethernet interface view で、GigabitEthernet 1 を VLAN 3 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port access vlan 3

関連コマンド

remote-configuration

2.1.43 port hybrid pvid

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

AP の Ethernet interface view では、hybrid ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、hybrid ポートの PVID は、リンクタイプがアクセスされているときにポートが属する VLAN の ID です。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port hybrid pvid コマンドは AP 上の hybrid ポートの PVID を設定します。

undo port hybrid pvid コマンドは AP の hybrid ポートの PVID を 1 に設定します。

存在しない VLAN を hybrid ポートの PVID として使用できます。**undo vlan** コマンドを使用して hybrid ポートの PVID を削除すると、ポートの PVID 設定は変更されません。

パケットを正しく送信するには、AP の hybrid ポートと AP に接続されたスイッチの hybrid ポートに同じ PVID を設定します。

hybrid ポートが PVID からパケットを送信できるようにするには、**port hybrid vlan** コマンドを使用して、hybrid ポートを PVID に割り当てる必要があります。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

GigabitEthernet 1 を hybrid ポートとして設定し、AP **ap1** の Layer 2 Ethernet interface view で PVID を VLAN 100 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-ap1-gigabitethernet-1] port hybrid pvid vlan 100

GigabitEthernet 1 を hybrid ポートとして設定し、AP グループ 1 のモデル **QX-W1020** の Layer 2 Ethernet interface view で PVID を VLAN 100 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port hybrid pvid vlan 100

関連コマンド

- **port hybrid vlan**
- **port link-type**
- **remote-configuration**

2.1.44 port hybrid vlan

🕮 メモ：

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

AP の Ethernet interface view では、hybrid ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、hybrid ポートは、そのリンクタイプがアクセスされているときにポートが属する VLAN のタグなしメンバです。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目をスペースで区切って指定します。各項目は、VLAN ID または VLAN ID の範囲を *vlan-id1*～*vlan-id2* の形式で指定します。VLAN ID の値の範囲は 1～4094 です。*vlan-id2* 引数の値は、*vlan-id1* 引数の値よりも小さくすることはできません。指定された VLAN は、装置上にすでに存在している必要があります。

tagged: 指定された VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: ポートを、指定された VLAN のタグなしメンバとして設定します。VLAN のタグなしメンバは、VLAN タグを削除した後、VLAN からパケットを送信します。

説明

port hybrid vlan コマンドは特定の VLAN に hybrid ポートを割り当てます。

undo port hybrid vlan コマンドは指定された VLAN から hybrid ポートを削除します。

hybrid ポートは、複数の VLAN を許可できます。hybrid ポートでこのコマンドを複数回実行すると、hybrid ポートは指定されたすべての VLAN を許可します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP ap1 の Layer 2 Ethernet interface view で、次の作業を実行します。

1) GigabitEthernet 1 を hybrid ポートとして設定します。
2) VLAN 100、タグ付きメンバとして VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-ap1-gigabitethernet-1] port hybrid vlan 2 4 50 to 100 tagged

AP グループ 1 のモデル **QX-W1020** の AP の Layer 2 Ethernet interface view では、次の作業を行います。

1) GigabitEthernet 1 を hybrid ポートとして設定します。
2) VLAN 100、タグ付きメンバとして VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- **port link-type**
- **remote-configuration**

2.1.45 port-isolate enable

メモ:

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port-isolate { **enable** | **disable** }

undo port-isolate

デフォルト

AP の Ethernet interface view では、AP は AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、ポートアイソレーションは有効です。

AP の aggregate interface view では、AP は AP グループの aggregate interface view の設定を使用します。

AP グループの aggregate interface view では、ポートアイソレーションは有効です。

View

AP の Ethernet interface view

AP group の Ethernet interface view

AP の aggregate interface view

AP group の aggregate interface view

定義済みユーザロール

network-admin

パラメータ

disable: ポートアイソレーションを無効にします。

enable: ポートアイソレーションを有効にします。

説明

port-isolate enable コマンドはポートアイソレーションを有効にします。

port-isolate disable コマンドはポートアイソレーションを無効にします。

undo port port-isolate コマンドはデフォルトに戻します。

Ethernet interface view での設定は、そのインタフェースにのみ適用されます。

aggregate interface view での設定は、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定の適用に失敗した場合、装置はどのアグリゲーションメンバポートもアイソレーショングループに割り当てません。設定の適用失敗がアグリゲーションメンバポートで起きた場合、装置は失敗が起きたポートをスキップし、別のアグリゲーションメンバポートをアイソレーショングループに割り当てます。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の GigabitEthernet 1 でポートアイソレーションを有効にします。

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap3-gigabitethernet-1] port-isolate enable

AP グループ 1 のモデル **QX-W1020** の GigabitEthernet 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port-isolate enable

AP ap1 のアグリゲートインタフェース Bridge-Aggregation 1 に対してポートアイソレーションを有効にします。

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] bridge-aggregation 1

[AC-wlan-ap-ap1-bridge-aggregation-1] port-isolate enable

AP グループ 1 のモデル **QX-W1020** のアグリゲートインタフェース Bridge-Aggregation 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-bridge-aggregation-1] port-isolate enable

関連コマンド

- **remote-configuration**
- **remote-configuration synchronize**

2.1.46 port link-aggregation group

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port link-aggregation group *group-id*

undo port link-aggregation

デフォルト

AP の Ethernet interface view では、AP は AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、インタフェースはアグリゲーショングループに所属していません。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

group-id: アグリゲーションインタフェースの番号でアグリゲーショングループを指定します。番号の範囲は装置のモデルにより異なります。

説明

port link-aggregation group コマンドはアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドはアグリゲーショングループからインタフェースを除外します。

1 つのアグリゲーショングループに割り当てられるイーサネットインタフェースは 1 つだけです。

アグリゲーショングループに参加すると、インタフェースはグループに設定された設定を引き継ぎます。

port link-aggregation group コマンドを実行する前に、指定したアグリゲーショグループが既に存在し、AP がアグリゲートインタフェースをサポートしていることを確認してください。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の GigabitEthernet 1 をアグリゲーショングループ 1 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-aggregation group 1

AP グループ 1 のモデル **QX-W1020** の GigabitEthernet 1 をアグリゲーショングループ 1 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-aggregation group 1

関連コマンド

- **remote-configuration**
- **remote-configuration synchronize**

2.1.47 port link-type

🕮 **メモ**：

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

AP の Ethernet interface view では、イーサネットポートは AP グループの Ethernet interface view で設定を使用します。

AP グループの Ethernet interface view では、各イーサネットポートは access ポートです。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートリンクタイプを access に設定します。

hybrid: ポートリンクタイプを hybrid に設定します。

trunk: ポートリンクタイプを trunk に設定します。

説明

port link-type コマンドは AP 上のイーサネットポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

イーサネットポートのリンクタイプを trunk から hybrid へ、またはその逆に変更するには、まずリンクタイプを access に設定します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP **ap1** の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

AP グループ 1 のモデル **QX-W1020** の AP の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type trunk

関連コマンド

remote-configuration

2.1.48 port trunk permit vlan

🕮 メモ：

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

AP の Ethernet interface view では、trunk ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、trunk ポートは VLAN 1 からのパケットだけを通過させます。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目をスペースで区切って指定します。各項目は、VLAN ID または VLAN ID の範囲を *vlan-id1*～*vlan-id2* の形式で指定します。VLAN ID の値の範囲は 1～4094 です。*vlan-id2* 引数の値は、*vlan-id1* 引数の値よりも小さくすることはできません。

all: すべての VLAN を指定します。

説明

port trunk permit vlan コマンドは指定された VLAN に trunk ポートを割り当てます。

undo port trunk permit vlan コマンドは指定された VLAN から trunk ポートを削除します。

trunk ポートは、複数の VLAN を許可できます。このコマンドを trunk ポート上で複数回実行すると、trunk ポートは指定されたすべての VLAN を許可します。

trunk ポートでは、PVID からのパケットだけがタグなしを通過できます。

許可されていない VLAN ユーザがポートを介して制限されたリソースにアクセスするのを防ぐには、**port trunk permit vlan all** コマンドを慎重に使用してください。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

GigabitEthernet 1 を trunk ポートとして設定し、AP **ap1** の Layer 2 Ethernet interface view で VLAN 100、VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-ap1-gigabitethernet-1] port trunk permit vlan 2 4 50 to 100

GigabitEthernet 1 を trunk ポートとして設定し、AP グループ 1 のモデル **QX-W1020** の AP の Ethernet interface view で VLAN 100、VLAN 2、VLAN 4、および VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port trunk permit vlan 2 4 50 to 100

関連コマンド

- **port link-type**
- **remote-configuration**

2.1.49 port trunk pvid

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

AP の Ethernet interface view では、trunk ポートは AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、trunk ポートの PVID は VLAN 1 です。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port trunk pvid コマンドは AP 上の trunk ポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

存在しない VLAN を trunk ポートの PVID として使用できます。**undo vlan** コマンドを使用して trunk ポートの PVID を削除すると、ポートの PVID 設定は変更されません。

パケットを正しく送信するには、AP の hybrid ポートと AP に接続されたスイッチの hybrid ポートに同じ PVID を設定します。

trunk ポートが PVID からパケットを送信できるようにするには、**port trunk permit vlan** コマンドを使用して、trunk ポートを PVID に割り当てる必要があります。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP **ap1** の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定し、PVID を VLAN 100 に設定し、VLAN 100 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap3-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-ap3-gigabitethernet-1] port trunk pvid vlan 100

[AC-wlan-ap-ap3-gigabitethernet-1] port trunk permit vlan 100

AP グループの Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定し、PVID を VLAN 100 に設定し、VLAN 100 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port trunk pvid vlan 100

[AC-wlan-ap-group-1-ap-model-QX-W1020-gigabitethernet-1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**
- **remote-configuration**

2.1.50 qos priority

🕮 **メモ**:

- このコマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

AP の Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、ポートプライオリティは 0 です。

AP の aggregate interface view では、AP グループの aggregate interface view の設定を使用します。

AP グループの aggregate interface view では、ポートプライオリティは 0 です。

View

AP の Ethernet interface view

AP グループの GigabitEthernet interface view

AP の aggregate interface view

AP グループの aggregate interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティを 0～7 の範囲で指定します。

説明

qos priority コマンドはポートプライオリティを設定します。

undo qos priority コマンドはデフォルトに戻します。

本設定は **remote-configuration synchronize** コマンドを実行したときにのみ、オンラインの AP に適用されます。

AP view の設定は AP group view の設定より優先されます。

例

AP の GigabitEthernet interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] qos priority 2

AP グループの GigabitEthernet interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-gigabitethernet-1] qos priority 2

AP の Layer 2 aggregate interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] interface bridge-aggregation 1

[AC-wlan-ap-ap1-Bridge-Aggregation1] qos priority 2

AP グループの Layer 2 aggregate interface view でポートプライオリティを 2 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] interface bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-Bridge-Aggregation1] qos priority 2

関連コマンド

remote-configuration synchronize

2.1.51 qos trust

🕮 **メモ：**

- このコマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

AP の Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP グループの Ethernet interface view では、設定されていません。

AP の aggregate interface view では、AP グループの aggregate interface view の設定を使用します。

AP グループの aggregate interface view では、設定されていません。

View

AP の Ethernet interface view

AP グループの Ethernet interface view

AP の aggregate interface view

AP グループの aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: 802.1p プライオリティをマッピングに使用します。

dscp: DSCP プライオリティをマッピングに使用します。

説明

qos trust コマンドはポートプライオリティを設定します。

undo qos trust コマンドはデフォルトに戻します。

本設定は **remote-configuration synchronize** コマンドを実行したときにのみ、オンラインの AP に適用されます。

AP view の設定は AP group view の設定より優先されます。

例

AP の GigabitEthernet interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] qos trust dot1p

AP グループの GigabitEthernet interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-gigabitethernet-1] qos trust dot1p

AP の Layer 2 aggregate interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] interface bridge-aggregation 1

[AC-wlan-ap-ap1-Bridge-Aggregation1] qos trust dot1p

AP グループの Layer 2 aggregate interface view で信頼されたパケットプライオリティタイプを dot1p に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1010

[AC-wlan-ap-group-1-ap-model-QX-W1010] interface bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1010-Bridge-Aggregation1] qos trust dot1p

関連コマンド

remote-configuration synchronize

2.1.52 remote-configuration

🕮 **メモ**：

remote-configuration を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

remote-configuration { **disable** | **enable** }

undo remote-configuration enable

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、リモート設定の割り当てが無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: リモート構成割り当て機能を無効にします。

enable: リモート構成割り当て機能を有効にします。

説明

> 🕮 **メモ：**
>
> このコマンドのサポートは、AP モデルによって異なります。

remote-configuration enable コマンドはリモート構成割り当て機能を有効にします。

remote-configuration disable コマンドはリモート構成割り当て機能を無効にします。

undo remote-configuration コマンドはデフォルトに戻します。

AC は、リモート設定割り当て機能がイネーブルになっている場合にのみ、関連する VLAN 設定を AP に割り当てます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のリモート設定割り当て機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] remote-configuration enable

APgroup **group1** のリモート設定割り当て機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] remote-configuration enable

2.1.53 remote-configuration synchronize

Syntax

remote-configuration synchronize

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、リモートコンフィグレーションシンクロナイゼーションは起動していません。

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

⚠ **注意：**

- このコマンドは、オンラインの AP のすべての VLAN、リンクアグリゲーション、ポート設定（ポートアイソレーション設定を除く）を削除し、AC で設定した設定内容を AP に反映させます。使用の際はご注意ください。
- AP が AC に接続された状態で、AP の設定内容を AC 上で変更した場合、**remote-configuration synchronize** コマンドを実行するまで変更内容が AP に反映されません。

remote-configuration synchronize コマンドは AC の設定を AP に同期します。

AP のコンフィグレーションファイルを更新するには、**map-configuration** コマンドを使用してコンフィグレーションファイルを AP に展開することができます。しかし、コンフィグレーションファイルを AP に展開する前に、そのファイルにコマンドを記述しておく必要があります。この方法は、時間がかかり、AP が数多く存在するネットワークでは適用できません。

本機能により、AC は VLAN、リンクアグリゲーション、ポートアイソレーションといった設定を、オンラインの AP に対して直接同期させることができます。

remote-configuration synchronize コマンドを使用する前に、**remote-configuration enable** が設定されていることを確認してください。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** に対してリモートコンフィグレーションシンクロナイゼーションを起動します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] remote-configuration synchronize

AP グループ **group1** の AP に対してリモートコンフィグレーションシンクロナイゼーションを起動します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] remote-configuration synchronize

関連コマンド

remote-configuration

2.1.54 reset wlan ap

Syntax

reset wlan ap { **all** | **name** *ap-name* | **model** *model-name* | **ap-group** *group-name* }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているすべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

model *model-name*: モデル名で AP モデルを指定します。

ap-group *group-name*: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

reset wlan ap コマンドはすべての AP または指定した AP をリセットします。このコマンドは、AP と AC 間の CAPWAP トンネルを終了し、AP に関するすべての接続情報を削除します。

例

AP **ap1** をリセットします。

<AC> reset wlan ap name ap1

```
Reset the AP that has established or is to establish a primary tunnel with the
AC. Continue? [Y/N]:
```

2.1.55 reset wlan ap reboot-log

Syntax

reset wlan ap reboot-log { **all** | **name** *ap-name* }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

reset wlan ap reboot-log コマンドはすべての AP または指定された AP の再起動ログを消去します。

例

AP **ap1** の再起動ログを削除します。

<AC> reset wlan ap reboot-log name ap1

関連コマンド

display wlan ap reboot-log

2.1.56 reset wlan tunnel latency ap

Syntax

reset wlan tunnel latency ap { **all** | **name** *ap-name* }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

reset wlan tunnel latency ap コマンドはすべての AP または指定された AP のトンネル待ち時間情報を消去します。

このコマンドは、マスタ AC とのトンネルを確立し、Run 状態の AP でのみ有効です。

例

AP **ap1** のトンネル待ち時間情報を削除します。

<AC> reset wlan tunnel latency ap name ap1

関連コマンド

- **display wlan tunnel latency ap name**
- **tunnel latency-detect**

2.1.57 retransmit-count

Syntax

retransmit-count *value*

undo retransmit-count

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、AC 要求再送信の最大試行回数は 3 回です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

value: AC 要求再送信の最大試行回数を 2～5 の範囲で指定します。

説明

retransmit-count コマンドは AC 要求の再送信の最大試行回数を設定します。

undo retransmit-count コマンドはデフォルトに戻します。

AC は、要求再送の最大試行回数に達するか応答が受信されるまで、再送信間隔で AP に送信された要求を送信します。

AC から AP に送信される要求には、次のタイプがあります。

- イメージデータ要求
- 設定更新要求
- リセット要求
- データ転送要求

- IEEE 802.11 WLAN 設定要求
- ステーション設定要求

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** の AC 要求の再送信の最大試行回数を 4 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] retransmit-count 4

AP group **group1** の AP の AC 要求再送信の最大試行数を 4 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] retransmit-count 4

関連コマンド

retransmit-interval

2.1.58 retransmit-interval

Syntax

retransmit-interval *interval*

undo retransmit-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、要求の再送信間隔は 5 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: 要求の再送信間隔を 3～8 秒の範囲で指定します。

説明

retransmit-interval コマンドは AC が AP への要求を再送信する間隔を設定します。

undo retransmit-interval コマンドはデフォルトに戻します。

AC から AP に送信される要求には、次のタイプがあります。

- イメージデータ要求
- 設定更新要求
- リセット要求
- データ転送要求
- IEEE 802.11 WLAN 設定要求
- ステーション設定要求

AP view の設定は、AP group view の設定よりも優先されます。

例

AC が AP **ap3** に要求を送信する際の、要求の再送信間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] retransmit-interval 6

AC が AP group **group1** 内の AP に要求を送信際の、要求の再送信間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] retransmit-interval 6

関連コマンド

retransmit-count

2.1.59 serial-id (AP group view)

Syntax

serial-id *serial-id*

undo serial-id *serial-id*

デフォルト

シリアル ID による AP group ルールは設定されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

serial-id: AP のシリアル ID を、大文字と小文字を区別しない 1～63 文字で指定します。

説明

serial-id コマンドはシリアル ID で AP group ルールを作成します。

undo serial-id コマンドはシリアル ID で AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

シリアル ID で複数の AP group ルールを設定できます。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先度は、降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group の view でこのコマンドを実行することはできません。

例

AP group **group1** のシリアル ID で AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] serial-id 210235A1BSC123000037

関連コマンド

wlan ap-group

2.1.60 serial-id (AP view)

Syntax

serial-id *serial-id*

undo serial-id *serial-id*

デフォルト

AP にシリアル ID は指定されていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

serial-id: AP のシリアル ID を、大文字と小文字を区別しない 1～63 文字で指定します。

説明

serial-id コマンドは AP のシリアル ID を指定します。

undo serial-id コマンドはデフォルトに戻します。

AP が AC との CAPWAP トンネルを確立している際に、AP のシリアル ID を変更または削除すると、CAPWAP トンネルが終了します。その後、AP は AC と CAPWAP トンネルを再確立します。

例

AP **ap1** のシリアル ID を **210235A1BSC123000050** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] serial-id 210235A1BSC123000050

2.1.61 snmp-agent trap enable wlan ap

Syntax

snmp-agent trap enable wlan ap

undo snmp-agent trap enable wlan ap

デフォルト

AP 管理の SNMP 通知は無効になっています。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan ap コマンドは AP 管理の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan ap コマンドはデフォルトに戻します。

重要な AP 管理イベントを NMS に報告するには、AP 管理の SNMP 通知を有効にします。AP 管理イベント通知が正しく送信されるようにするには、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* の説明に従って SNMP も設定する必要があります。

例

AP 管理の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan ap

2.1.62 snmp-agent trap enable wlan capwap

Syntax

snmp-agent trap enable wlan capwap

undo snmp-agent trap enable wlan capwap

デフォルト

CAPWAP の SNMP 通知は無効になっています。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan capwap コマンドは CAPWAP の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan capwap コマンドはデフォルトに戻します。

重要な CAPWAP イベントを NMS に報告するには、CAPWAP の SNMP 通知を有効にします。CAPWAP イベント通知が正しく送信されるようにするには、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* の説明に従って SNMP も設定する必要があります。

例

CAPWAP の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan capwap

2.1.63 statistics-interval

Syntax

statistics-interval *interval*

undo statistics-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、統計値報告間隔は 50 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: 統計値報告間隔を 0～240 秒の範囲で指定します。AP の統計値報告を無効にするには、統計値報告間隔を 0 に設定します。

説明

statistics-interval コマンドは AP が統計値報告を AC に送信する間隔を設定します。

undo statistics-interval コマンドはデフォルトに戻します。

このコマンドを実行すると、AP が統計情報を報告する間隔を変更できます。これらの統計情報を使用して、AP 上の無線の動作ステータスを監視できます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の統計値報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] statistics-interval 10

AP group **group1** の AP の統計値報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] statistics-interval 10

2.1.64 tunnel encryption

Syntax

tunnel encryption { **disable** | **enable** }

undo tunnel encryption enable

デフォルト

AP view：AP group view の設定を使用

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: CAPWAP 制御トンネル暗号化を無効にします。

enable: CAPWAP 制御トンネル暗号化を有効にします。

説明

tunnel encryption enable コマンドは CAPWAP 制御トンネル暗号化を有効にします。

tunnel encryption disable コマンドは CAPWAP 制御トンネル暗号化を無効にします。

undo tunnel encryption enable コマンドはデフォルトに戻します。

本コマンド適用時、CAPWAP トンネルが再接続されます。

本機能を有効にすると、AP は AC から暗号化フラッグがついた検出応答を受信したとき、AC と CAPWAP トンネルを確立します。CAPWAP トンネル確立されると、DTLS ハンドシェークのあとに AC と AP は CAPWAP 制御トンネル内で転送された制御パケットを暗号化します。

AP view の設定は AP group view の設定より優先されます。

例

AP **ap1** に対して CAPWAP 制御トンネル暗号化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] tunnel encryption enable

```
This operation will restart the AP. Continue? [Y/N]
```

APgroup **group1** に CAPWAP 制御トンネル暗号化を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] tunnel encryption enable

```
This operation will restart member APs that are not enabled with CAPWAP control
tunnel encryption. Continue? [Y/N]
```

2.1.65 tunnel latency-detect

Syntax

tunnel latency-detect { **start** | **stop** }

デフォルト

CAPWAP トンネル待ち時間検出は開始されません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

start: CAPWAP トンネル待ち時間検出は開始します。

stop: CAPWAP トンネル待ち時間検出は停止します。

説明

tunnel latency-detect コマンドは CAPWAP トンネル待ち時間検出を設定します。

CAPWAP トンネル待ち時間検出により、CAPWAP 制御フレームもしくは AP から AC へのデータフレームおよびその逆方向通信の送信待ち時間を検出できます。

AP がオフラインのとき、CAPWAP トンネル待ち時間検出は自動的に停止します。AP が再びオンラインになると、**tunnel latency-detect start** コマンドを実行して、CAPWAP トンネル待ち時間検出を再始動させる必要があります。

tunnel latency-detect start コマンドは、マスタ AC との CAPWAP トンネルを確立し、Run 状態にある AP でのみ有効です。

例

AP **ap1** の CAPWAP トンネル待ち時間検出を開始します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] tunnel latency-detect start

関連コマンド

- **display wlan tunnel latency ap name**
- **reset wlan tunnel latency ap**

2.1.66 usb

Syntax

usb { **disable** | **enable** }

undo usb

デフォルト

AP view では、AP は AP group's AP model view で設定を使用します。

AP group's AP model view では、USB インタフェースが無効になっています。

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

disable: AP 上の USB インタフェースを無効にします。

enable: AP 上の USB インタフェースを有効にします。

説明

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

usb enable コマンドは AP 上の USB インタフェースを有効にします。

usb disable コマンドは AP 上の USB インタフェースを無効にします。

undo usb コマンドはデフォルトに戻します。

このコマンドは、次のいずれかの要件が満たされている場合にのみ、AP で有効になります。

- AP の電力レベルが高い。
- AP の電力レベルは中程度で、MIMO モードは 1×1 です。

AP view の設定は、AP group's AP model view の設定よりも優先されます。

例

AP view で USB インタフェースを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] usb enable

AP group **g1** の AP model view で USB インタフェースを有効にします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1020

[AC-wlan-ap-group-g1-ap-model-QX-W1020] usb enable

関連コマンド

power-level default

2.1.67 vlan

🕮 **メモ：**

このコマンドは **remote-configuration** コマンドにて設定可能です。

Syntax

vlan *vlan-id1* [**to** *vlan-id2*]

undo vlan *vlan-id1* [**to** *vlan-id2*]

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、VLAN 1（デフォルト VLAN）が AP に存在します。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

vlan-id1: VLAN ID を 1～4094 の範囲で指定します。

vlan-id1 **to** *vlan-id2*: VLAN 範囲を指定します。*vlan-id1* および *vlan-id2* 引数は VLAN ID を指定します。2 つの引数の値の範囲は 1～4094 です。*vlan-id2* 引数の値は、*vlan-id1* 引数の値よりも小さくすることはできません。

all: 予約済み VLAN を除くすべての VLAN を指定します。このキーワードは、AP で作成できる VLAN の最大数が 4094 未満の場合はサポートされません。このキーワードのサポートは、AP モデルによって異なります。

説明

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

vlan *vlan-id* コマンドは AP の VLAN を作成し、AP の VLAN view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは予約済み VLAN を除き、AP の VLAN *vlan-id1*～*vlan-id2* を作成します。

vlan all コマンドは AP の VLAN 1～4094 を作成します。

undo vlan コマンドは AP の指定された VLAN を削除します。

VLAN 1（デフォルト VLAN）または予約済み VLAN を作成または削除することはできません。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** の VLAN 2 を作成し、VLAN の VLAN view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] vlan 2

[AC-wlan-ap-ap1-vlan2]

APgroup **group1** の VLAN 2 を作成し、VLAN の VLAN view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] vlan 2

[AC-wlan-ap-group-1-vlan2]

関連コマンド

remote-configuration

2.1.68 wlan ap

Syntax

wlan ap *ap-name* { **model** *model-name* }

undo wlan ap *ap-name*

デフォルト

手動 AP は存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ap-name: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

model *model-name*: AP のモデル名を指定します。AP を作成するときは、モデル名を指定する必要があります。

表 2-22 に装置で指定可能な AP モデル名を示します。

表 2-22 wlan ap コマンドで指定可能な AP モデル名

指定可能な AP モデル / Anchor-AC モードの AP モデル	QX-W1010 QX-W1020 QX-W1030	QX-W1110	QX-W1120	QX-W1130
QX-W1030 の場合	指定可能	管理対象外	管理対象外	管理対象外
QX-W1110 の場合	指定可能	指定可能	指定可能	指定可能
QX-W1120 の場合	指定可能 (v7.2.47 以降)	指定可能 (V7.2.55 以降)	指定可能	指定可能
QX-W1130 の場合	指定可能 (v7.2.47 以降)	指定可能 (V7.2.55 以降)	指定可能	指定可能

説明

wlan ap コマンドは AP を作成し AP view へ移行します。

undo wlan ap コマンドは AP を削除します。

指定された AP がすでに存在する場合、AP view に入ります。

指定された AP が CAPWAP トンネルを確立している場合、undo wlan ap コマンドはトンネルも終了します。

例

QX-W1020 モデルで AP **ap1** を作成します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1]

2.1.69 wlan apdb

Syntax

wlan apdb *model-name hardware-version software-version*

undo wlan apdb *model-name hardware-version*

デフォルト

AP モデルのハードウェアバージョンに対するソフトウェアバージョンは、APDB ユーザスクリプト内に記憶されているソフトウェアバージョンです。

View

System view

定義済みユーザロール

network-admin

パラメータ

model-name: APDB の AP モデル名を指定します。

hardware-version: APDB のハードウェアバージョンを指定します。

software-version: AP ソフトウェアバージョンを大文字と小文字を区別しない 1～31 文字で指定します。

説明

⚠ **注意**：

CAPWAP トンネルの確立に失敗しないようにするには、NEC サポートの案内に従ってこのコマンドを使用してください。

wlan apdb コマンドは AP モデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定します。

undo wlan apdb コマンドはデフォルトに戻します。

APDB には、AP モデルのハードウェアバージョンに対するソフトウェアバージョンのマッピングが記憶されています。このコマンドを使用して、ソフトウェア更新用の AP モデルのハードウェアバージョンに対するソフトウェアバージョンを再指定することができます。ソフトウェア更新機能は、AP がオンラインになったときに、このコマンドで指定されたソフトウェアバージョンにソフトウェアを更新します。

例

APDB 内の AP モデル QX-W1020 のハードウェアバージョン **Ver.C** に対するソフトウェアバージョンを E2108 に指定します。

<AC> system-view

[AC] wlan apdb QX-W1020 Ver.C E2108

関連コマンド

firmware-upgrade

2.1.70 wlan apdb file

Syntax

wlan apdb file *user.apdb*

undo wlan apdb file

デフォルト

APDB ユーザスクリプトはロードされません。

View

System view

定義済みユーザロール

network-admin

パラメータ

user.apdb: APDB ユーザープロファイルを名前で指定します。大文字と小文字が区別される 1～63 文字です。apdb はファイル名の拡張子です。

説明

wlan apdb file コマンドは APDB ユーザスクリプトをロードします。

undo wlan apdb file コマンドは APDB ユーザスクリプトを削除します。

このコマンドは、ユーザスクリプト内の AP モデル情報を APDB に追加します。

AC 上で複数のユーザスクリプトをロードする場合、直近でロードされたユーザスクリプトは、古いユーザスクリプトを上書きします。

以下の状況下で新たなユーザスクリプトをロードするために、各状況に応じて以下の操作のいずれかを実行します。

- 手動 AP または、古いユーザスクリプト内にモデルが記載されているオンラインの自動 AC が存在するとき、AC 上で一致する AP モデル情報を削除します。
- AP がすでに AP group に追加されている場合、古いユーザスクリプト内にモデルが記載されている AP を、AP group から取り除きます。
- 古いユーザスクリプトが、ソフトウェアバージョンがすでに設定された AP モデルを含む場合、元のソフトウェアバージョンを復元するために **wlan apdb** コマンドを使用します。

ファイルシステム内のユーザスクリプトを修正または削除する場合、AC は再起動後ユーザスクリプト内の AP モデルの設定を失います。

例

#ユーザスクリプト **user.apdb** をロードします。

<AC> system-view

[AC] wlan apdb file user.apdb

関連コマンド

wlan apdb

2.1.71 wlan ap-group

Syntax

wlan ap-group *group-name*

undo wlan ap-group *group-name*

デフォルト

デフォルトの AP group **default-group** が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

wlan ap-group コマンドは AP group を作成します。

undo wlan ap-group コマンドは AP group を削除します。

指定された AP group が存在する場合、AP group view に移行します。

デフォルトの AP group は削除できません。

例

group1 という名前の AP group を作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1]

関連コマンド

display wlan ap-group

2.1.72 wlan ap-image-deploy

🕮 **メモ：**

- このコマンドは、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
- このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan ap-image-deploy { **all** | **name** *ap-name* | **ap-group** *group-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているすべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

ap-group *group-name*: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

wlan ap-image-deploy コマンドはオンライン状態の AP にイメージファイルを展開します。展開したソフトウェアを有効にするためには AP を再起動する必要があります。

このコマンドを実行する前に、AC のストレージメディアにイメージファイルをアップロードする必要があります。**wlan image-load filepath** コマンドを実行して、ストレージメディアを指定できます。

例

#すべてのオンライン状態の AP にイメージファイルを展開します。

<Sysname> system-view
[Sysname] wlan ap-image-deploy all

関連コマンド

wlan image-load filepath

2.1.73 wlan auto-ap enable

Syntax

wlan auto-ap enable

undo wlan auto-ap enable

デフォルト

自動 AP 機能は無効です。

View

System view

定義済みユーザロール

network-admin

説明

wlan auto-ap enable コマンドは自動 AP 機能を有効にします。

undo wlan auto-ap enable コマンドは自動 AP 機能を無効にします。

自動 AP 機能により、AP は手動 AP 設定なしで AC に接続可能となります。数多くの AP を WLAN 内に配置する際の設定が単純化されます。

自動 AP を設定するために、自動 AP を手動 AP に変換するための自動 AP パーシステンスを使用するか、もしくは AP group を通じてそれを設定しなければなりません。

例

#自動 AP 機能を有効にします。

<AC> system-view

[AC] wlan auto-ap enable

2.1.74 wlan auto-ap persistent

Syntax

wlan auto-ap persistent { **all** | **name** *auto-ap-name* [*new-ap-name*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべてのオンライン自動 AP を指定します。このキーワードを指定すると、コマンドはすべてのオンライン自動 AP を名前が変更されていない手動 AP に変換します。

auto-ap-name: オンライン自動 AP を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

new-ap-name: 新しい AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。指定しない場合、変換された手動 AP は自動 AP の名前を使用します。

説明

wlan auto-ap persistent コマンドはオンライン自動 AP を手動 AP に変換します。

例

MAC アドレスが 0afb-4212-cd36 の自動 AP を手動 AP **ap2** に変換します。

<AC> system-view

[AC] wlan auto-ap persistent name 0afb-4212-cd36 ap2

2.1.75 wlan auto-persistent enable

Syntax

wlan auto-persistent enable

undo wlan auto-persistent enable

デフォルト

自動 AP パーシステンスは無効です。

View

System view

定義済みユーザロール

network-admin

説明

wlan auto-persistent enable コマンドは自動 AP パーシステンスを有効しオンラインになった後に自動 AP を自動的に手動 AP に変換します。

undo wlan auto-persistent enable コマンドはデフォルトに戻します。

このコマンドは、コマンドを実行した後にオンラインになった自動 AP でのみ有効です。すでにオンラインになっている自動 AP の場合は、**wlan auto-ap persistent** コマンドを使用して、手動 AP に変換します。

例

#自動 AP パーシステンスを有効にします。

<AC> system-view

[AC] wlan auto-persistent enable

2.1.76 wlan capwap discovery-policy unicast

Syntax

wlan capwap discovery-policy unicast

undo wlan capwap discovery-policy

デフォルト

AC は、ユニキャスト、マルチキャスト、ブロードキャストの発見要求に応答できます。

View

System view

定義済みユーザロール

network-admin

説明

wlan capwap discovery-policy unicast コマンドは AC がユニキャスト発見要求にのみ応答するようにします。

undo wlan capwap discovery-policy コマンドはデフォルトに戻します。

例

AC がユニキャスト発見要求にのみ応答するようにします。

<AC> system-view

[AC] wlan capwap discovery-policy unicast

2.1.77 wlan global-configuration

Syntax

wlan global-configuration

View

System view

定義済みユーザロール

network-admin

説明

wlan global-configuration コマンドは global configuration view へ移行します。

AP view、AP group view、global configuration view での AP の設定の優先度は降順です。1 つの view で設定が構成されていない場合は、優先度の低い view の設定が使用されます。3 つの view の全てに設定がされていない場合、AP は最も優先度の低い view のデフォルト設定を使用します。

例

global configuration view へ移行します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration]

2.1.78 wlan image-load filepath

🕮 **メモ：**

- このコマンドは Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
- このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan image-load filepath { **local** | **ram** }

undo wlan image-load filepath

View

System view

定義済みユーザロール

network-admin

パラメータ

local:AP イメージファイルを優先して取得する場所としてローカルフォルダを指定します。ローカルフォルダに AP イメージファイルが含まれていない場合、AC は RAM から

AP イメージファイルを取得します。RAM に AP イメージファイルが含まれていない場合、AC は AP イメージファイルを取得することはできません。

ram：AP イメージファイルを優先して取得する場所として RAM を指定します。RAM に AP イメージファイルが含まれていない場合、AC はローカルフォルダから AP イメージファイルを取得します。ローカルフォルダに AP イメージファイルが含まれていない場合、AC は AP イメージファイルを取得することはできません。

説明

AC のイメージファイルには AP イメージファイルが含まれています。AC は、起動時に AP イメージファイルを RAM に読み込みます。

local キーワードは、次の条件を満たす場合にだけ指定します。

- 必要な AP イメージファイルが AC のイメージファイルに含まれていない。
- AP がオンラインになるときに使用するソフトウェアバージョンが、wlan apdb コマンドを使用して指定されている。

local キーワードを指定する場合は、AC がデフォルトのファイルシステムとして CF またはフラッシュカードを使用し、AP イメージファイルが AC 上のファイルシステムのルートディレクトリに保存されていることを確認してください。

AC は、. ipe の AP イメージファイルのみを AP に割り当てることができます。

例

#AP イメージファイルを優先して取得する場所として、AC のローカルフォルダを指定します。

<Sysname> system-view
[Sysname] wlan image-load filepath local

2.1.79 wlan re-group

Syntax

wlan re-group { **ap** *ap-name* | **ap-group** *old-group-name* | **mac-address** *mac-address* | **serial-id** *serial-id* } *group-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

ap-group *old-group-name*: 送信元 AP group を指定します。送信元 AP group をデフォルト AP group にすることはできません。

mac-address *mac-address*: MAC アドレスで AP group ルールを指定します。

serial-id *serial-id*: シリアル ID で AP group ルールを指定します。

group-name: 宛先 AP group を指定します。宛先 AP group をデフォルト AP group にすることはできません。

説明

wlan re-group コマンドは AP group ルールまたは AP group ルールのリストを指定された AP group に移動します。

例

AP group **group1** を作成し、ap1、ap2、ap3 という AP 名で AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap ap1 ap2 ap3

[AC-wlan-ap-group-group1] quit

#AP group **group2** を作成し、AP 名で AP group ルールを group2 に移動します。

[AC] wlan ap-group group2

[AC-wlan-ap-group-group2] quit

[AC] wlan re-group ap ap1 group2

2.1.80 wlan rename-ap

Syntax

wlan rename-ap *ap-name new-ap-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap-name: 手動 AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

new-ap-name: 新しい AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

wlan rename-ap コマンドは手動 AP の名前を変更します。

例

AP **ap1** の名前を **ap1-office** に変更します。

<AC> system-view

[AC] wlan rename-ap ap1 ap1-office

2.1.81 wlan save ap-configuration

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。

Syntax

wlan save ap-configuration { **all** | **ap-group** *group-name* | **name** *ap-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているオンライン状態のすべての AP を指定します。

ap-group *group-name*: AP group 内のオンライン状態の AP を指定します。*group-name* は大文字と小文字を区別しない 1～31 文字です。

name *ap-name*: オンライン状態の AP を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列で、大文字と小文字を区別します。

説明

wlan save ap-configuration コマンドは、指定した AP、AP グループ、または全てのオンライン状態の AP を対象に、現在のコンフィグを AP 上に保存し、次回の起動に使用するスタートアップコンフィグレーションファイルとして設定します。

例

全てのオンライン状態の AP の現在のコンフィグを保存します

<AC> system-view

[AC] wlan save ap-configuration all

This operation will save the configuration of ap. Continue? [Y/N]: y

[AC]

2.1.82 wlan timezone-sync enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。

Syntax

wlan timezone-sync enable

undo wlan timezone-sync enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan timezone-sync enable コマンドはタイムゾーンの同期を有効にします。

undo wlan timezone-sync enable コマンドはタイムゾーンの同期を無効にします。。

例

タイムゾーンの同期を有効にします。

<AC> system-view

[AC] wlan timezone-sync enable

目次

3 章 無線管理の設定 3-1
3.1 無線管理の設定コマンド 3-1
3.1.1 a-mpdu 3-1
3.1.2 a-msdu 3-2
3.1.3 ani 3-3
3.1.4 auto-channel european-gap enable 3-4
3.1.5 beacon-interval 3-5
3.1.6 bss-color 3-6
3.1.7 channel 3-8
3.1.8 channel auto-select 3-9
3.1.9 channel band-width 3-11
3.1.10 channel-usage measure 3-12
3.1.11 channel-usage threshold 3-13
3.1.12 client dot11ac-only 3-14
3.1.13 client dot11ax-only 3-15
3.1.14 client dot11b-forbidden 3-16
3.1.15 client dot11n-only 3-17
3.1.16 client max-count 3-19
3.1.17 continuous-mode 3-20
3.1.18 display wlan ap continuous-mode 3-21
3.1.19 display wlan ap radio 3-22
3.1.20 display wlan ap radio channel 3-24
3.1.21 display wlan ap radio type 3-25
3.1.22 display wlan statistics ap radio 3-26
3.1.23 distance 3-41
3.1.24 dl-ofdma 3-42
3.1.25 dot11ac mandatory maximum-nss 3-43
3.1.26 dot11ax mandatory maximum-nss 3-45
3.1.27 dot11ac multicast-nss 3-46
3.1.28 dot11ax multicast-nss 3-47
3.1.29 dot11ac support maximum-nss 3-48
3.1.30 dot11ax support maximum-nss 3-49
3.1.31 dot11g protection 3-50
3.1.32 dot11n mandatory maximum-mcs 3-52
3.1.33 dot11n multicast-mcs 3-53
3.1.34 dot11n protection 3-54
3.1.35 dot11n support maximum-mcs 3-56

3.1.36 dtim 3-57
3.1.37 fragment-threshold 3-59
3.1.38 green-energy-management 3-60
3.1.39 ldpc 3-61
3.1.40 long-retry threshold 3-62
3.1.41 max-power 3-63
3.1.42 mu-txbf 3-65
3.1.43 power-lock 3-67
3.1.44 preamble 3-68
3.1.45 protection-mode 3-69
3.1.46 protection-threshold 3-71
3.1.47 radar-channel-switchback disable 3-72
3.1.48 radio 3-73
3.1.49 radio { disable | enable } 3-74
3.1.50 radio-type 2.4g 3-75
3.1.51 radio-type 5g 3-76
3.1.52 rate 3-77
3.1.53 reset wlan statistics ap radio 3-79
3.1.54 short-gi 3-80
3.1.55 short-retry threshold 3-81
3.1.56 stbc 3-82
3.1.57 su-txbf 3-84
3.1.58 twt negotiate 3-85
3.1.59 type 3-87
3.1.60 ul-ofdma 3-89
3.1.61 wlan radio 3-90

3章 無線管理の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

3.1 無線管理の設定コマンド

3.1.1 a-mpdu

Syntax

a-mpdu { **disable** | **enable** }

undo a-mpdu

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、A-MPDU アグリゲーション手法は有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: A-MPDU アグリゲーション手法を無効にします。

enable: A-MPDU アグリゲーション手法を有効にします。

説明

a-mpdu enable コマンドは A-MPDU アグリゲーション手法を有効にします。

a-mpdu disable コマンドは A-MPDU アグリゲーション手法を無効にします。

undo a-mpdu コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac、802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、A-MPDU アグリゲーション手法を無効化します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] a-mpdu disable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、A-MPDU アグリゲーションを無効化します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] a-mpdu disable

3.1.2 a-msdu

Syntax

a-msdu { **disable** | **enable** }

undo a-msdu

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、A-MSDU アグリゲーション手法は有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: A-MSDU アグリゲーション手法を無効にします。

enable: A-MSDU アグリゲーション手法を有効にします。

説明

a-msdu enable コマンドは A-MSDU アグリゲーション手法を有効にします。

a-msdu disable コマンドは A-MSDU アグリゲーション手法を無効にします。

undo a-msdu コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac、802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g に変更すると、コマンドが無効になります。

装置は A-MSDU を受信することができますが、送信することはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、A-MSDU アグリゲーション手法を無効化します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] a-msdu disable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、A-MPDU アグリゲーションを無効化します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] a-msdu disable

3.1.3 ani

Syntax

ani { **disable** | **enable** }

undo ani

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ANI は有効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: ANI（Adaptive Noise Immunity）を無効にします。

enable: ANI（Adaptive Noise Immunity）を有効にします。

説明

ani enable コマンドは ANI（Adaptive Noise Immunity）を有効にします。

ani disable コマンドは ANI（Adaptive Noise Immunity）を無効にします。

undo ani コマンドはデフォルトに戻します。

ANI は周辺環境からの干渉を減少させるために、環境に基づいた騒音防止レベルを調整できるようにします。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、ANI を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] ani enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、ANI を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] ani enable

3.1.4 auto-channel european-gap enable

Syntax

auto-channel european-gap enable

undo auto-channel european-gap enable

デフォルト

2.4GHz 無線ではヨーロッパ以外のチャネルギャップ 5 を使用して、チャネル 1,6,11 を自動的に選択します。

View

Global configuration view

定義済みユーザロール

network-admin

説明

auto-channel european-gap enable コマンドは 2.4GHz 無線を設定して、ヨーロッパのギャップを自動チャネル選択に使用します。

undo auto-channel european-gap enable コマンドはデフォルトに戻します。

2.4GHz 無線でヨーロッパチャネルギャップ 6 を使用してチャネル 1,7、および 13 を自動的に選択するには、このコマンドを設定します。

例

自動チャネル選択のためにヨーロッパのチャネルギャップを使用するように 2.4 GHz 無線を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] auto-channel european-gap enable

関連コマンド

channel

3.1.5 beacon-interval

Syntax

beacon-interval *interval*

undo beacon-interval

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ビーコン間隔は 100TU(Time Unit)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

interval: ビーコン間隔を 32TU から 8191TU の範囲で指定します。

説明

beacon-interval コマンドはビーコン間隔を設定します。

undo beacon-interval コマンドはデフォルトに戻します。

例

AP **ap1** のビーコン間隔を 1000TU に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] beacon-interval 1000

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、ビーコン間隔を 1000TU に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] beacon-interval 1000

3.1.6 bss-color

🕮 **メモ**:

- **bss-color** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **bss-color** コマンドは QX-W1100 シリーズの AP でのみサポートしています。

Syntax

bss-color { **disable** | **enable** }

undo bss-color

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン V7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

bss-color enable コマンドは BSS カラーリングを有効にします。

bss-color disable コマンドは BSS カラーリングを無効にします。

undo bss-color コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

BSS カラーリングを使用すると、システムは各 BSS にカラーを割り当て、クライアントへのデータパケットにカラーID を含めることができます。データパケットにカラーID が含まれることで、クライアントは関連付いた AP からパケットが送信されたかどうかを識別できます。衝突を避けるために、関連付けられた BSS と同じカラーの 802.11 ax データパケットを検出したクライアントは送信を延期します。

高密度環境で BSS カラーリングを有効にすると、システムパフォーマンスとチャネル使用率が向上します。

Radio view の設定は AP group radio view の設定よりも優先されます。

例

AP **ap1** の Radio1 で BSS カラーリングを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] bss-color enable

AP グループ **apgroup1** の AP の Radio1 で BSS カラーリングを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] bss-color enable

関連コマンド

type dot11ax

3.1.7 channel

Syntax

channel { *channel-number* | **auto** { **lock** | **unlock** } }

undo channel [**auto**]

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP は無線チャネルを自動的に選択し、チャネルはロックされません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channel-number: 数字でチャネルを指定します。この引数の値の範囲は、地域コードおよび無線モードにより異なります。

auto lock: AP が自動的に無線チャネルを選択し、チャネルをロックするよう設定します。

auto unlock: AP が自動的に無線チャネルを選択し、チャネルをロックしないよう設定します。

説明

channel コマンドは無線の動作チャネルを設定します。

undo channel コマンドはデフォルトに戻します。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。30 分後、変更前に使用していたチャネルに戻り、静止タイマを起動します。静止時間内にレーダ信号が検出されなければ、無線はそのチャネルの使用を開始します。静止時間内にレーダ信号が検出されると、無線は再びチャネルを変更します。

例

AP **ap1** の動作チャネルを **48** に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 48

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、動作チャネルを **48** に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel 48

3.1.8 channel auto-select

Syntax

channel auto-select { **blacklist** | **whitelist** } *channel-number*

undo channel auto-select { **blacklist** | **whitelist** } { **all** | *channel-number* }

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、チャネル選択のブラックリストまたはホワイトリストは存在しません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

blacklist: チャネル選択ブラックリストにチャネルを追加します。AP はブラックリストにあるチャネルを選択しません。

whitelist: チャネル選択ホワイトリストにチャネルを追加します。AP はホワイトリストにあるチャネルのみを選択します。

channel-number: チャネル番号によりチャネルを指定します。この引数の値の範囲は、地域コードおよび無線モードにより異なります。

all: チャネル選択ブラックリストまたはホワイトリストのすべてのチャネルを指定します。

説明

channel auto-select コマンドはチャネル選択のブラックリストまたはホワイトリストを設定します。

undo channel auto-select コマンドはブラックリストまたはホワイトリストから指定したチャネルを削除します。

同じ AP に対してブラックリストとホワイトリストの両方にチャネル選択を設定することはできません。

この機能は、AP が自動チャネル選択モードで作動する場合に限り有効になります。

例

AP **ap1** のチャネル選択ホワイトリストにチャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel auto-select whitelist 56 60 64

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、チャネル選択ホワイトリストにチャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel auto-select whitelist 56 60 64

関連コマンド

channel

3.1.9 channel band-width

Syntax

channel band-width { **20** | **40** [**auto-switch**] | **80** | **160** }

undo channel band-width

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、帯域幅モードは 802.11ac/ax では 80MHz、802.11an では 40MHz、802.11gac/gax と 802.11gn では 20MHz です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

20: 帯域幅を 20 MHz に設定します。

40: 帯域幅を 40 MHz に設定します。

80: 帯域幅を 80 MHz に設定します。

160: 帯域幅を 160 MHz に設定します。

🕮 **メモ：**

160MHz は QX-W1130 の Radio1 のみでサポートします。

---

auto-switch: 無線が 20MHz から 40MHz の間で帯域幅モードを切り替えることを許可します。このキーワードは、802.11g、802.11gac、802.11gax にのみ適用されます。

説明

channel band-width コマンドは帯域幅モードを設定します。

undo channel band-width コマンドはデフォルトに戻します。

本コマンドは 802.11n、802.11ac、802.11ax、802.11gac、802.11gax 無線にのみ適用可能です。無線モードを変更すると、新しい無線モードでは、本コマンドのデフォルト設定に戻ります。

帯域幅モードが 40MHz の場合、ボンディングできる 2 つの隣接したチャネルが存在する場合は、無線は 40MHz の帯域を使用します。ボンディングできる隣接チャネルがない場合は、無線は 20MHz の帯域を使用します。

帯域幅モードが 80MHz の場合、ボンディングできる隣接したチャネルが存在する場合は、無線は 80MHz の帯域を使用します。80MHz にボンディングできる隣接チャネルはないが、40MHz チャネルにボンディングできる 2 つの隣接チャネルが存在する場合は、40MHz の帯域が使用されます。隣接するチャネルがない場合は、無線は 20MHz の帯域を使用します。

帯域幅モードが 160MHz の場合、ボンディングできる隣接したチャネルが存在する場合は、無線は 160MHz の帯域を使用します。160MHz にボンディングできる隣接チャネルはないが、80MHz チャネルにボンディングできる 2 つの隣接チャネルが存在する場合は、80MHz の帯域が使用されます。隣接するチャネルがない場合は、無線は 20MHz の帯域を使用します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP ap1 の帯域幅モードを 40MHaz に設定します。

<AC> system-view

[AC] wlan ap **ap1** model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] channel band-width 40

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、帯域幅モードを 40MHaz に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel band-width 40

3.1.10 channel-usage measure

Syntax

channel-usage measure

View

Radio view

定義済みユーザロール

network-admin

説明

channel-usage measure コマンドはオンデマンドチャネル使用量測定を実行します。

この機能により、AP はサポートされているチャネルをスキャンし、スキャン後にチャネルの使用状況を表示できます。チャネルをスキャンするのに約 1 秒かかります。

例

AP **ap1** の無線 2 でオンデマンドのチャネル使用状況測定を実行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] channel-usage measure

```
Please wait......Done.
Channel  Usage
1        63%
2        61%
3        55%
4        45%
5        64%
6        74%
7        66%
8        48%
9        35%
10       38%
11       54%
12       30%
13       72%
```

3.1.11 channel-usage threshold

Syntax

channel-usage threshold *threshold*

undo channel-usage threshold

デフォルト

90%

View

Radio view

定義済みユーザロール

network-admin

パラメータ

threshold:チャネル使用率アラームしきい値をパーセンテージで指定します。値の範囲は 5 から 100 です。

説明

channel-usage threshold コマンドはチャネル使用率アラームしきい値を設定します。

undo channel-usage threshold コマンドはデフォルトに戻します。

チャネル使用率がしきい値を超えると、装置は info-center にアラームを報告します。

例

AP **ap1** の Radio1 のチャネル使用率アラームしきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel-usage threshold 20

3.1.12 client dot11ac-only

Syntax

client dot11ac-only { **disable** | **enable** }

undo client dot11ac-only

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11ac クライアント限定アクセスを無効にします。

enable: 802.11ac クライアント限定アクセスを有効にします。

説明

client dot11ac-only enable コマンドは 802.11ac 無線で 802.11ac クライアントの接続のみを許可し、802.11ax 無線で 802.11ac/ax クライアントの接続のみを許可します。

client dot11ac-only disable コマンドは 802.11ac クライアントを無効にします。

undo client dot11ac-only コマンドはデフォルトに戻します。

本コマンドは 802.11ac/ax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、本コマンドは無効になります。

本コマンドを有効にすると、802.11ac/ax 以外のクライアントはログオフされます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11ac クライアントにのみアクセスを許可します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] client dot11ac-only enable

AP グループ apgroup1 の型番 **QX-W1020** の AP で、802.11ac クライアントにのみアクセスを許可します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] client dot11ac-only enable

関連コマンド

dot11ac mandatory maximum-nss

3.1.13 client dot11ax-only

Syntax

client dot11ax-only { **disable** | **enable** }

undo client dot11ax-only

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11ax クライアント限定アクセスを無効にします。

enable: 802.11ax クライアント限定アクセスを有効にします。

説明

client dot11ax-only enable コマンドは 802.11ax 無線で 802.11ax クライアントの接続のみを許可します。

client dot11ax-only disable コマンドは 802.11ax クライアント限定アクセスを無効にします。

undo client dot11ax-only コマンドはデフォルトに戻します。

本コマンドは 802.11ax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、802.11n、802.11ac に変更すると、コマンドは無効になります。

本コマンドを有効にすると、802.11ax 以外のクライアントはログオフされます。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax mandatory maximum-nss

3.1.14 client dot11b-forbidden

Syntax

client dot11b-forbidden { **disable** | **enable** }

undo client dot11b-forbidden

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

mdc-admin

パラメータ

disable: 802.11b クライアント拒否を有効にします。

enable: 802.11b クライアント拒否を無効にします。

説明

client dot11b-forbidden enable コマンドは 802.11b クライアント接続を拒否にします。

client dot11b-forbidden disable コマンドは 802.11b クライアント拒否を無効にします。

undo client dot11b-forbidden コマンドはデフォルトに戻します。

802.11g または 802.11gn 無線で 802.11b クライアントを拒否することにより、低速な 802.11b クライアントの影響を減少させ、無線データ転送を高速化することができます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11b クライアントを拒否します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] client dot11b-forbidden enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11b クライアントを拒否します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-model-QX-W1020-radio-1] client dot11b-forbidden enable

3.1.15 client dot11n-only

Syntax

client dot11n-only { **disable** | **enable** }

undo client dot11n-only

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無効。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11n/ac/ax クライアント限定アクセスを無効にします。

enable: 802.11n/ac/ax クライアント限定アクセスを有効にします。

説明

client dot11n-only enable コマンドは 802.11ac 無線で 802.11an/ac クライアントの接続のみを許可し、802.11ax 無線で 802.11an/ac/ax クライアントの接続のみを許可します。

client dot11n-only disable コマンドは 802.11n/ac/ax クライアント限定アクセスを無効にします。

undo client dot11n-only コマンドはデフォルトに戻します。

本コマンドは 802.11n、802.11ac、802.11ax 無線にのみ適用可能です。無線モードを 802.11a/b/g に変更することで、本機能は無効になります。

本コマンドを有効にすると、802.11a/b/g クライアントはログオフされます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11n/ac/ax クライアント限定アクセスを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] client dot11n-only enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11n/ac/ax クライアント限定アクセスを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client dot11n-only enable

3.1.16 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP に接続できるクライアント数に制限はありません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

max-number: AP に接続できるクライアントの最大数を指定します。この引数の値の範囲は、AP モデルによって異なります。

説明

client max-count コマンドは AP に接続できるクライアントの最大数を設定します。

undo client max-count コマンドはデフォルトに戻します。

クライアント数が最大に達すると、AP は新しいクライアントの許可を停止します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、AP に接続できるクライアントの最大数を 38 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] client max-count 38

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、AP に接続できるクライアントの最大数を 38 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client max-count 38

3.1.17 continuous-mode

Syntax

continuous-mode { **mcs** *mcs-index* | **nss** *nss-index* **vht-mcs** *vhtmcs-index* | **rate** *rate-value* }

undo continuous-mode

デフォルト

無効

View

Radio view

定義済みユーザロール

network-admin

パラメータ

mcs *mcs-index*: 0〜76 の範囲の MCS インデックスを指定します。このオプションは、802.11n、802.11ac、および 802.11gac 無線にのみ適用されます。

nss *nss-index* **vht-mcs** *vhtmcs-index*: VHT-MCS インデックスを指定します。nss-index および vhtmcs-index 引数の値の範囲は、それぞれ 1〜8 および 0〜9 です。このオプションは、802.11ac および 802.11gac 無線にのみ適用されます。

rate *rate-value*: 送信レートを Mbps で指定します。このオプションは、すべての無線タイプに適用されます。

説明

continuous-mode コマンドは無線の連続モードを有効にします。

undo continuous-mode コマンドはデフォルトに戻します。

この機能はネットワークテストにのみ使用されます。それ以外の環境では使用しないでください。

指定されたレートで連続データパケット送信を可能にします。この機能が有効になっているときは、送信レートを変更する以外の操作は実行しないでください。

例

連続モードを有効にし、送信レートを 6Mbps に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] continuous-mode rate 6

関連コマンド

display wlan ap continuous-mode

3.1.18 display wlan ap continuous-mode

Syntax

display wlan ap { **all** | **name** *ap-name* } **continuous-mode**

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap continuous-mode コマンドは連続モードに関する情報を表示します。

例

AP **ap1** の無線の連続モードに関する情報を表示します。

<AC> display wlan ap name ap1 continuous-mode

```
AP name    Radio ID    Radio type      Rate    Mcs-Index   Nss   Vht-mcs
ap1        1           802.11a         6       N/A         N/A   N/A
```

表 3-1 コマンド出力

フィールド	説明
Mcs-Index	MCS index.
Nss	NSS index.
Vht-mcs	VHT-MCS index.

関連コマンド

continuous-mode

3.1.19 display wlan ap radio

Syntax

display wlan ap all radio [**frequency-band** { **5** | **2.4** }]

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

frequency-band: 周波数帯を指定します。

5: 5GHz 周波数帯を指定します。

2.4: 2.4GHz 周波数帯を指定します。

説明

display wlan ap radio コマンドは無線情報を表示します。

例

すべての AP の無線情報を表示します。

<AC> display wlan ap all radio

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
```

```
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 32
Remaining APs: 31
Total AP licenses: 20
Remaining AP licenses: 19

AP name               RID State Channel         Usage TxPower AntGain EIRP
                                                (%)   (dBm)   (dBi)   (dBm)
ap1                   1   Up    48(auto)        10    20      10      30
```

すべての AP の 2.4 GHz 無線情報を表示します。

<AC> display wlan ap all radio frequency-band 2.4

```
AP name               RID State Channel         Usage TxPower AntGain EIRP
                                                (%)   (dBm)   (dBi)   (dBm)
ap1                   2   Up    104(auto)       15    20      10      30
```

表 3-2 コマンド出力

フィールド	説明
Total number of inside APs	内部APは、アンカーAPがACとして動作するときに無線管理のために自動的に作成される手動APです。内部APの名前とシリアルIDは、アンカーAPのMACアドレスとシリアルIDです。
Total number of connected WTUs	このフィールドは、将来の使用のために予約されています。
Maximum supported APs	AC上のサポートされているAPの最大数です。
Remaining APs	サポートされているAPの残りの数です。
Total AP licenses	APライセンスの総数です。
Remaining AP licenses	残りのAPライセンスの数です。
State	無線状態: ● Up. ● Down.
Usage	使用チャネルです。
TxPower (dBm)	送信電力です。デフォルトでは、サポートされる最大電力がパケットの送信に使用されます。
AntGain (dBi)	アンテナ利得です。
EIRP (dBm)	効果的な等方放射電力です。

3.1.20 display wlan ap radio channel

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio channel**

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap radio channel コマンドは無線チャネル情報を表示します。

例

AP **ap3** の無線チャネル情報を表示します。

<AC> display wlan ap name ap3 radio channel

```
AP name               RID Channel        Band-width         CenterFreq
                                        (MHz)
ap3                   1   36(auto)        20/40/80/160/(80+80) 42/58
ap3                   2   120             20/40/80           155
```

表 3-3 コマンド出力

フィールド	説明
Band-width (MHz)	サポートされるチャネル帯域幅です。
CenterFreq	中央周波数です。このフィールドは、サポートされているチャネル帯域幅が80MHzに達した場合にのみ使用できます。このフィールドには、160MHzまたは80+80MHzの帯域幅がサポートされている場合のメインチャネルとセカンダリチャネルの中心周波数が表示されます。

3.1.21 display wlan ap radio type

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio type**

View

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan ap radio type コマンドは無線タイプ情報を表示します。

例

AP **ap1** の無線タイプ情報を表示します。

<AC> display wlan ap name ap1 radio type

```
AP name               RID  AP state  Radio state  Radio type
ap1                   1    Up       Up           802.11n(5GHz)
ap1                   2    Up       Down         802.11n(2.4GHz)
```

表 3-4 コマンド出力

フィールド	説明
AP state	APの状態: ● Up–APはACとCAPWAPトンネルを確立しました。 ● Down–APはACとCAPWAPトンネルを確立していません。
Radio state	無線状態: ● Up. ● Down.

3.1.22 display wlan statistics ap radio

🕮 メモ：

- **display wlan statistics ap radio** コマンドはソフトウェアバージョン 7.2.50 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan statistics ap { **all** | **name** *ap-name* } **radio**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap: AP を指定します。

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan statistics ap radio コマンドは無線統計情報を表示します。

例

#AP ap1 の無線統計情報を表示します

<AC>display wlan statistics ap name ap1 radio

```
                        Radio statistics
--------------------------------------------------------------------------------
 AP name:ap1                              Radio ID:1
--------------------------------------------------------------------------------
Transmitted frame statistics:
   Total frames                         :176
   Total frame bytes                     :45205
   Unicast frames                       :31
   Unicast frame bytes                   :8085
   Broadcast/Multicast frames             :184
   Broadcast/Multicast frame bytes        :39664
   Other frames                         :18446744073709551577
```

```
Other frame bytes                    :18446744073709549072

Discarded frames                     :35
Failed RTS frames                    :0
Retransmissions                      :0
Successful RTS frames                :0
Retransmitted frames                 :0
No-ACK frames                        :0
Authentication frames                :1
Association frames                   :1

Packet statistics by size:
  Smaller than or equal to 128       :72
  Between 128 and 512 (inclusive)    :89
  Between 512 and 1024 (inclusive)   :0
  Larger than 1024                   :0

Packet statistics by rate:
   1 Mbps  :0          2 Mbps  :0
 5.5 Mbps  :0          6 Mbps  :2
   9 Mbps  :0         11 Mbps  :0
  12 Mbps  :0         18 Mbps  :0
  24 Mbps  :0         36 Mbps  :0
  48 Mbps  :0         54 Mbps  :0

Packet statistics based on data rate:
 6.5 Mbps  :0                      7.2 Mbps  :0
  13 Mbps  :0                     13.5 Mbps  :0
14.4 Mbps  :0                       15 Mbps  :0
19.5 Mbps  :0                     21.7 Mbps  :0
  26 Mbps  :0                       27 Mbps  :0
28.9 Mbps  :0                     29.3 Mbps  :0
  30 Mbps  :0                     32.5 Mbps  :0
  39 Mbps  :0                     40.5 Mbps  :0
43.3 Mbps  :0                       45 Mbps  :0
  52 Mbps  :0                       54 Mbps  :0
57.8 Mbps  :0                     58.5 Mbps  :0
  60 Mbps  :0                       65 Mbps  :0
72.2 Mbps  :0                       78 Mbps  :0
  81 Mbps  :0                     86.5 Mbps  :0
86.7 Mbps  :0                     87.8 Mbps  :0
  90 Mbps  :0                       96 Mbps  :0
97.5 Mbps  :0                      104 Mbps  :0
```

```
   108 Mbps  :0                    115.6 Mbps  :0
   117 Mbps  :0                     120 Mbps  :0
 121.5 Mbps  :0                     130 Mbps  :0
   135 Mbps  :0                    144.4 Mbps  :0
   150 Mbps  :0                     156 Mbps  :0
   162 Mbps  :0                     173 Mbps  :0
 173.3 Mbps  :0                    175.5 Mbps  :0
   180 Mbps  :0                     192 Mbps  :0
   195 Mbps  :0                     200 Mbps  :0
   208 Mbps  :0                     216 Mbps  :0
 216.7 Mbps  :0                    231.1 Mbps  :0
   234 Mbps  :0                     240 Mbps  :0
   243 Mbps  :0                     260 Mbps  :0
   263 Mbps  :0                    263.3 Mbps  :0
   270 Mbps  :0                    288.9 Mbps  :0
 292.5 Mbps  :0                     300 Mbps  :0
   312 Mbps  :0                     324 Mbps  :0
   325 Mbps  :0                     344 Mbps  :0
 346.7 Mbps  :0                     351 Mbps  :0
   360 Mbps  :0                    364.5 Mbps  :0
   390 Mbps  :0                     400 Mbps  :0
   405 Mbps  :0                     432 Mbps  :0
 433.3 Mbps  :0                     450 Mbps  :0
   468 Mbps  :0                     480 Mbps  :0
   486 Mbps  :0                     520 Mbps  :0
 526.5 Mbps  :0                     540 Mbps  :0
   585 Mbps  :0                     600 Mbps  :0
   648 Mbps  :0                     650 Mbps  :0
   702 Mbps  :0                     720 Mbps  :0
   780 Mbps  :0                    789.9 Mbps  :0
   800 Mbps  :0                    866.7 Mbps  :0
 877.5 Mbps  :0                     936 Mbps  :0
   975 Mbps  :0                    1040 Mbps  :0
  1053 Mbps  :0                    1170 Mbps  :0
  1300 Mbps  :0                    1404 Mbps  :0
  1560 Mbps  :0                   1733.3 Mbps  :0
--------------------------------------------------------------------------------
Received frame statistics:
   Total frames                        :4232
   Total frame bytes                    :1011302
   Unicast frames                      :861
   Unicast frame bytes                  :185001
   Broadcast/Multicast frames           :3371
```

```
Broadcast/Multicast frame bytes        :821056
Fragmented frames                     :0
Duplicate frames                      :0
FCS failures                         :0
Decryption errors                     :0
Authentication frames                  :0
Association frames                    :0

Packet statistics by size:
  Smaller than or equal to 128         :322
  Between 128 and 512 (inclusive)      :3910
  Between 512 and 1024 (inclusive)     :0
  Larger than 1024                    :0

Packet statistics by rate:
    1 Mbps  :0          2 Mbps  :0
  5.5 Mbps  :0          6 Mbps  :5
    9 Mbps  :0         11 Mbps  :0
   12 Mbps  :0         18 Mbps  :0
   24 Mbps  :0         36 Mbps  :0
   48 Mbps  :0         54 Mbps  :19

Packet statistics based on data rate:
 6.5 Mbps  :0                      7.2 Mbps  :0
  13 Mbps  :0                     13.5 Mbps  :0
14.4 Mbps  :0                       15 Mbps  :0
19.5 Mbps  :0                     21.7 Mbps  :0
  26 Mbps  :0                       27 Mbps  :0
28.9 Mbps  :0                     29.3 Mbps  :0
  30 Mbps  :0                     32.5 Mbps  :0
  39 Mbps  :0                     40.5 Mbps  :0
43.3 Mbps  :0                       45 Mbps  :0
  52 Mbps  :0                       54 Mbps  :19
57.8 Mbps  :0                     58.5 Mbps  :0
  60 Mbps  :0                       65 Mbps  :0
72.2 Mbps  :0                       78 Mbps  :0
  81 Mbps  :0                     86.5 Mbps  :0
86.7 Mbps  :0                     87.8 Mbps  :0
  90 Mbps  :0                       96 Mbps  :0
97.5 Mbps  :0                      104 Mbps  :0
 108 Mbps  :0                    115.6 Mbps  :0
 117 Mbps  :8                      120 Mbps  :0
121.5 Mbps  :0                     130 Mbps  :0
```

```
  135 Mbps  :0                    144.4 Mbps  :0
  150 Mbps  :0                      156 Mbps  :0
  162 Mbps  :0                      173 Mbps  :0
173.3 Mbps  :0                    175.5 Mbps  :4
  180 Mbps  :0                      192 Mbps  :0
  195 Mbps  :0                      200 Mbps  :0
  208 Mbps  :0                      216 Mbps  :0
216.7 Mbps  :0                    231.1 Mbps  :0
  234 Mbps  :0                      240 Mbps  :0
  243 Mbps  :0                      260 Mbps  :0
  263 Mbps  :0                    263.3 Mbps  :0
  270 Mbps  :0                    288.9 Mbps  :0
292.5 Mbps  :0                      300 Mbps  :0
  312 Mbps  :0                      324 Mbps  :0
  325 Mbps  :0                      344 Mbps  :0
346.7 Mbps  :0                      351 Mbps  :0
  360 Mbps  :0                    364.5 Mbps  :0
  390 Mbps  :0                      400 Mbps  :0
  405 Mbps  :0                      432 Mbps  :0
433.3 Mbps  :0                      450 Mbps  :0
  468 Mbps  :0                      480 Mbps  :0
  486 Mbps  :0                      520 Mbps  :0
526.5 Mbps  :0                      540 Mbps  :0
  585 Mbps  :0                      600 Mbps  :0
  648 Mbps  :0                      650 Mbps  :0
  702 Mbps  :0                      720 Mbps  :0
  780 Mbps  :0                    789.9 Mbps  :0
  800 Mbps  :0                    866.7 Mbps  :0
877.5 Mbps  :0                      936 Mbps  :0
  975 Mbps  :0                     1040 Mbps  :0
 1053 Mbps  :0                     1170 Mbps  :0
 1300 Mbps  :0                     1404 Mbps  :0
 1560 Mbps  :0                    1733.3 Mbps  :0
--------------------------------------------------------------------------------
                        Radio statistics
--------------------------------------------------------------------------------
 AP name:ap1                                Radio ID:2
--------------------------------------------------------------------------------
Transmitted frame statistics:
   Total frames                        :0
   Total frame bytes                    :0
   Unicast frames                      :0
   Unicast frame bytes                  :0
```

```
Broadcast/Multicast frames            :0
Broadcast/Multicast frame bytes        :0
Other frames                          :0
Other frame bytes                      :0

Discarded frames                      :0
Failed RTS frames                     :0
Retransmissions                       :0
Successful RTS frames                  :0
Retransmitted frames                   :0
No-ACK frames                         :0
Authentication frames                  :0
Association frames                     :0

Packet statistics by size:
  Smaller than or equal to 128         :0
  Between 128 and 512 (inclusive)      :0
  Between 512 and 1024 (inclusive)     :0
  Larger than 1024                    :0

Packet statistics by rate:
    1 Mbps  :0          2 Mbps  :0
  5.5 Mbps  :0          6 Mbps  :0
    9 Mbps  :0         11 Mbps  :0
   12 Mbps  :0         18 Mbps  :0
   24 Mbps  :0         36 Mbps  :0
   48 Mbps  :0         54 Mbps  :0

Packet statistics based on data rate:
 6.5 Mbps  :0                       7.2 Mbps  :0
  13 Mbps  :0                      13.5 Mbps  :0
14.4 Mbps  :0                        15 Mbps  :0
19.5 Mbps  :0                      21.7 Mbps  :0
  26 Mbps  :0                        27 Mbps  :0
28.9 Mbps  :0                      29.3 Mbps  :0
  30 Mbps  :0                      32.5 Mbps  :0
  39 Mbps  :0                      40.5 Mbps  :0
43.3 Mbps  :0                        45 Mbps  :0
  52 Mbps  :0                        54 Mbps  :0
57.8 Mbps  :0                      58.5 Mbps  :0
  60 Mbps  :0                        65 Mbps  :0
72.2 Mbps  :0                        78 Mbps  :0
  81 Mbps  :0                      86.5 Mbps  :0
```

```
  86.7 Mbps  :0                      87.8 Mbps  :0
    90 Mbps  :0                       96 Mbps  :0
  97.5 Mbps  :0                      104 Mbps  :0
   108 Mbps  :0                     115.6 Mbps  :0
   117 Mbps  :0                      120 Mbps  :0
 121.5 Mbps  :0                      130 Mbps  :0
   135 Mbps  :0                     144.4 Mbps  :0
   150 Mbps  :0                      156 Mbps  :0
   162 Mbps  :0                      173 Mbps  :0
 173.3 Mbps  :0                     175.5 Mbps  :0
   180 Mbps  :0                      192 Mbps  :0
   195 Mbps  :0                      200 Mbps  :0
   208 Mbps  :0                      216 Mbps  :0
 216.7 Mbps  :0                     231.1 Mbps  :0
   234 Mbps  :0                      240 Mbps  :0
   243 Mbps  :0                      260 Mbps  :0
   263 Mbps  :0                     263.3 Mbps  :0
   270 Mbps  :0                     288.9 Mbps  :0
 292.5 Mbps  :0                      300 Mbps  :0
   312 Mbps  :0                      324 Mbps  :0
   325 Mbps  :0                      344 Mbps  :0
 346.7 Mbps  :0                      351 Mbps  :0
   360 Mbps  :0                     364.5 Mbps  :0
   390 Mbps  :0                      400 Mbps  :0
   405 Mbps  :0                      432 Mbps  :0
 433.3 Mbps  :0                      450 Mbps  :0
   468 Mbps  :0                      480 Mbps  :0
   486 Mbps  :0                      520 Mbps  :0
 526.5 Mbps  :0                      540 Mbps  :0
   585 Mbps  :0                      600 Mbps  :0
   648 Mbps  :0                      650 Mbps  :0
   702 Mbps  :0                      720 Mbps  :0
   780 Mbps  :0                     789.9 Mbps  :0
   800 Mbps  :0                     866.7 Mbps  :0
 877.5 Mbps  :0                      936 Mbps  :0
   975 Mbps  :0                     1040 Mbps  :0
  1053 Mbps  :0                     1170 Mbps  :0
  1300 Mbps  :0                     1404 Mbps  :0
  1560 Mbps  :0                    1733.3 Mbps  :0
-------------------------------------------------------------------------------
--
Received frame statistics:
   Total frames                        :0
```

```
Total frame bytes                    :0
Unicast frames                      :0
Unicast frame bytes                  :0
Broadcast/Multicast frames            :0
Broadcast/Multicast frame bytes        :0
Fragmented frames                    :0
Duplicate frames                     :0
FCS failures                        :0
Decryption errors                    :0
Authentication frames                :0
Association frames                   :0

Packet statistics by size:
  Smaller than or equal to 128        :0
  Between 128 and 512 (inclusive)      :0
  Between 512 and 1024 (inclusive)     :0
  Larger than 1024                   :0

Packet statistics by rate:
    1 Mbps  :0          2 Mbps  :0
  5.5 Mbps  :0          6 Mbps  :0
    9 Mbps  :0         11 Mbps  :0
   12 Mbps  :0         18 Mbps  :0
   24 Mbps  :0         36 Mbps  :0
   48 Mbps  :0         54 Mbps  :0

Packet statistics based on data rate:
 6.5 Mbps  :0                       7.2 Mbps  :0
  13 Mbps  :0                      13.5 Mbps  :0
14.4 Mbps  :0                        15 Mbps  :0
19.5 Mbps  :0                      21.7 Mbps  :0
  26 Mbps  :0                        27 Mbps  :0
28.9 Mbps  :0                      29.3 Mbps  :0
  30 Mbps  :0                      32.5 Mbps  :0
  39 Mbps  :0                      40.5 Mbps  :0
43.3 Mbps  :0                        45 Mbps  :0
  52 Mbps  :0                        54 Mbps  :0
57.8 Mbps  :0                      58.5 Mbps  :0
  60 Mbps  :0                        65 Mbps  :0
72.2 Mbps  :0                        78 Mbps  :0
  81 Mbps  :0                      86.5 Mbps  :0
86.7 Mbps  :0                      87.8 Mbps  :0
  90 Mbps  :0                        96 Mbps  :0
```

```
 97.5 Mbps  :0                    104 Mbps  :0
  108 Mbps  :0                  115.6 Mbps  :0
  117 Mbps  :0                    120 Mbps  :0
121.5 Mbps  :0                    130 Mbps  :0
  135 Mbps  :0                  144.4 Mbps  :0
  150 Mbps  :0                    156 Mbps  :0
  162 Mbps  :0                    173 Mbps  :0
173.3 Mbps  :0                  175.5 Mbps  :0
  180 Mbps  :0                    192 Mbps  :0
  195 Mbps  :0                    200 Mbps  :0
  208 Mbps  :0                    216 Mbps  :0
216.7 Mbps  :0                  231.1 Mbps  :0
  234 Mbps  :0                    240 Mbps  :0
  243 Mbps  :0                    260 Mbps  :0
  263 Mbps  :0                  263.3 Mbps  :0
  270 Mbps  :0                  288.9 Mbps  :0
292.5 Mbps  :0                    300 Mbps  :0
  312 Mbps  :0                    324 Mbps  :0
  325 Mbps  :0                    344 Mbps  :0
346.7 Mbps  :0                    351 Mbps  :0
  360 Mbps  :0                  364.5 Mbps  :0
  390 Mbps  :0                    400 Mbps  :0
  405 Mbps  :0                    432 Mbps  :0
433.3 Mbps  :0                    450 Mbps  :0
  468 Mbps  :0                    480 Mbps  :0
  486 Mbps  :0                    520 Mbps  :0
526.5 Mbps  :0                    540 Mbps  :0
  585 Mbps  :0                    600 Mbps  :0
  648 Mbps  :0                    650 Mbps  :0
  702 Mbps  :0                    720 Mbps  :0
  780 Mbps  :0                  789.9 Mbps  :0
  800 Mbps  :0                  866.7 Mbps  :0
877.5 Mbps  :0                    936 Mbps  :0
  975 Mbps  :0                   1040 Mbps  :0
 1053 Mbps  :0                   1170 Mbps  :0
 1300 Mbps  :0                   1404 Mbps  :0
 1560 Mbps  :0                  1733.3 Mbps  :0
--------------------------------------------------------------------------------
                          Radio statistics
--------------------------------------------------------------------------------
 AP name:ap1                              Radio ID:3
--------------------------------------------------------------------------------
Transmitted frame statistics:
```

```
Total frames                        :0
Total frame bytes                    :0
Unicast frames                      :0
Unicast frame bytes                  :0
Broadcast/Multicast frames            :0
Broadcast/Multicast frame bytes       :0
Other frames                        :0
Other frame bytes                    :0

Discarded frames                     :0
Failed RTS frames                    :0
Retransmissions                     :0
Successful RTS frames                :0
Retransmitted frames                 :0
No-ACK frames                       :0
Authentication frames                :0
Association frames                   :0

Packet statistics by size:
  Smaller than or equal to 128        :0
  Between 128 and 512 (inclusive)     :0
  Between 512 and 1024 (inclusive)    :0
  Larger than 1024                   :0

Packet statistics by rate:
    1 Mbps  :0          2 Mbps  :0
  5.5 Mbps  :0          6 Mbps  :0
    9 Mbps  :0         11 Mbps  :0
   12 Mbps  :0         18 Mbps  :0
   24 Mbps  :0         36 Mbps  :0
   48 Mbps  :0         54 Mbps  :0

Packet statistics based on data rate:
 6.5 Mbps  :0                       7.2 Mbps  :0
  13 Mbps  :0                      13.5 Mbps  :0
14.4 Mbps  :0                        15 Mbps  :0
19.5 Mbps  :0                      21.7 Mbps  :0
  26 Mbps  :0                        27 Mbps  :0
28.9 Mbps  :0                      29.3 Mbps  :0
  30 Mbps  :0                      32.5 Mbps  :0
  39 Mbps  :0                      40.5 Mbps  :0
43.3 Mbps  :0                        45 Mbps  :0
  52 Mbps  :0                        54 Mbps  :0
```

```
 57.8 Mbps  :0                    58.5 Mbps  :0
   60 Mbps  :0                      65 Mbps  :0
 72.2 Mbps  :0                      78 Mbps  :0
   81 Mbps  :0                    86.5 Mbps  :0
 86.7 Mbps  :0                    87.8 Mbps  :0
   90 Mbps  :0                      96 Mbps  :0
 97.5 Mbps  :0                     104 Mbps  :0
  108 Mbps  :0                   115.6 Mbps  :0
  117 Mbps  :0                     120 Mbps  :0
121.5 Mbps  :0                     130 Mbps  :0
  135 Mbps  :0                   144.4 Mbps  :0
  150 Mbps  :0                     156 Mbps  :0
  162 Mbps  :0                     173 Mbps  :0
173.3 Mbps  :0                   175.5 Mbps  :0
  180 Mbps  :0                     192 Mbps  :0
  195 Mbps  :0                     200 Mbps  :0
  208 Mbps  :0                     216 Mbps  :0
216.7 Mbps  :0                   231.1 Mbps  :0
  234 Mbps  :0                     240 Mbps  :0
  243 Mbps  :0                     260 Mbps  :0
  263 Mbps  :0                   263.3 Mbps  :0
  270 Mbps  :0                   288.9 Mbps  :0
292.5 Mbps  :0                     300 Mbps  :0
  312 Mbps  :0                     324 Mbps  :0
  325 Mbps  :0                     344 Mbps  :0
346.7 Mbps  :0                     351 Mbps  :0
  360 Mbps  :0                   364.5 Mbps  :0
  390 Mbps  :0                     400 Mbps  :0
  405 Mbps  :0                     432 Mbps  :0
433.3 Mbps  :0                     450 Mbps  :0
  468 Mbps  :0                     480 Mbps  :0
  486 Mbps  :0                     520 Mbps  :0
526.5 Mbps  :0                     540 Mbps  :0
  585 Mbps  :0                     600 Mbps  :0
  648 Mbps  :0                     650 Mbps  :0
  702 Mbps  :0                     720 Mbps  :0
  780 Mbps  :0                   789.9 Mbps  :0
  800 Mbps  :0                   866.7 Mbps  :0
877.5 Mbps  :0                     936 Mbps  :0
  975 Mbps  :0                    1040 Mbps  :0
 1053 Mbps  :0                    1170 Mbps  :0
 1300 Mbps  :0                    1404 Mbps  :0
 1560 Mbps  :0                  1733.3 Mbps  :0
```

```
--------------------------------------------------------------------------------
Received frame statistics:
  Total frames                        :0
  Total frame bytes                    :0
  Unicast frames                      :0
  Unicast frame bytes                  :0
  Broadcast/Multicast frames            :0
  Broadcast/Multicast frame bytes       :0
  Fragmented frames                   :0
  Duplicate frames                    :0
  FCS failures                        :0
  Decryption errors                    :0
  Authentication frames                :0
  Association frames                   :0

  Packet statistics by size:
    Smaller than or equal to 128        :0
    Between 128 and 512 (inclusive)     :0
    Between 512 and 1024 (inclusive)    :0
    Larger than 1024                  :0

  Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :0
     9 Mbps  :0         11 Mbps  :0
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :0

  Packet statistics based on data rate:
   6.5 Mbps  :0                      7.2 Mbps  :0
    13 Mbps  :0                     13.5 Mbps  :0
  14.4 Mbps  :0                       15 Mbps  :0
  19.5 Mbps  :0                     21.7 Mbps  :0
    26 Mbps  :0                       27 Mbps  :0
  28.9 Mbps  :0                     29.3 Mbps  :0
    30 Mbps  :0                     32.5 Mbps  :0
    39 Mbps  :0                     40.5 Mbps  :0
  43.3 Mbps  :0                       45 Mbps  :0
    52 Mbps  :0                       54 Mbps  :0
  57.8 Mbps  :0                     58.5 Mbps  :0
    60 Mbps  :0                       65 Mbps  :0
  72.2 Mbps  :0                       78 Mbps  :0
```

81 Mbps :0	86.5 Mbps :0
86.7 Mbps :0	87.8 Mbps :0
90 Mbps :0	96 Mbps :0
97.5 Mbps :0	104 Mbps :0
108 Mbps :0	115.6 Mbps :0
117 Mbps :0	120 Mbps :0
121.5 Mbps :0	130 Mbps :0
135 Mbps :0	144.4 Mbps :0
150 Mbps :0	156 Mbps :0
162 Mbps :0	173 Mbps :0
173.3 Mbps :0	175.5 Mbps :0
180 Mbps :0	192 Mbps :0
195 Mbps :0	200 Mbps :0
208 Mbps :0	216 Mbps :0
216.7 Mbps :0	231.1 Mbps :0
234 Mbps :0	240 Mbps :0
243 Mbps :0	260 Mbps :0
263 Mbps :0	263.3 Mbps :0
270 Mbps :0	288.9 Mbps :0
292.5 Mbps :0	300 Mbps :0
312 Mbps :0	324 Mbps :0
325 Mbps :0	344 Mbps :0
346.7 Mbps :0	351 Mbps :0
360 Mbps :0	364.5 Mbps :0
390 Mbps :0	400 Mbps :0
405 Mbps :0	432 Mbps :0
433.3 Mbps :0	450 Mbps :0
468 Mbps :0	480 Mbps :0
486 Mbps :0	520 Mbps :0
526.5 Mbps :0	540 Mbps :0
585 Mbps :0	600 Mbps :0
648 Mbps :0	650 Mbps :0
702 Mbps :0	720 Mbps :0
780 Mbps :0	789.9 Mbps :0
800 Mbps :0	866.7 Mbps :0
877.5 Mbps :0	936 Mbps :0
975 Mbps :0	1040 Mbps :0
1053 Mbps :0	1170 Mbps :0
1300 Mbps :0	1404 Mbps :0
1560 Mbps :0	1733.3 Mbps :0

表 3-5 コマンド出力

フィールド	説明
送信フレーム統計情報	
Total frames	プローブ応答とビーコンフレームを含む、送信されたフレームの合計数。
Total frame bytes	プローブ応答とビーコンフレームを含む、送信されたフレームの合計バイト数。
Unicast frames	送信されたユニキャストフレームの総数（プローブ応答を除く）。
Unicast frame bytes	送信されたユニキャストフレームの合計バイト数（プローブ応答を除く）。
Broadcast/Multicast frames	送信されたブロードキャストおよびマルチキャストフレームの総数（ビーコンフレームを除く）。
Broadcast/Multicast frame bytes	送信されたブロードキャストフレームとマルチキャストフレームの合計バイト数（ビーコンフレームを除く）。
Others frames	他の送信フレームの合計数。
Others frame bytes	他の送信フレームの合計バイト数。
Discarded frames	破棄されたフレームの合計数。
Failed RTS frames	失敗したRTSフレームの合計数。
Retransmissions	再送された回数。
Successful RTS frames	成功したRTSフレームの合計数。
Retransmitted frames	再送されたフレームの合計数。
No-ACK frames	No-ACKフレームの合計数。
Authentication frames	Authenticationフレームの合計数。
Association frames	Associationフレームの合計数
Packet statistics by size	パケットサイズによって分類されたパケットの総数。 Smaller than or equal to 128 ：128バイト以下のパケット数 Between 128 and 512 (inclusive)：129～512バイトのパケット数 Between 512 and 1024 (inclusive)：513～1024バイトのパケット数 Larger than 1024：1024バイトを超えるパケット数
Packet statistics by rate	802.11 a/b/gレートによって分類されたパケットの総数。

フィールド	説明
Packet statistics based on data rate	802.11 nレートによって分類されたパケットの総数。デバイスが802.11 nをサポートしていない場合、このフィールドは使用できません。
受信フレーム統計情報	
Total frames	受信したフレームの総数。
Total frame bytes	受信したフレームの合計バイト数。
Unicast frames	受信したユニキャストフレームの総数。
Unicast frame bytes	受信したユニキャストフレームの合計バイト数。
Broadcast/Multicast frames	受信したブロードキャストフレームとマルチキャストフレームの総数。
Broadcast/Multicast frame bytes	受信したブロードキャストフレームとマルチキャストフレームの合計バイト数。
Fragmented frames	受信したフラグメント化されたフレームの総数。
Duplicate frames	重複受信したフレームの総数
FCS failures	FCSエラーが発生した受信パケットの総数。
Decryption errors	復号化エラーのある受信パケットの合計数。
Authentication frames	受信したAuthenticationフレームの合計数。
Association frames	受信したAssociationフレームの合計数
Packet statistics by size	パケットサイズによって分類された受信パケットの総数。 Smaller than or equal to 128 ：128バイト以下のパケット数 Between 128 and 512 (inclusive)：129～512バイトのパケット数 Between 512 and 1024 (inclusive)：513～1024バイトのパケット数 Larger than 1024：1024バイトを超えるパケット数
Packet statistics by rate	802.11 a/b/gレートによって分類された受信パケットの総数。
Packet statistics based on data rate	802.11 nレートによって分類された受信パケットの総数。デバイスが802.11 nをサポートしていない場合、このフィールドは使用できません。

3.1.23 distance

Syntax

distance *distance*

undo distance

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、最大伝送距離は 1km です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

distance: 最大伝送距離を指定します。範囲は 1～40km です。

説明

distance コマンドは最大伝送距離を設定します。

undo distance コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大伝送距離を 5km に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] distance 5

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大伝送距離を 5km に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] distance 5

3.1.24 dl-ofdma

🕮 メモ：

- **dl-ofdma** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **dl-ofdma** コマンドは QX-W1100 シリーズの AP でのみサポートしています。

Syntax

dl-ofdma { **disable** | **enable** }

undo dl-ofdma

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン V7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

dl-ofdma enable コマンドはダウンリンク OFDMA を有効にします。

dl-ofdma disable コマンドはダウンリンク OFDMA を無効にします。

undo dl-ofdma コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

Radio view の設定は AP group radio view の設定よりも優先されます。

OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります。

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮

- 衝突バックオフの削減

例

AP ap1 の Radio1 でダウンリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] dl-ofdma enable

AP グループ apgroup1 の AP の Radio1 でダウンリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] dl-ofdma enable

関連コマンド

type dot11ax

3.1.25 dot11ac mandatory maximum-nss

Syntax

dot11ac mandatory maximum-nss *nss-number*

undo dot11ac mandatory maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS が設定されている場合、最大必須 NSS は設定されていません。
- 最大サポート NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大必須 NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11ac mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11ac mandatory maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大必須 NSS は、最大サポート NSS より大きくすることはできません。

最大必須 NSS の変更後、無線に接続している、変更された NSS をサポートしないクライアントの接続が解除されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大必須 NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac mandatory maximum-nss 7

AP グループ 1 の型番 **QX-W1020** の AP で、最大必須 NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11ac

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac mandatory maximum-nss 7

関連コマンド

dot11ac support maximum-nss

3.1.26 dot11ax mandatory maximum-nss

Syntax

dot11ax mandatory maximum-nss *nss-number*

undo dot11ax mandatory maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS が設定されている場合、最大必須 NSS は設定されていません。
- 最大サポート NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大必須 NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11ax mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11ax mandatory maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、および 802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大必須 NSS は、最大サポート NSS より大きくすることはできません。

最大必須 NSS の変更後、無線に接続している、変更された NSS をサポートしないクライアントの接続が解除されます。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax support maximum-nss

3.1.27 dot11ac multicast-nss

Syntax

dot11ac multicast-nss *nss-number* **vht-mcs** *index*

undo dot11ac multicast-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS か最大必須 NSS が設定されている場合、マルチキャスト NSS は設定されていません。
- 最大サポート NSS と最大必須 NSS のいずれも設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、マルチキャスト NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1～8 です。

index: VHT-MCS インデックスを指定します。範囲は 0～9 です。

説明

dot11ac multicast-nss コマンドはマルチキャスト NSS と VHT-MCS インデックスを設定します。

undo dot11ac multicast-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

本コマンドを設定する前に、**dot11ac mandatory maximum-nss** コマンドを設定しなければいけません。

マルチキャスト NSS は、最大必須 NSS より大きくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大必須 MSS を 2 に、マルチキャスト NSS を 2 に、VHT-MCS インデックスを 2 にそれぞれ設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac mandatory maximum-nss 2

[AC-wlan-ap-ap1-radio-1] dot11ac multicast-nss 2 vht-mcs 2

AP グループ 1 の型番 **QX-W1020** の AP で、最大必須 MSS を 2 に、マルチキャスト NSS を 2 に、VHT-MCS インデックスを 2 にそれぞれ設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac mandatory maximum-nss 2

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac multicast-nss 2 vht-mcs 2

関連コマンド

dot11ac mandatory maximum-nss

3.1.28 dot11ax multicast-nss

Syntax

dot11ax multicast-nss *nss-number* **he-mcs** *index*

undo dot11ax multicast-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート NSS か最大必須 NSS が設定されている場合、マルチキャスト NSS は設定されていません。
- 最大サポート NSS と最大必須 NSS のいずれも設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、マルチキャスト NSS は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1～8 です。

index: HE-MCS インデックスを指定します。範囲は 0～11 です。

説明

dot11ax multicast-nss コマンドはマルチキャスト NSS と HE-MCS インデックスを設定します。

undo dot11ax multicast-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、および 802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

本コマンドを設定する前に、**dot11ax mandatory maximum-nss** コマンドを設定しなければいけません。

マルチキャスト NSS は、最大必須 NSS より大きくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax mandatory maximum-nss

3.1.29 dot11ac support maximum-nss

Syntax

dot11ac support maximum-nss *nss-number*

undo dot11ac support maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 NSS が設定されている場合、最大サポート NSS は 8 となります。
- 最大必須 NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サポート NSS は 8 となります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11ac support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11ac support maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大サポート NSS は、最大必須 NSS より小さくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大サポート NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac support maximum-nss 7

AP グループ 1 の型番 **QX-W1020** の AP で、最大サポート NSS を 7 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11ac

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac support maximum-nss 7

関連コマンド

dot11ac mandatory maximum-nss

3.1.30 dot11ax support maximum-nss

Syntax

dot11ax support maximum-nss *nss-number*

undo dot11ax support maximum-nss

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 NSS が設定されている場合、最大サポート NSS は 8 となります。
- 最大必須 NSS が設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サポート NSS は 8 となります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11ax support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11ax support maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、および 802.11gax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドが無効になります。

最大サポート NSS は、最大必須 NSS より小さくすることはできません。

radio view の設定は、AP group radio view の設定に優先します。

関連コマンド

dot11ax mandatory maximum-nss

3.1.31 dot11g protection

Syntax

dot11g protection { **disable** | **enable** }

undo dot11g protection

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、802.11g 保護は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11g 保護を無効にします。

enable: 802.11g 保護を有効にします。

説明

dot11g protection enable コマンドは 802.11g 保護を有効にします。

dot11g protection disable コマンドは 802.11g 保護を無効にします。

undo dot11g protection コマンドはデフォルトに戻します。

本コマンドは、802.11g、802.11n(2.4GHz)および 802.11gac 無線にのみ適用されます。無線モードを 802.11g、802.11n(2.4GHz)または 802.11gac 以外に変更した場合、802.11g 保護設定は削除されます。

802.11g、802.11n、802.11gac 装置は、チャネル上で 802.11b 信号を検出したときに限り、データを送信する前に RTS/CTS パケットもしくは CTS-to-self パケットを送信します。

802.11g 保護は、802.11b クライアントが 802.11g、802.11n(2.4GHz)または 802.11gac の AP に接続されたときに自動的に有効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、802.11g 保護を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] type dot11gn

[AC-wlan-ap-ap1-radio-2] dot11g protection enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11g 保護を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-2] type dot11gn

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] dot11g protection enable

関連コマンド

protection-mode

3.1.32 dot11n mandatory maximum-mcs

Syntax

dot11n mandatory maximum-mcs *index*

undo dot11n mandatory maximum-mcs

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大サポート MCS インデックスが設定されている場合、最大必須 MCS は設定されていません。
- 最大サポート MCS インデックスが設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大必須 MCS インデックスは設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

index: 最大必須 MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n mandatory maximum-mcs コマンドは最大必須 MCS インデックスを設定します。

undo dot11n mandatory maximum-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

最大必須 MCS インデックスは、**dot11n multicast-mcs** コマンドを設定する前に設定しなければいけません。

最大必須 MCS インデックスの変更後、無線に接続している、変更された MCS インデックスをサポートしないクライアントの接続が解除されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大必須 MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n mandatory maximum-mcs 14

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大必須 MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n mandatory maximum-mcs 14

3.1.33 dot11n multicast-mcs

Syntax

dot11n multicast-mcs *index*

undo dot11n multicast-mcs

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 MCS インデックスか最大サポート MCS インデックスが設定されている場合、マルチキャスト MCS インデックスは設定されていません。
- 最大必須 MCS インデックスと最大サポート MCS インデックスのいずれも設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、マルチキャスト MCS インデックスは設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

index: マルチキャスト MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n multicast-mcs コマンドはマルチキャスト MCS インデックスを設定します。

undo dot11n multicast-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

マルチキャスト MCS インデックスは、802.11n、802.11ac、802.11ax クライアントが存在する場合にのみ有効です。

802.11a/b/g クライアントが存在する場合、AP とクライアントは 802.11a/b/g マルチキャストレートを使用してマルチキャストパケットを送信します。

マルチキャスト MCS インデックスは、帯域モードが 20MHz か 40MHz かによらず、20MHz 帯域モードのレートにマッピングされます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、マルチキャスト MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n mandatory maximum-mcs 14

[AC-wlan-ap-ap1-radio-1] dot11n multicast-mcs 14

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、マルチキャスト MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n mandatory maximum-mcs 14

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n multicast-mcs 14

3.1.34 dot11n protection

Syntax

dot11n protection { **disable** | **enable** }

undo dot11n protection

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、802.11n 保護は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11n 保護を無効にします。

enable: 802.11n 保護を有効にします。

説明

dot11n protection enable コマンドは 802.11n 保護を有効にします。

dot11n protection disable コマンドは 802.11n 保護を無効にします。

undo dot11n protection コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線のモードを 802.11n、802.11ac、802.11ax、および 802.11gac 以外のモードに変更すると、802.11n 保護設定が削除されます。

802.11n 装置は、チャネル上で 802.11a/b/g 信号を検出したときに限り、データを送信する前に RTS/CTS パケットもしくは CTS-to-self パケットを送信します。

802.11n 保護は、802.11a/b/g クライアントが 802.11n、802.11ac、802.11ax、または 802.11gac の AP に接続されたときに自動的に有効になります。

radio view の設定は、AP group radio view の設定に優先します。

🕮 **メモ**:

802.11n 装置とは、802.11n および 802.11ac、802.11ax 装置のことを指します。

例

AP **ap1** で、802.11n 保護を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n protection enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、802.11n 保護を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n protection enable

関連コマンド

protection-mode

3.1.35 dot11n support maximum-mcs

Syntax

dot11n support maximum-mcs *index*

undo dot11n support maximum-mcs

デフォルト

radio view でのデフォルト設定は以下の通りです。

- 最大必須 MCS インデックスが設定されている場合、最大必須 MCS は 76 となります。
- 最大必須 MCS インデックスが設定されていない場合、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サポート MCS インデックスは 76 となります。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

index: 最大サポート MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n support maximum-mcs コマンドは最大サポート MCS インデックスを設定します。

undo dot11n support maximum-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

最大サポート MCS インデックスは、最大必須 MCS インデックスより小さくなることはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大サポート MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n support maximum-mcs 14

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大サポート MCS インデックスを 14 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n support maximum-mcs 14

3.1.36 dtim

Syntax

dtim *counter*

undo dtim

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、DTIM 間隔は 1 となっています。AP はバッファリングされたブロードキャストおよびマルチキャストフレームを毎回ビーコンフレームごとに送信します。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

counter: DTIM 間隔を指定します。範囲は 1～31 です。

説明

dtim コマンドは DTIM（Delivery Traffic Indication Map）間隔を設定します。

undo dtim コマンドはデフォルトに戻します。

AP は、DTIM（Delivery Traffic Indication Map）に従ったビーコンを周期的にブロードキャストします。ビーコンをブロードキャストした後、AP は DTIM 間隔の値に基づいてバッファリングされたブロードキャストおよびマルチキャストフレームを送信します。例えば、DTIM 間隔を 5 に設定した場合、AP はバッファリングされたブロードキャストおよびマルチキャストフレームを 5 ビーコンフレームごとに送信します。

クライアント数が最大に達すると、AP は新しいクライアントの許可を停止します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、DTIM 間隔を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] dtim 5

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、DTIM 間隔を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dtim 5

3.1.37 fragment-threshold

Syntax

fragment-threshold *size*

undo fragment-threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、フラグメンテーションしきい値は 2346 バイトです。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

size: フラグメンテーションしきい値を指定します。範囲は 256～2346 バイトです。この引数の値は偶数でなければいけません。

説明

fragment-threshold コマンドはフレームのフラグメンテーションしきい値を設定します。

undo fragment-threshold コマンドはデフォルトに戻します。

フラグメンテーションしきい値より大きいフレームは、伝送の前にフラグメントされます。フラグメンテーションしきい値より小さいフレームは、フラグメントされずに伝送されます。

干渉が大きい WLAN では、ネットワーク処理能力と効率を向上させるために、フラグメンテーションしきい値を低く設定してください。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、フラグメンテーションしきい値を 2048 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] fragment-threshold 2048

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、フラグメンテーションしきい値を 2048 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] fragment-threshold 2048

3.1.38 green-energy-management

Syntax

green-energy-management { **disable** | **enable** }

undo green-energy-management

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、エネルギ節約機能は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: エネルギ節約機能を無効にします。

enable: エネルギ節約機能を有効にします。

説明

green-energy-management enable コマンドはエネルギ節約機能を有効にします。

green-energy-management disable コマンドはエネルギ節約機能を無効にします。

undo green-energy-management コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、エネルギ節約機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] green-energy-management enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、エネルギ節約機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] green-energy-management enable

3.1.39 ldpc

Syntax

ldpc { **disable** | **enable** }

undo ldpc

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、LDPC は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: LDPC を無効にします。

enable: LDPC を有効にします。

説明

ldpc enable コマンドは LDPC を有効にします。

ldpc disable コマンドは LDPC を無効にします。

undo ldpc コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

装置は LDPC パケットを受信できますが、送信することはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、LDPC を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] ldpc disable

AP グループ 1 の型番 **QX-W1020** の AP で、LDPC を無効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] ldpc disable

3.1.40 long-retry threshold

Syntax

long-retry threshold *count*

undo long-retry threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、大きいフレームの最大再送信回数は 4 回です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

count: 大きいフレームのハードウェア最大再送信回数を指定します。範囲は 1～15 です。

説明

long-retry threshold コマンドは大きいフレームのハードウェア最大再送信回数を設定します。

undo long-retry threshold コマンドはデフォルトに戻します。

このタスクを実行して、RTS しきい値を超えるフレームのハードウェア再送信の最大数を設定します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、大きいフレームのハードウェア最大再送信回数を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] long-retry threshold 5

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、大きいフレームのハードウェア最大再送信回数を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] long-retry threshold 5

関連コマンド

- **protection-threshold**
- **short-retry threshold**

3.1.41 max-power

Syntax

max-power *radio-power*

undo max-power

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP はサポートされる最大伝送電力を使用します。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

radio-power: 最大伝送電力を指定します。

QX-W1000 シリーズの範囲は

QX-W1010 の場合、radio 1 が 1～20dBm、radio 2 が 1～16dBm、

QX-W1020 の場合、radio 1 が 1～12dBm、radio 2 が 1～20dBm、radio 3 が 1～14dBm、

QX-W1030 の場合、radio 1 が 1～11dBm、radio 2 が 1～19dBm、radio 3 が 1～14dBm

です。

QX-W1100 シリーズの範囲は

ソフトウェアバージョン 7.2.63 を含む以前のソフトウェアでは、

QX-W1110 の場合、radio1 が 1～18dBm、radio2 が 1～16dBm、

QX-W1120 の場合、radio 1 が 1～11dBm、radio 2（2.4GHz）が 1～14dBm、radio2（5GHzW56 帯）が 1～19ｄBm、radio 3（2.4GHz）が 1～14dBm、radio3（5GHz、W56 帯）が 1～19ｄBm

QX-W1130 の場合、radio 1 が 1～13dBm、radio 2 が 1～20dBm、radio 3 が 1～14dBm

ソフトウェアバージョン 7.2.67 を含む以降のソフトウェアでは、

QX-W1110 の場合、radio1 が 1～18dBm、radio2 が 1～17dBm、

QX-W1120 の場合､radio 1 が 1～12dBm､radio 2(2.4GHz)が 1～15dBm、radio2(5GHz、W56 帯）が 1～19dBm、radio 3（2.4GHz）が 1～14dBm、radio3（5GHz、W56 帯）が 1～19ｄBm、

QX-W1130 の場合、radio 1 が 1～13dBm、radio 2 が 1～20dBm、radio 3 が 1～15dBm

です。

説明

max-power コマンドは最大伝送電力を設定します。

undo max-power コマンドはデフォルトに戻します。

無線でサポートされる伝送電力の範囲は、カントリーコード、チャネル、AP モデル、無線モード、アンテナタイプ、帯域幅モードにより変化します。最大伝送電力を設定後に無線に対するこれらの特性を変更した場合、設定された最大伝送電力がサポートされた伝送電力の範囲外になる可能性があります。この場合、システムは自動的に最大伝送電力を有効な値に適応させます。

電力ロックを有効にした場合、ロックされた電力が最大伝送電力になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、最大伝送電力を 11dBm に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] max-power 11

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、最大伝送電力を 11dBm に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] max-power 11

3.1.42 mu-txbf

Syntax

mu-txbf { **disable** | **enable** }

undo mu-txbf

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンによりデフォルト状態が異なります。

ソフトウェアバージョン7.2.21 を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.27, 7.2.27a から 7.2.59 のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン 7.2.63 のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.67 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: マルチユーザ送信ビームフォーミング（TxBF）を無効にします。

enable: マルチユーザ送信ビームフォーミング（TxBF）を有効にします。

説明

mu-txbf enable コマンドはマルチユーザ送信ビームフォーミング（TxBF）を有効にします。

mu-txbf disable コマンドはマルチユーザ送信ビームフォーミング（TxBF）を無効にします。

undo mu-txbf コマンドはデフォルトに戻します。

このコマンドは、802.11ac、802.11gac、802.11ax、802.11gax 無線にのみ適用されます。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、コマンドが無効になります。

TxBF を使用すると、AP はチャネル情報に基づいて送信パラメータを調整し、意図したクライアントに RF 信号を集中させることができます。この機能により、RF 信号の品質が向上します。

マルチユーザ TxBF は 802.11ac Wave2 の一部です。マルチユーザ TxBF を使用すると、異なる RF 信号を意図したクライアントに集中させ、干渉や伝送遅延を減らすことができます。これにより、トラフィックスループットと帯域幅使用率が改善されます。マルチユーザ TxBF は、多数のクライアントを持ち、高い帯域幅使用率と低い伝送遅延を必要とする WLAN に適用できます。

マルチユーザ TxBF は、シングルユーザ TxBF が有効な場合にのみ有効です。

マルチユーザ TxBF で有効になっている AP のデフォルトの MIMO 設定を変更しないことを推奨します。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** のマルチユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] su-txbf enable

[AC-wlan-ap-ap1-radio-1] mu-txbf enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、マルチユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] su-txbf enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] mu-txbf enable

関連コマンド

- **mimo**
- **su-txbf**

3.1.43 power-lock

Syntax

power-lock { **disable** | **enable** }

undo power-lock

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、電力ロック機能は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 電力ロック機能を無効にします。

enable: 電力ロック機能を有効にします。

説明

power-lock enable コマンドは電力ロック機能を有効にします。

power-lock disable コマンドは電力ロック機能を無効にします。

undo power-lock コマンドはデフォルトに戻します。

このコマンドは TPC(RRM)機能と同時に使用します。TPC(RRM)機能は電力値を自動的に変更します。変更中の電力値をそのまま継続して使用したい場合に"power-lock enable"にします。通常はこのコマンドを使用する必用はありません。電力値の変更が多い場合、一部の装置の電力値を固定して状況が変化するか確認することができます。

電力ロックを有効にした場合、現在の電力がロックされて最大伝送電力となります。ロックされた電力は、AC 再起動後も有効になります。

電力ロックが有効にされた無線が、ロックされた電力より低い電力を供給する新たなチャネルに切り替わった場合、新しいチャネルによってサポートされた最大電力が有効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、電力ロック機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] power-lock enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、電力ロック機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-lock enable

3.1.44 preamble

Syntax

preamble { **long** | **short** }

undo preamble

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、short が使用されます。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

long: 長いプリアンブルを指定します。 長いプリアンブルは、従来モデルのすべての無線装置との互換性が確保されます。

short: 短いプリアンブルを指定します。短いプリアンブルはネットワーク性能を改善します。

説明

preamble コマンドはプリアンブルタイプを設定します。

undo preamble コマンドはデフォルトに戻します。

本コマンドは、802.11b、802.11g、802.11gn 無線でのみ適用可能です。

プリアンブルとは、送信側と受信側の間で伝送信号を同期させるためのパケットヘッダ内のビットのセットです。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、プリアンブルタイプを **long** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] preamble long

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、プリアンブルタイプを **long** に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] preamble long

3.1.45 protection-mode

Syntax

protection-mode { **cts-to-self** | **rts-cts** }

undo protection-mode

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、CTS-to-self モードが使用されます。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

cts-to-self: CTS-to-self モードを指定します。

rts-cts: RTS/CTS モードを指定します。

説明

protection-mode コマンドは衝突回避モードを設定します。

undo protection-mode コマンドはデフォルトに戻します。

AP に対して以下の衝突回避モードのいずれかを指定することができます。

- **RTS/CTS**－AP は、クライアントにデータを送信する前に、RTS パケットを送信します。RTS パケットを受信した後、クライアントは CTS パケットを AP に送信します。CTS パケット受信後、AP はデータの送信を開始します。また、その RTS パケットもしくは CTS パケットを検出した別の装置が、指定された時間内にデータを送信することはありません。
- **CTS-to-self**－AP は、クライアントにデータを送信する前に、CTS パケットを送信します。この CTS パケットには、AP 自体の MAC アドレスが宛先 MAC アドレスとして付随されています。CTS-to-self パケット受信後、AP はデータの送信を開始します。また、その CTS-to-self パケットを受信した別の装置が、指定された時間内にデータを送信することはありません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、RTS/CTS モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] protection-mode rts-cts

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、RTS/CTS モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] protection-mode rts-cts

関連コマンド

- **dot11g protection**
- **dot11n protection**
- **protection-threshold**

3.1.46 protection-threshold

Syntax

protection-threshold *size*

undo protection-threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP グループ radio view では、RTS しきい値は 2346 バイトです。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

size: RTS しきい値を指定します。範囲は 0～2346 バイトです。

説明

protection-threshold コマンドは RTS しきい値を設定します。

undo protection-threshold コマンドはデフォルトに戻します。

システムは、パケットが RTS しきい値より大きい場合に限り衝突回避を実行します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、RTS しきい値を 2048 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] protection-threshold 2048

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、RTS しきい値を 2048 バイトに設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] protection-threshold 2048

関連コマンド

protection-mode

3.1.47 radar-channel-switchback disable

🕮 **メモ：**

- QX-W1100 シリーズの Anchor-AC は、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからこのコマンドをサポートしています。
- QX-W1000 シリーズの Anchor-AC は、ソフトウェアバージョン 7.2.74 を含む以降のソフトウェアからこのコマンドをサポートしています。

Syntax

radar-channel-switchback disable

undo radar-channel-switchback

デフォルト

有効

View

Global configuration view

定義済みユーザロール

network-admin

説明

radar-channel-switchback disable コマンドは、レーダチャネルスイッチバックを無効にします。

undo radar-channel-switchback コマンドは、デフォルトに戻します。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。

レーダチャネルスイッチバックを無効にすると、レーダ信号の検出によるチャネル変更をしてから 30 分経過しても、AP が元のチャネルに切り替えないようにすることができます。この場合、AP は新しいチャネルを使用し続けます。

例

レーダチャネルスイッチバックを無効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] radar-channel-switchback disable

3.1.48 radio

Syntax

radio *radio-id*

View

AP view

AP group AP model view

定義済みユーザロール

network-admin

パラメータ

radio-id: 無線を ID で指定します。範囲は装置モデルにより異なります。

説明

radio コマンドは radio view に入ります。

例

radio view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1]

AP グループ radio view に移行します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-apgroup1] ap-model QX-W1020

[AC-wlan-ap-apgroup1-ap-model-QX-W1020] radio 1

3.1.49 radio { disable | enable }

Syntax

radio { **disable** | **enable** }

undo radio

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、無線は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 無線を無効にします。

enable: 無線を有効にします。

説明

radio enable コマンドは無線を有効にします。

radio disable コマンドは無線を無効にします。

undo radio コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、無線を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] radio enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、無線を有効にします。

Enable radio 1 for APs with model QX-W1020 in AP group apgroup1.

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] radio enable

3.1.50 radio-type 2.4g

🕮 メモ：

radio-type 2.4g コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

radio-type 2.4g { dot11g | dot11gac | dot11gax | dot11gn }

undo radio-type 2.4g

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11g: 802.11g モードを指定します。

dot11gac: 802.11gac モードを指定します。

dot11gax: 802.11gax モードを指定します。

dot11gn: 802.11n (2.4 GHz) モードを指定します。

説明

radio-type 2.4g コマンドは 2.4 GHz 帯の無線モードを指定します。

undo radio-type 2.4g コマンドはデフォルトに戻します。

デフォルトでは、無線に設定した無線モードが、この無線によって提供されるすべての BSS に適用されます。

無線が異なる無線モードを使用して BSS を提供するには、このコマンドを実行してサービステンプレート毎に異なる無線モードを指定し、サービステンプレートを無線にバインドします。

2.4 GHz 無線モードのレベルは、802.11gax、802.11gac、802.11gn、802.11g の順に低くなります。Service template view と Radio view の両方で無線モードを設定すると、下位レベルの無線モードが有効になります。無線表示で指定した無線モードのレベルが、バインドされたサービステンプレートのいずれかで指定した無線モードよりも高いことを確認してください。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

2.4 GHz 帯の無線モードを 802.11 n に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] radio-type 2.4g dot11gn

関連コマンド

display wlan service-template

3.1.51 radio-type 5g

🕮 **メモ**:

radio-type 5g コマンドはソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

radio-type 5g { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** }

undo radio-type 5g

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a モードを指定します。

dot11ac: 802.11ac モードを指定します。

dot11an: 802.11n (5 GHz)モードを指定します。

dot11ax: 802.11ax モードを指定します。

説明

radio-type 5g コマンドは 5 GHz 帯の無線モードを指定します。

undo radio-type 5g コマンドはデフォルトに戻します。

デフォルトでは、無線に設定した無線モードが、この無線によって提供されるすべての BSS に適用されます。

無線が異なる無線モードを使用して BSS を提供するには、このコマンドを実行してサービステンプレート毎に異なる無線モードを指定し、サービステンプレートを無線にバインドします。

5 GHz 無線モードのレベルは、802.11ax、802.11ac、802.11an、802.11a の順に低くなります。Service template view と Radio view の両方で無線モードを設定すると、下位レベルの無線モードが有効になります。Radio view で指定した無線モードのレベルが、バインドされたサービステンプレートのいずれかで指定した無線モードよりも高いことを確認してください。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

5 GHz 帯の無線モードを 802.11 n に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] radio-type 5g dot11an

関連コマンド

display wlan service-template

3.1.52 rate

Syntax

rate { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }

undo rate

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では以下となります。

- 802.11a/802.11an/802.11ac/802.11ax
  - **禁止速度**－なし

- **必須速度**－6、12、24
- **マルチキャスト速度**－必須速度から選択されます。
- **サポート速度**－9、18、36、48、54

- 802.11b
  - **禁止速度**－なし
  - **必須速度**－1、2
  - **マルチキャスト速度**－最大の必須速度
  - **サポート速度**－5.5、11
- 802.11g/802.11gn/802.11gac
  - **禁止速度**－なし
  - **必須速度**－1、2、5.5、11
  - **マルチキャスト速度**－必須速度から選択
  - **サポート速度**－6、9、12、18、24、36、48、54

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disabled: AP で使用できない速度を指定します。

mandatory: AP と接続するためにクライアントがサポートしなければならない速度を指定します。

multicast: AP がパケットをマルチキャストする速度を指定します。マルチキャスト速度は、必須速度の中から選択されなければなりません。

supported: AP がサポートする速度を指定します。クライアントが AP と接続した後に、クライアントは AP と通信するために、サポートされた速度の中から、より高い速度や低い速度を選択することが可能です。

auto: マルチキャスト速度として、必須速度を自動的に選択します。

rate-value: 速度を Mbps で指定します。スペース区切りで複数の速度を設定することができます。利用可能な引数は以下の通りです。

- **802.11a/802.11an/802.11ac/802.11ax**－6、9、12、18、24、36、48、54
- **802.11b**－1、2、5.5、11
- **802.11g/802.11gn802.11gac**－1、2、5.5、6、9、11、12、18、24、36、48、54

説明

rate コマンドは無線の伝送速度を設定します。

undo rate コマンドはデフォルトに戻します。

必須速度とマルチキャスト速度を未設定にすることはできません。必須速度が 1 種類しかない場合は、サポート速度または禁止速度として必須速度を指定することはできません。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、必須速度として 6Mbps、12Mbps、24Mbps を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rate mandatory 6 12 24

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、必須速度として 6Mbps、12Mbps、24Mbps を設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] rate mandatory 6 12 24

3.1.53 reset wlan statistics ap radio

🕮 **メモ**:

- **reset wlan statistics ap radio** コマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

reset wlan statistics ap { **all** | **name** *ap-name* } **radio**

View

User view

定義済みユーザロール

network-admin

パラメータ

ap: AP を指定します。

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

reset wlan statistics ap radio コマンドは無線統計情報を削除します。

例

#AP **ap1** の無線統計情報を削除します

<AC> reset wlan statistics ap name ap1 radio

3.1.54 short-gi

Syntax

short-gi { **disable** | **enable** }

undo short-gi

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ショート GI は有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: ショート GI(Guard Interval)を無効にします。

enable: ショート GI(Guard Interval)を有効にします。

説明

short-gi enable コマンドはショート GI(Guard Interval)を有効にします。

short-gi disable コマンドはショート GI(Guard Interval)を無効にします。

undo short-gi コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、ショート GI を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] short-gi disable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、ショート GI を無効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] short-gi disable

3.1.55 short-retry threshold

Syntax

short-retry threshold *count*

undo short-retry threshold

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、小さいフレームのハードウェア最大再送信回数は 7 回です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

count: 小さいフレームのハードウェア最大再送信回数を指定します。範囲は 1～15 です。

説明

short-retry threshold コマンドは小さいフレームのハードウェア最大再送信回数を設定します。

undo short-retry threshold コマンドはデフォルトに戻します。

このタスクを実行して、RTS しきい値未満のフレームのハードウェア再送信の最大数を設定します。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、小さいフレームのハードウェア最大再送信回数を 10 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] short-retry threshold 10

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、小さいフレームのハードウェア最大再送信回数を 10 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] short-retry threshold 10

関連コマンド

- **long-retry threshold**
- **protection-threshold**

3.1.56 stbc

Syntax

stbc { **disable** | **enable** }

undo stbc

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、STBC は有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: STBC を無効にします。

enable: STBC を有効にします。

説明

stbc enable コマンドは STBC を有効にします。

stbc disable コマンドは STBC を無効にします。

undo stbc コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gac 無線にのみ適用可能です。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、STBC を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] stbc enable

AP グループ 1 の型番 **QX-W1020** の AP で、STBC を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] stbc enable

3.1.57 su-txbf

Syntax

su-txbf { **disable** | **enable** }

undo su-txbf

デフォルト

radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンによりデフォルト状態が異なります。

ソフトウェアバージョン7.2.21 を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.27, 7.2.27a から 7.2.59 のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン 7.2.63 のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン7.2.67 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: シングルユーザの TxBF を無効にします。

enable: シングルユーザの TxBF を有効にします。

説明

su-txbf enable コマンドはシングルユーザの TxBF を有効にします。

su-txbf disable コマンドはシングルユーザの TxBF を無効にします。

undo su-txbf コマンドはデフォルトに戻します。

このコマンドは、802.11ac、802.11gac、802.11ax、802.11gax 無線にのみ適用されます。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、コマンドが無効になります。

シングルユーザ TxBF を使用すると、AP は目的の 1 つのクライアントへの信号を改善できます。シングルユーザ TxBF は、広く普及しているクライアント、ネットワーク品質の悪い WLAN、および深刻な信号減衰に適用されます。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** のシングルユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] su-txbf enable

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、シングルユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] su-txbf enable

関連コマンド

mu-txbf

3.1.58 twt negotiate

🕮 **メモ**：

- **twt negotiate** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **twt negotiate** コマンドは QX-W1100 シリーズの AP でのみサポートしています。

Syntax

twt negotiate { **disable** | **enable** }

undo twt negotiate

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン V7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

twt negotiate enable コマンドは Target Wake Time(TWT)ネゴシエーションを有効にします。

twt negotiate disable コマンドは TWT ネゴシエーションを無効にします。

undo twt negotiate コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

Trget Wake Time (TWT) ネゴシエーションを使用すると、クライアントと AP はサービス期間中にのみデータパケットを交換し、クライアントの休止状態をスケジュールして、クライアントの電力消費量と無線リソースの競合を減らすことができます。

TWT ネゴシエーションを有効にすると、クライアントはサービス期間、TWT 間隔、および最初のスリープ状態解除時間(クライアントによって計算される)を含むネゴシエーション要求を AP に送信します。このような要求を受信すると、AP は応答を送信します。クライアントはスケジュールに従って起動し、その AP からのトリガーフレームを待機します。トリガーフレームを受信すると、クライアントはサービス期間に入り、その AP とのデータパケットの交換を開始します。サービス期間が終了すると、データパケットの交換が完了していなくても、クライアントは休止モードに入ります。

無線は、最大 8 台のクライアントに TWT サービスを提供できます。8 つのクライアントの TWT ネゴシエーション要求に応答した後、無線は他のクライアントからの要求を拒否します。

Radio view の設定は AP group radio view の設定よりも優先されます。

例

AP ap1 の Radio1 で TWT ネゴシエーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] twt negotiate enable

AP グループ apgroup1 の AP の Radio1 で TWT ネゴシエーションを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] twt negotiate enable

関連コマンド

type dot11ax

3.1.59 type

Syntax

type { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gn** }

undo type

デフォルト

QX-W1010 の Radio1、Radio2 の無線モードは、それぞれ dot11ac、dot11gn です。

QX-W1020、QX-W1030 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ac、dot11ac、dot11gn です。

QX-W1110 の Radio1、Radio2 の無線モードは、それぞれ dot11ax、dot11gax です。

QX-W1120 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ax、dot11ax、dot11gn です。

QX-W1130 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ax、dot11ax、dot11gax です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11an: 802.11n(5GHz)無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gac: 802.11gac 無線モードを指定します。

dot11gax: 802.11gax 無線モードを指定します。

dot11gn: 802.11n(2.4GHz)無線モードを指定します。

🕮 **メモ：**

802.11ac を 2.4GHz で使用するモードを 802.11gac と定義します。
802.11ax を 2.4GHz で使用するモードを 802.11gax と定義します。

説明

type コマンドは無線モードを指定します。

undo type コマンドはデフォルトに戻します。

⚠ **注意：**

有効になっている無線のモードを変更すると、すべての接続されたクライアントが接続解除されます。

🕮 **メモ：**

- QX-W1100 シリーズは Raido3 で 802.11a、ac、an も指定できますが設定した場合 Raido3 が無効になります。
- QX-W1120 は Radio3 で 802.11gax を設定することができません。Radio 3 を 802.11a、ac、an のいずれかに設定することで、Radio 2 を 802.11gax に設定することができます。

AP group radio view で無線のモードを変更すると、無線のモードに関連するコマンドのデフォルト設定が復元されます。

radio view の設定は、AP group radio view の設定に優先します。

例

AP **ap1** で、無線モードを 802.11n (5 GHz)に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

AP グループ **apgroup1** の型番 **QX-W1020** の AP で、無線モードを 802.11n (5 GHz)に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

3.1.60 ul-ofdma

🕮 **メモ**:

- **ul-ofdma** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **ul-ofdma** コマンドは QX-W1100 シリーズの AP でのみサポートしています。

Syntax

ul-ofdma { **disable** | **enable** }

undo ul-ofdma

デフォルト

radio view では、AP group radio view の設定を使用します。

AP group radio view では、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.55 を含む以前のソフトウェアでは無効(コンフィグ上は非表示)です。

ソフトウェアバージョン V7.2.56 を含む以降のソフトウェアでは有効(コンフィグ上は非表示)です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

ul-ofdma enable コマンドはアップリンク OFDMA を有効にします。

ul-ofdma disable コマンドはアップリンク OFDMA を無効にします。

undo ul-ofdma コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

Radio view の設定は AP group radio view の設定よりも優先されます。

OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります。

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮
- 衝突バックオフの削減

例

AP ap1 の Radio1 でアップリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] ul-ofdma enable

AP グループ apgroup1 の AP の Radio1 でアップリンク OFDMA を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] ul-ofdma enable

関連コマンド

type dot11ax

3.1.61 wlan radio

Syntax

wlan radio { **disable** | **enable** }

undo wlan radio

デフォルト

radio view または AP group radio view で無線が有効になっていない場合、無線は無効になります。

View

System view

定義済みユーザロール

network-admin

パラメータ

disable: すべての無線を無効にします。

enable: すべての無線を有効にします。

説明

wlan radio enable コマンドはすべての無線を有効にします。

wlan radio disable コマンドはすべての無線を無効にします。

undo wlan radio コマンドはデフォルトに戻します。

⚠ **注意**：

この機能は、すべての手動 AP とオンライン自動 AP で有効です。

---

wlan radio { **disable** | **enable** }コマンドと **radio** { **disable** | **enable** }コマンドを使用すると、最新の設定が有効になります。

例

すべての無線を有効にする。

<AC> system-view

[AC] wlan radio enable

関連コマンド

radio { **disable** | **enable** }

目次

4 章 WLAN アクセスの設定 4-1
4.1 WLAN アクセスの設定コマンド 4-1
4.1.1 access-control acl 4-1
4.1.2 beacon ssid-hide 4-2
4.1.3 broadcast-probe reply 4-3
4.1.4 client association-location 4-5
4.1.5 client cache aging-time 4-6
4.1.6 client forwarding-location 4-7
4.1.7 client frame-format 4-8
4.1.8 client idle-timeout 4-9
4.1.9 client keep-alive 4-10
4.1.10 client keep-alive interval 4-11
4.1.11 client max-count 4-12
4.1.12 client preferred-vlan authorized 4-13
4.1.13 client vlan-alloc 4-13
4.1.14 description 4-14
4.1.15 display wlan ap region-code 4-15
4.1.16 display wlan blacklist 4-16
4.1.17 display wlan bss 4-17
4.1.18 display wlan client 4-19
4.1.19 display wlan client device-information 4-27
4.1.20 display wlan client failure 4-28
4.1.21 display wlan client online-duration 4-30
4.1.22 display wlan client status 4-31
4.1.23 display wlan service-template 4-33
4.1.24 display wlan statistics client 4-39
4.1.25 display wlan statistics connect-history 4-40
4.1.26 display wlan statistics service-template 4-42
4.1.27 display wlan whitelist 4-43
4.1.28 inherit exclude service-template 4-44
4.1.29 map-configuration 4-45
4.1.30 nas-id 4-46
4.1.31 nas-port-id 4-47
4.1.32 nas-vlan 4-48
4.1.33 quick-association enable 4-49
4.1.34 region-code 4-50
4.1.35 region-code-lock 4-51

4.1.36 reset wlan client 4-53
4.1.37 reset wlan dynamic-blacklist 4-53
4.1.38 reset wlan statistics client 4-54
4.1.39 reset wlan statistics service-template 4-55
4.1.40 service-template 4-56
4.1.41 service-template enable 4-57
4.1.42 snmp-agent trap enable wlan client 4-58
4.1.43 snmp-agent trap enable wlan client-audit 4-59
4.1.44 ssid 4-59
4.1.45 unknown-client 4-61
4.1.46 user-profile 4-62
4.1.47 vlan 4-63
4.1.48 wlan client failure history aging 4-64
4.1.49 wlan client forwarding enable 4-64
4.1.50 wlan client reauthentication-period 4-65
4.1.51 wlan dynamic-blacklist active-on-ap 4-66
4.1.52 wlan dynamic-blacklist lifetime 4-67
4.1.53 wlan link-test 4-68
4.1.54 wlan nas-port-id format 4-70
4.1.55 wlan permit-ssid 4-71
4.1.56 wlan service-template 4-72
4.1.57 wlan static-blacklist mac-address 4-72
4.1.58 wlan web-server api-path 4-73
4.1.59 wlan web-server host 4-74
4.1.60 wlan web-server max-client-entry 4-75
4.1.61 wlan whitelist mac-address 4-76

4章 WLAN アクセスの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

4.1 WLANアクセスの設定コマンド

4.1.1 access-control acl

🕮 メモ：

access-control acl コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

access-control acl *acl-number*

undo access-control acl

デフォルト

設定無し

View

AP view

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number: レイヤ 2 ACL の番号を 4000 から 4999 の範囲で指定します。

説明

access-control acl コマンドは ACL にもとづくアクセスに使用する ACL を設定します。

undo access-control acl コマンドはデフォルトに戻します。

この機能は、指定された ACL ルールを使用してクライアントアクセスを制御します。デバイスはアソシエーション要求を受信すると、次のアクションを実行します。

- クライアントの MAC アドレスがルール内の MAC アドレス属性または MAC アドレス OUI 属性と一致し、ルールアクションが permit の場合に、クライアントに WLAN

へのアクセスを許可します。複数のクライアントが OUI 属性に一致する場合、これらのすべてのクライアントは WLAN へのアクセスを許可されます。

- 一致するルールが見つからない場合、または一致するルールのアクションが deny の場合、クライアントの WLAN へのアクセスを拒否します。

この機能を設定する場合は、次の制約事項および注意事項に従ってください。

- 指定した ACL に permit ルールが設定されていない場合、クライアントのアクセスは許可されません。
- 指定できる ACL は 1 つだけです。このコマンドを複数回実行した場合は、最新の設定が有効になります。
- AP View の設定は、サービステンプレート View の設定よりも優先されます。

例

ACL 4000 を作成し、MAC アドレスが 006e-35b2-000e のクライアントおよび指定された OUI のクライアントアクセスを許可する ACL ルールを作成します。サービステンプレート service 1 に ACL4000 を指定します。

<AC> system-view

[AC] acl mac 4000

[AC-acl-mac-4000] rule 0 permit source-mac 006e-35b2-000e ffff-ffff-ffff

[AC-acl-mac-4000] rule 1 permit source-mac 006e-3500-0000 ffff-ff00-0000

[AC-acl-mac-4000] quit

[AC] wlan service-template service1

[AC-wlan-st-service1] access-control acl 4000

ACL 4000 を作成し、MAC アドレスが 006e-35b2-000e のクライアントおよび指定された OUI のクライアントを許可する ACL ルールを作成します。AP ap1 に ACL 4000 を指定します。

<AC> system-view

[AC] acl mac 4000

[AC-acl-mac-4000] rule 0 permit source-mac 006e-35b2-000e ffff-ffff-ffff

[AC-acl-mac-4000] rule 1 permit source-mac 006e-3500-000f ffff-ff00-0000

[AC-acl-mac-4000] quit

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] access-control acl 4000

4.1.2 beacon ssid-hide

Syntax

beacon ssid-hide

undo beacon ssid-hide

デフォルト

SSID はビーコンフレームでアドバタイズされます。

View

Service template view

定義済みユーザロール

network-admin

説明

beacon ssid-hide コマンドはビーコンフレームでサービスセット識別子（SSID）のアドバタイズを無効にします。

undo beacon ssid-hide コマンドはデフォルトに戻します。

このコマンドを有効にすると、無線がビーコンフレーム内で SSID を伝送しないようになり、指定したサービステンプレートが無線にバインドされた後にプローブ要求に応答しなくなります。

例

ビーコンフレームで SSID の通知を無効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] beacon ssid-hide

4.1.3 broadcast-probe reply

Syntax

broadcast-probe reply { **disable** | **enable** }

undo broadcast-probe reply

デフォルト

AP view：AP group view の設定を使用します。

AP group view：ブロードキャストプローブ要求に応答します。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: AP のブロードキャストプローブ要求への応答を無効にします。

enable: AP のブロードキャストプローブ要求への応答を有効にします。

説明

broadcast-probe reply enable コマンドは AP がブロードキャストプローブ要求に応答できるようにします。

broadcast-probe reply disable コマンドは AP がブロードキャストプローブ要求に応答できなくなります。(SSID が空欄である場合の ANY 接続拒否)

undo broadcast-probe reply コマンドはデフォルトに戻します。

ブロードキャストプローブ要求には SSID は含まれません。AP はブロードキャストプローブ要求を受信すると、AP のサービス情報を含んだプローブ応答を返信します。ユニキャストプローブ要求を送信するクライアントが AP に接続することができるようにするには、AP がブロードキャストプローブ要求に応答しないようにします。

AP view の設定は、AP group view の設定よりも優先されます。

🕮 **メモ：**

SSID が“ANY”の文字列である ANY 接続は、本コマンドの有効無効に限らず“ANY”の文字列を持つサービステンプレートを作成しなければ接続されません。

例

AP **ap1** をブロードキャストプローブ要求に応答しないようにします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] broadcast-probe reply disable

AP グループ **group1** の AP をブロードキャストプローブ要求に応答しないようにします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] broadcast-probe reply disable

4.1.4 client association-location

Syntax

client association-location { **ac** | **ap** }

undo client association-location

デフォルト

AC

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac: AC でのクライアントの関連付けを有効にします。

ap: AP でのクライアントの関連付けを有効にします。

説明

client association-location コマンドは AC または AP でのクライアントアソシエーションを有効にします。

undo client association-location コマンドはデフォルトに戻します。

client association-location コマンドと **client-security authentication-location** コマンドでは同一の装置を指定してください。**client-security authentication-location** コマンドの詳細については、*コマンドマニュアルの“WLAN 認証”*を参照してください。

このコマンドを実行する前に、サービステンプレート が無効であることを確認してください。

例

AC でのクライアントの関連付けを有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client association-location ac

関連コマンド

client-security authentication-location（*コマンドマニュアルの “WLAN 認証”*）

4.1.5 client cache aging-time

Syntax

client cache aging-time aging-time

undo client cache aging-time

デフォルト

180 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

aging-time: エージングタイムを指定します。設定範囲は 0～86400 秒です。エージングタイムを 0 に設定した場合、クライアントがオフラインになった直後にクライアントのキャッシュ情報を削除します。

説明

client cache aging-time コマンドはクライアントキャッシュエージングタイムを設定します。

undo client cache aging-time コマンドはデフォルトに戻します。このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

クライアントキャッシュは、クライアント用の PMK リストやアクセス VLAN などの情報を保存します。クライアントはキャッシュエージングタイムが経過する前に別の AP にローミングすると、キャッシュ情報を継承できます。キャッシュエージングタイムが経過する前にクライアントがオンラインにならない場合、そのキャッシュ情報はクリアされます。

例

エージングタイムを 100 秒に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client cache aging-time 100

4.1.6 client forwarding-location

Syntax

client forwarding-location { **ac** | **ap** }

undo client forwarding-location

デフォルト

AP

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac: AC がクライアントデータトラフィックを転送します。

ap: AP がクライアントデータトラフィックを転送します。

説明

client forwarding-location コマンドはクライアントデータトラフィックフォワーダを指定します。

ソフトウェアバージョン 7.2.19 を含む以前のソフトウェアでは、**undo client forwarding-location** コマンドは ac が設定されます。

ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでは、**undo client forwarding-location** コマンドは ap が設定されます。

このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

AC トラフィックがクライアントトラフィックフォワーダとして設定されている場合、クライアントのトラフィックフォワーディングが有効になっていることを確認してください。

例

AP がクライアントデータトラフィックを転送するように設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client forwarding-location ap

4.1.7 client frame-format

Syntax

client frame-format { **dot3** | **dot11** }

undo client frame-format

デフォルト

802.3 カプセル化フォーマット

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot3: クライアントデータフレームを 802.3 フォーマットでカプセル化します。

dot11: クライアントデータフレームを 802.11 フォーマットでカプセル化します。

説明

client frame-format コマンドはクライアントデータフレームのカプセル化モードを設定します。

undo client frame-format コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

このコマンドは、中央転送モードでのみ有効です。

例

#クライアントデータフレームを 802.11 フォーマットでカプセル化します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client frame-format dot11

関連コマンド

client forwarding-location

4.1.8 client idle-timeout

Syntax

client idle-timeout *interval*

undo client idle-timeout

デフォルト

AP view：AP group view の設定を使用します。

AP group view：

ソフトウェアバージョン 7.2.79b を含む以前のソフトウェアは 3600 秒

ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアは 300 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: クライアントアイドルタイムアウト時間を指定します。設定範囲は 60～86400 秒です。

説明

client idle-timeout コマンドはクライアントアイドルタイムアウトタイマを設定します。

undo client idle-timeout コマンドはデフォルトに戻します。

クライアントアイドルタイムアウト時間内にオンラインクライアントが接続した AP にフレームを送信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1** のクライアントアイドルタイムアウト時間を 2000 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] client idle-timeout 2000

AP group **group1** のクライアントアイドルタイムアウト時間を 2000 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] client idle-timeout 2000

4.1.9 client keep-alive

Syntax

client keep-alive { **disable** | **enable** }

undo client keep-alive

デフォルト

AP view： AP group view の設定を使用します。

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: クライアントキープアライブを無効にします。

enable: クライアントキープアライブを有効にします。

説明

client keep-alive enable コマンドはクライアントキープアライブを有効にします。

client keep-alive disable コマンドはクライアントキープアライブを無効にします。

undo client keep-alive コマンドはデフォルトに戻します。

AP は、クライアントにキープアライブ間隔でキープアライブパケットを送信し、クライアントがオンラインかどうかを確認できます。キープアライブ間隔 3 回でクライアントからの応答を受信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1 のクライアントキープアライブを有効にします。**

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] client keep-alive enable

AP group **group1**.**のクライアントキープアライブを有効にします。**

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] client keep-alive enable

関連コマンド

client keep-alive interval

4.1.10 client keep-alive interval

Syntax

client keep-alive interval *value*

undo client keep-alive interval

デフォルト

AP view：AP group view の設定を使用します。

AP group view：300 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: クライアントのキープアライブ間隔を指定します。設定範囲は 3～1800 秒です。

説明

client keep-alive interval コマンドはクライアントキープアライブ間隔を設定します。

undo client keep-alive interval コマンドはデフォルトに戻します。

このコマンドを実行する前に、クライアントキープアライブを有効にしてください。

AP は、クライアントにキープアライブ間隔でキープアライブパケットを送信し、クライアントがオンラインかどうかを確認できます。キープアライブ間隔 3 回でクライアントからの応答を受信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap1 の**キープアライブ間隔を 20 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] client keep-alive interval 20

AP group **group1 の**キープアライブ間隔を 20 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] client keep-alive interval 20

関連コマンド

client keep-alive enable

4.1.11 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

制限なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

max-number: 1～512 の範囲内のクライアントの最大数を指定します。

説明

client max-count コマンドはサービステンプレートに関連するクライアントの最大数を設定します。

undo client max-count コマンドはデフォルトに戻します。

この機能を設定すると、新しいクライアントは最大数に達すると WLAN にアクセスできなくなります。

例

サービステンプレート **service1** の関連するクライアントの最大数を 38 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client max-count 38

4.1.12 client preferred-vlan authorized

Syntax

client preferred-vlan authorized

undo client preferred-vlan authorized

デフォルト

クライアントは、ローミング後に許可 VLAN を使用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client preferred-vlan authorized コマンドはローミング後に許可 VLAN を優先するようにクライアントを設定します。

undo client preferred-vlan authorized コマンドはローミング後にクライアント VLAN が変更されないように設定します。

この機能は 802.1X および MAC 認証クライアントでのみ有効です。

通常、クライアントの VLAN は、クライアントのローミング後も変更されません。ただし、クライアントが別の AP にローミングした後に QMC で設定されたセキュリティ警告をトリガすると、ユーザ分離のために発行された許可 VLAN が有効になります。

例

ローミング後に許可 VLAN を優先するようにクライアントを設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client preferred-vlan authorized

4.1.13 client vlan-alloc

Syntax

client vlan-alloc { **dynamic** | **static** }

undo client vlan-alloc { **dynamic** | **static** }

デフォルト

dynamic

View

Service template view

定義済みユーザロール

Predefined user roles

network-admin

パラメータ

dynamic: ダイナミック VLAN 割り当てを指定します。

static: スタティック VLAN 割り当てを指定します。

説明

client vlan-alloc コマンドはクライアントの VLAN 割り当て方法を指定します。

undo client vlan-alloc コマンドはデフォルトに戻します。

クライアントが初めてオンラインになると、無線はランダムな VLAN を割り当てます。クライアントが再びオンラインになると、クライアントに割り当てられた VLAN は割り当て方法に依存します。

- **Static allocation**−クライアントは、割り当てられた VLAN を継承します。IP アドレスのリースが期限切れになっていない場合、クライアントは同じ IP アドレスを使用します。この方法は、IP アドレスを節約するのに役立ちます。
- **Dynamic allocation**−クライアントに VLAN が再割り当てされます。この方法では、すべての VLAN のクライアントで負荷を分散させます。

例

クライアントの VLAN 割り当て方法をダイナミックに指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client vlan-alloc dynamic

4.1.14 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

text: description 名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

description コマンドはサービステンプレートの説明を構成します。

undo description コマンドはデフォルトに戻します。

例

サービステンプレート service1 に description 名 wlanst を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] description wlanst

4.1.15 display wlan ap region-code

Syntax

display wlan ap { **all** | **name** *ap-name* } **region-code**

View

すべての view

定義済みユーザロール

network-admin

パラメータ

all: 全ての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan region-code ap コマンドはすべての AP または指定した AP の地域コード情報を表示します。

例

すべての AP の地域コード情報を表示します。

<AC> display wlan ap all region-code

```
Region Code
--------------------------------------------------------------------------
AP name              Region Code
ap1                  JP  JAPAN
ap2                  JP  JAPAN
ap3                  JP  JAPAN
```

表 4-1 コマンド出力

フィールド	説明
Region Code	地域コード。地域コードの詳細については、表 4-13を参照してください。

4.1.16 display wlan blacklist

Syntax

display wlan blacklist { **dynamic** | **static** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: 動的なブラックリストを指定します。

static: 静的なブラックリストを指定します。

説明

display wlan blacklist コマンドはブラックリストエントリを表示します。

例

静的なブラックリストエントリを表示します。

<AC> display wlan blacklist static

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

動的なブラックリストエントリを表示します。

<AC> display wlan blacklist dynamic

```
Total number of clients: 3
MAC address    APID  Lifetime (s)  Duration (hh:mm:ss)
000f-e2cc-0001  1    300           00:02:11
000f-e2cc-0002  2    300           00:01:17
000f-e2cc-0003  3    300           00:02:08
```

表 4-2 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
APID	不正なクライアントを検出したAPのID。
Lifetime (s)	エントリの寿命（秒単位）。
Duration (hh:mm:ss)	エントリが動的ブラックリストに追加されてからエントリ期間。

4.1.17 display wlan bss

🕮 メモ：

display wlan bss コマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan bss { **all** | **ap** *ap-name* | **bssid** *bssid* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての BSS を表示します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

bssid *bssid*: BSS を ID で指定します。ID は、48 ビットの 16 進数で H-H-H の形式で指定してください。

verbose: 詳細な BSS 情報を表示します。 このキーワードを指定しない場合、BSS 情報の概要を表示します。

説明

display wlan bss コマンドは BSS（Basic Service Set）情報を表示します。

例

すべての BSS の簡潔な情報を表示します。

<AC> display wlan bss all

```
Current BSS number: 4
Max BSS number: 400
Bound BSS number: 4
AP name                RID  SSID                      BSSID
ap1                    1    SSID1                     0f00-ef65-6400
ap1                    2    SSID1                     0f00-ef65-6401
ap2                    1    SSID1                     0f00-ef14-dd08
ap2                    2    SSID1                     0f00-ef14-dd09
```

ID が 0f00-ef65-6400 の BSS の詳細情報を表示します。

<AC> display wlan bss bssid 0f00-ef65-6400 verbose

```
AP name                    : ap1
BSSID                      : 0f00-ef65-6400
Radio ID                   : 1
Service template name      : servcie1
SSID                       : SSID1
VLAN ID                    : 1
Service VLAN ID            : N/A
AKM mode                   : Not configured
User authentication mode   : Bypass
```

表 4-3 コマンド出力

フィールド	説明
AKM mode	AKMモード： • 802.1X • PSK • 設定なし
User authentication mode	ユーザ認証モード： • **Bypass**ークライアント認証なし • **MAC** • **802.1X** • **OUI**

4.1.18 display wlan client

Syntax

display wlan client [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5** }] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

radio *radio-id*: 指定した無線に接続されているクライアントに関する情報を表示します。*radio-id* の範囲は、デバイスモデルによって異なります。このオプションを指定しないと、指定した AP に接続されているすべてのクライアントに関する情報が表示されます。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

service-template *service-template-name*: 指定したサービステンプレートに関連付けられているクライアントに関する情報を表示します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

frequency-band: 指定されたバンドで作業しているクライアントに関する情報を表示します。

2.4: 2.4GHz 帯を指定します。

5: 5GHz 帯を指定します。

verbose: 詳細なクライアント情報を表示します。このキーワードを指定しない場合、クライアント情報の概要を表示します。

説明

display wlan client コマンドはクライアント情報を表示します。

例

すべてのクライアントに関する簡潔なクライアント情報を表示します。

<AC> display wlan client

```
Total number of clients: 3

MAC address    Username  AP name       RID   IP address     IPv6 address   VLAN
000f-e265-6400 N/A       ap1           1     1.1.1.1                       100
000f-e265-6401 user      ap2           1     3.0.0.3                       200
000f-e214-dd08 N/A       ap1           1     5.5.5.3        1::2:0:0:3     1
```

表 4-4 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
Username	クライアントユーザ名 ● クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） ● **N/A**（802.1X認証またはMAC認証を使用していない場合） 🕮 **メモ：** クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。
AP name	クライアントが関連付けられているAPの名前。
RID	クライアントが関連付けられている無線のID。
IP address	クライアントのIPv4アドレス。
IPv6 address	クライアントのIPv6アドレス。
VLAN ID	クライアントが属するVLANのID。

すべてのクライアントに関する詳細なクライアント情報を表示します。

<AC> display wlan client verbose

```
Total number of clients: 1

MAC address                    : 000f-e265-6400
IPv4 address                   : 10.1.1.114
IPv6 address                   : 2001::1234:5678:0102:0304
Username                       : N/A
AID                            : 1
AP ID                          : 1
AP name                        : ap1
Radio ID                       : 1
SSID                           : office
BSSID                          : 0026-3e08-1150
VLAN ID                        : 3
Sleep count                    : 0
Wireless mode                  : 802.11ac
 Channel bandwidth             : 80MHz
 SM power save                 : Disabled
 Short GI for 20MHz            : Supported
 Short GI for 40MHz            : Supported
 Short GI for 80MHz            : Supported
 Short GI for 160/80+80MHz     : Not supported
 STBC RX capability            : Supported
 STBC TX capability            : Supported
 LDPC RX capability            : Supported
 Beamformee STS capability     : N/A
 Number of Sounding Dimensions : N/A
 SU beamformee capability      : Not supported
 MU beamformee capability      : Not supported
 Block Ack                     : N/A
 Supported VHT-MCS set         : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
 Supported HT MCS set          : 0, 1, 2, 3, 4, 5, 6, 7,
                                 8, 9, 10, 11, 12, 13, 14,
                                 15
 Supported rates               : 6, 9, 12, 18, 24, 36,
                                 48, 54 Mbps
 QoS mode                      : WMM
 Listen interval               : 250
 RSSI                          : 44
 Rx/Tx rate                    : 866.7/6 Mbps
 Speed                         : N/A
```

```
Authentication method          : Open system
Security mode                  : RSN
AKM mode                       : PSK
Cipher suite                   : CCMP
User authentication mode       : Bypass
WPA3 status                    : Disabled
Authorization CAR              : N/A
Authorization ACL ID           : N/A
Authorization user profile     : N/A
Roam status                    : N/A
Key derivation                 : SHA1
PMF status                     : N/A
Forwarding policy name         : Not configured
Online time                    : 0days 0hours 0minutes 52seconds
FT status                      : Inactive
BTM mode                       : Inactive
```

表 4-5 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
IPv4 address	クライアントIPv4アドレス。
IPv6 address	クライアントIPv6アドレス。
Username	クライアントユーザ名 • クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） • **N/A**（802.1X認証またはMAC認証を使用していない場合） 🕮 **メモ：** クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。
AID	アソシエーションID。
AP ID	クライアントが接続しているAPのID。
AP name	クライアントが接続しているAPの名前。
Radio ID	クライアントが接続している無線のID。
SSID	クライアントが接続しているSSID。

フィールド	説明
VLAN ID	クライアントが属するVLANのID。
Sleep count	スリープ状態への遷移数。
Wireless mode	無線モード。 ● 802.11a. ● 802.11b. ● 802.11g. ● 802.11gn. ● 802.11an. ● 802.11ac. ● 802.11ax.
Channel bandwidth	チャネル帯域幅、20MHz、40MHz、80MHz、160MHz。
SM Power Save	SM Power Saveは、クライアントの1つのアンテナだけをアクティブ状態、他のものはスリープ状態で動作させ、電力を節約することを可能にします。 ● **Enabled**–有効 ● **Disabled**–無効
SM power save mode	省電力モード。 ● Dynamic. ● Static.
Short GI for 20MHz	チャネル帯域幅が20MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 40MHz	チャネル帯域幅が40MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 80MHz	チャネル帯域幅が80MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 160/80+80MHz	チャネル帯域幅が160/80+80MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.

フィールド	説明
STBC Rx Capability	クライアントSTBC受信能力 ● Not supported. ● Supported.
STBC Tx Capability	クライアントSTBC送信能力 ● Not supported. ● Supported.
LDPC Rx capability	クライアントLDPC受信能力 ● Not supported. ● Supported.
SU beamformee capability	クライアントSU beamformee能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。
MU beamformee capability	クライアントMU beamformee能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。
Beamformee STS capability	クライアントbeamformee STS能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。
Block Ack	TIDを用いたブロックアックのネゴシエーション結果。 ● **IN**–受信方向からトラフィックのブロックアックを送信します。 ● **OUT**–送信方向からトラフィックのブロックアックを送信します。 ● **BOTH**–送受信方向からトラフィックのブロックアックを送信します。
Supported VHT-MCS set	クライアントによってサポートされたVHT-MCS
Supported HT MCS set	クライアントによってサポートされたHT-MCS
QoS mode	QoS モード。 ● **N/A**–WMMに対応しません。 ● **WMM**–WMMに対応します。 WMM情報ネゴシエーションは、WMMをサポートするAPとクライアントの間で実行されます。
Listen interval	クライアントがビーコンフレームを受信するためにウェイクアップする間隔。ビーコン間隔でカウントされます。

フィールド	説明
RSSI	受信した信号強度の表示。この値は、APによって検出されたクライアントの信号強度を示します。
Rx/Tx rate	データ、管理、制御フレームの送信および受信レート。
Speed	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Authentication method	認証方式、オープンシステム、または共有鍵。
Security mode	セキュリティモード。 ● **RSN**−ビーコンおよびプローブ応答はRSN IEを伝送します。 ● **WPA**−ビーコンおよびプローブ応答はWPA IEを伝送します。 ● **PRE-RSNA**-ビーコンおよびプローブ応答はRSN IE/WPA IEを伝送しません。
AKM mode	AKMモード。 ● 802.1X ● PSK ● Not configured.
Cipher suite	暗号スイート。 ● N/A. ● WEP40. ● WEP104. ● WEP128. ● CCMP. ● TKIP.
User authentication mode	ユーザ認証モード。 ● **Bypass**−クライアント認証なし。 ● **MAC**. ● **802.1X**. ● **OUI**.
Authorization ACL ID	許可されたACL番号表示 ● ACL番号：許可されたACLが有効になった場合 ● ACL番号+**Not effective**：許可されたACLが無効になった場合 ● **N/A**：許可されたACLがない場合

フィールド	説明
Authorization user profile	許可されたユーザプロファイル名表示 ● 許可されたユーザプロファイル名：許可されたACLが有効になった場合 ● 許可されたユーザプロファイル名+**Not effective**：許可されたACLが無効になった場合 ● **N/A**：許可されたユーザプロファイルがない場合
Roam status	Roam状態 ● Roaming in progress. ● Inter-AC slow roaming. ● Inter-AC fast roaming. ● Intra-AC slow roaming. ● Intra-AC fast roaming. ● **N/A**：クライアントがオンラインになった後、1つのBSSに留まっている場合
Key derivation	キー派生タイプ： ● **SHA1**–HMAC-SHA1ハッシュアルゴリズムを使用します。 ● **SHA256**–HMAC-SHA256ハッシュアルゴリズムを使用します。 ● **N/A**–アルゴリズムを使用しません。
PMF status	PMF状態 ● **Enabled**–管理フレーム保護が有効になっています。 ● **Disabled**–管理フレーム保護が無効になっています。 ● **N/A**–管理フレームの保護は行われません。
Forward policy	WLAN転送ポリシ ● **Not configured**–WLAN転送ポリシが設定されていません。 ● *policy-name*.
Online time	クライアントのオンライン期間。
FT status	Fast BSS transition (FT). ● **Active**-FT有効 ● **Inactive**-FT無効
BTM mode	BSS transition management (BTM). ● **Active**-BTM有効 ● **Inactive**-BTM無効

4.1.19 display wlan client device-information

🕮 メモ：

display wlan client device-information コマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client device-information [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。MAC アドレスを省略した場合、オンライン状態の全クライアントのデバイス情報を表示します。

説明

display wlan client device-information コマンドはクライアントのデバイス情報を表示します。

例

指定したクライアントのデバイス情報を表示します。

<AC> display wlan client device-information mac-address 80b6-5511-2233

```
MAC address                              : 80b6-5511-2233
 Vendor Name                              : Unknown
 Host Name                                : DESKTOP-abcdef
```

すべてのクライアントのデバイス情報を表示します。

<AC> display wlan client device-information

```
Total number of clients: 3

MAC address                              : 80b6-5511-2233
 Vendor Name                              : Unknown
 Host Name                                : DESKTOP-abcdef

 MAC address                              : b40e-de12-3456
 Vendor Name                              : PC
```

```
 Host Name                                : LAPTOP-112233

MAC address                              : 4826-2caa-bbcc
 Vendor Name                              : Apple
 Host Name                                : test
```

表 4-6 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
Vendor Name	クライアントのMACアドレスOUIから判別したベンダー名を表示します。 以下の場合は、Unknownが表示されます。 • クライアントがIOSオペレーティングシステムを使用している場合 • クライアントがランダムMACアドレスを使用している場合 • OUIリストからベンダーが特定できなかった場合
Host Name	クライアントのホスト名を表示します。 クライアントの送信したDHCP option21から情報を取得して表示します。 以下の場合は、Unknownが表示されます。 • クライアントがIOSオペレーティングシステムを使用している場合 • クライアントが固定IPアドレスを使用している場合

4.1.20 display wlan client failure

🕮 **メモ：**

display wlan client failure コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client failure

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan client failure コマンドはクライアントの接続失敗情報を表示します。

同じクライアントの失敗情報は最新情報のみ記録されます。

失敗したクライアントが最終的に接続に成功した場合、リストから削除されます。

失敗情報の記憶時間は **wlan client failure history aging** コマンドで設定できます。

例

クライアントの接続失敗情報を表示します。

<AC> display wlan client failure

```
association failures: 1
authentication failures: 1
-----------
 Association failures:
 Client-info                      AP name    R SSID    Time
 D8E2-657A-670F/-(-)               ap1        1 xxx     2022-09-12 15:09:49

 Authentication failures:
 Client-info                      AP name    R SSID    Time
 15AB-C5E7-DDE4/-(-)               ap2        1 yyy     2022-09-12 15:30:52
```

表 4-7 コマンド出力

フィールド	説明
association failures	アソシエーションフェーズで失敗したクライアントリストの数です。
authentication failures	認証フェーズで失敗したクライアント数です。
Association failures	アソシエーションフェーズで失敗したクライアントの情報を表示します。
Authentication failures	認証フェーズで失敗したクライアントの情報を示します。
Client-info	失敗したクライアントの情報です。MACアドレス、IPアドレス、ユーザ名が表示されます。情報がない部分は"-"で表示されます。
AP name	失敗したAP名
R	失敗したラジオ
SSID	失敗したSSID
Time	失敗時刻

4.1.21 display wlan client online-duration

🕮 メモ：

display wlan client online-duration コマンドは、QX-W1000 シリーズではソフトウェアバージョン 7.2.74 を含む以降、QX-W1100 シリーズではソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client online-duration [**ap** *ap-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: 1～64 文字で AP 名を指定します。大文字と小文字は区別されます。文字列には英字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）スラッシュ（/）、ハイフン(-)を使用できます。

説明

display wlan client online-duration コマンドはクライアントのオンライン時間の情報を表示します。

例

クライアントのオンライン時間情報を表示します。

<AC> display wlan client online-duration

```
Total number of online clients: 1

MAC address     IPv4 address     Online duration
abcd-ef13-f4a3  192.168.6.64     0days 0hours 0minutes 24seconds
```

表 4-8 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
IPv4 address	クライアントのIPv4アドレス

フィールド	説明
Online duration	クライアントのオンライン時間

4.1.22 display wlan client status

Syntax

display wlan client status [**mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。このオプションを指定しないと、すべてのクライアントに関するステータス情報が表示されます。

verbose: 詳細なクライアントのステータス情報を表示します。このキーワードを指定しない場合、コマンドはクライアント状況情報の概要を表示します。

説明

display wlan client status コマンドはクライアントステータス情報を表示します。

例

指定したクライアントに関する簡易的なステータス情報を表示します。

<AC> display wlan client status mac-address 001c-f08f-f804

```
MAC address    RSSI Rx/Tx(bps)    Speed(bps)     Discard AP name      RID
001c-f08f-f804 45   2.4G/6M       0.1K/0.2K      0.00%   ap1            1
```

すべてのクライアントの概要状況を表示します。

<AC> display wlan client status

```
Total number of clients: 2

MAC address    RSSI   Rx/Tx(bps)    Speed(bps)     Discard AP name     RID
001c-f08f-f804 45     2.4G/6M       0.1K/0.2K      0.00%     ap1         1
000f-e265-6401 35     2.4G/6M       0.1K/0.2K      0.00%     ap2         2
```

表 4-9 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス
RSSI	クライアントのRSSI
Rx/Tx rate	データ、管理、制御フレームの送信および受信レート
Speed(bps)	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入 N/A：送信レートと受信レートの両方が0の場合
Discard	クライアントに廃棄されるパケットの割合
AP name	クライアントが紐付いたAPの名前
RID	クライアントが紐付いた無線のID

特定のクライアントの詳細な状況を表示します。

<AC> display wlan client status mac-address 001c-f08f-f804 verbose

```
Total number of clients: 1

MAC address                    : 001c-f08f-f804
AP name                       : ap2
Radio ID                      : 2
Access time                    : 41 ms
RSSI                          : 0
Rx/Tx rate                     : 39/117 Mbps
Speed                         : 0.003/0.000Kbps
Received:
 Retransmitted packets           : 84
 Retransmitted packet ratio      : 64.12%
Sent:
 Retransmitted packets           : 0
 Retransmitted packet ratio      : 0.00%
Discarded:
 Discarded packets              : 0
 Discarded packet ratio          : 0.00%
```

表 4-10 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。

フィールド	説明
AP name	クライアントが紐付いたAPの名前
Radio ID	クライアントが紐付いた無線のID
Access time	クライアントがWLANに紐付く時間
RSSI	クライアントのRSSI
Rx/Tx rate	クライアントがデータ、管理パケット、制御パケットを送受信する速度
Speed(bps)	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Received	受信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Sent	送信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Discarded	廃棄パケット統計情報 ● 廃棄パケット ● 廃棄パケット比率

4.1.23 display wlan service-template

Syntax

display wlan service-template [*service-template-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。この引数を指定しない場合、すべてのサービステンプレートに関する情報が表示されます。

verbose: 詳細なサービステンプレート情報を表示します。

説明

display wlan service-template コマンドはサービステンプレート情報を表示します。

例

すべてのサービステンプレートに関する簡易情報を表示します。

<AC> display wlan service-template

```
Total number of service templates: 2
Service template name     SSID              Status
1                         2333              Enabled
2                         3222              Enabled
```

すべてのサービステンプレートに関する詳細情報を表示します。

<AC> display wlan service-template verbose

```
Service template name        : service1
Description                  : Not configured
SSID                         : wuxianfuwu
SSID-hide                    : Disabled
User-isolation               : Disabled
Service template status      : Disabled
Maximum clients per BSS      : 64
Frame format                 : Dot3
Seamless roam status         : Disabled
Seamless roam RSSI threshold : 0
Seamless roam RSSI gap       : 0
VLAN ID                      : 1
AKM mode                     : PSK
Security IE                  : RSN
Cipher suite                 : CCMP
TKIP countermeasure time     : 100 sec
PTK lifetime                 : 43200 sec
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : Bypass
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID                 : 1
802.1X handshake             : Enabled
```

```
802.1X handshake secure      : Disabled
802.1X domain               : my-domain
MAC-auth domain             : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Enabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization               : Permitted
Key derivation              : SHA1
PMF status                  : Optional
Hotspot policy number        : Not configured
Forwarding policy status     : Disabled
Forward policy name          : Not configured
Forwarder                   : AC
FT status                   : Enabled
QoS trust                   : Port
QoS priority                : 0
```

表 4-11 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
SSID-hide	SSIDステルス ● Disabled. ● Enabled.
User-isolation	ユーザ分離 ● Disabled. ● Enabled.
Service template status	サービステンプレート状態 ● Disabled. ● Enabled.
Maximum clients per BSS	BSSがサポートするクライアントの最大数。
Frame format	クライアントデータフレームのカプセル化フォーマット： ● **Dot3**–802.3フォーマット. ● **Dot11**–802.11フォーマット.

フィールド	説明
Seamless roam status	シームレスなローミング： ● Disabled. ● Enabled. 現在のリリースでは、このフィールドはサポートされていません。
Seamless roam RSSI threshold	シームレスなローミングRSSIしきい値。 現在のリリースでは、このフィールドはサポートされていません。
Seamless roam RSSI gap	シームレスなローミングRSSIギャップ。 現在のリリースでは、このフィールドはサポートされていません。
VLAN ID	クライアントがサービステンプレートを使用してオンラインになった後に属しているVLANのID。
AKM mode	AKMモード,802.1XまたはPSK.
Security IE	Security IE ● RSN. ● WPA.
Cipher suite	暗号方式 ● WEP40. ● WEP104. ● WEP128. ● TKIP. ● CCMP.
TKIP countermeasure time	TKIP対策時間。設定値0は、対策が取られていないことを表します。
GTK rekey	GTK rekeyが有効/無効： ● Enabled. ● Disabled.
GTK rekey method	GTK rekey方式。時間ベースまたはパケットベース
GTK rekey time	GTK rekey間隔.
GTK rekey packets	GTKをリフレッシュする前に送信できるパケット数。
GTK rekey client-offline	client-off GTK rekeyが有効/無効： ● Enabled. ● Disabled.

フィールド	説明
User authentication mode	認証モード: ● **Bypass**–認証なし。 ● **MAC**. ● **MAC-or-802.1X**. ● **802.1X**. ● **802.1X-or-MAC**. ● **OUI-or-802.1X**.
Intrusion protection	client-off GTK rekeyが有効/無効： ● Enabled. ● Disabled.
Intrusion protection mode	侵入防止モード： ● **Temporary-block**－ブロックリストに侵入者を一時的に追加します。 ● **Service-stop**－リセットされるまで、不正なパケットを受信するBSSによって提供されるすべてのサービスを停止します。 ● **Temporary-service-stop**－不正なパケットを受信したBSSが提供するアクセスサービスを一時的に停止します。
Temporary block time	一時的なブロック時間（秒）。
Temporary service stop time	一時的なサービス停止時間（秒）。
Fail VLAN ID	認証サーバが正常で認証に合格できない場合、クライアントが追加されるVLANのID。未設定の場合“**Not configured**”が表示されます。
Critical VLAN ID	認証サーバが異常で認証に合格できない場合、クライアントが追加されるVLANのID。未設定の場合“**Not configured**”が表示されます。
802.1X handshake	802.1Xハンドシェークが有効/無効： ● Enabled. ● Disabled.
802.1X handshake secure	セキュア802.1Xハンドシェークが有効/無効： ● Enabled. ● Disabled.
802.1X domain	802.1X認証ドメイン。未設定の場合“**Not configured**”が表示されます。
MAC-auth domain	MAC認証ドメイン。未設定の場合“**Not configured**”が表示されます。

フィールド	説明
Max 802.1X users per BSS	BSSでサポートされている802.1Xユーザの最大数
Max MAC-auth users per BSS	BSSでMAC認証に合格するサポートされるユーザの最大数。
802.1X re-authenticate	802.1X再認証が有効/無効： ● Enabled. ● Disabled.
Authorization fail mode	許可失敗モード ● **Offline**－認証に失敗すると、クライアントはログオフされます。 ● **Online**－認証に失敗しても、クライアントはログオフされません。
Accounting fail mode	アカウンティング失敗モード ● **Offline**－アカウンティングに失敗すると、クライアントはログオフされます。 ● **Online**－アカウンティングに失敗しても、クライアントはログオフされません。
Authorization	許可情報： ● **Permitted**－RADIUSサーバまたはローカルデバイスによって発行された許可情報を適用します。 ● **Ignored**－RADIUSサーバまたはローカルデバイスによって発行された認証情報を無視します。
Key derivation	キーの導出タイプ ● **SHA1**－HMAC-SHA1 hash algorithm使用 ● **SHA256**－HMAC-SHA256 hash algorithm使用 ● **SHA1-AND-SHA256**－HMAC SHA1 and SHA256 hash algorithm使用
PMF status	PMF状態 ● **Disabled**－管理フレームの保護が無効になっています。 ● **Optional**－オプションモードでの管理フレーム保護が有効になっています。 ● **Mandatory**－必須モードの管理フレーム保護が有効になっています。
Forwarding policy status	WLANフォワーディングポリシstatus ● Disabled. ● Enabled.

フィールド	説明
Forwarding policy name	WLANフォワーディングポリシ名 ● **Not configured**－設定なし ● *policy-name*.
Forwarder	クライアントトラフィックフォワーダ ● AC. ● AP.
FT status	FT状態 ● Disabled. ● Enabled.
QoS trust	QoSプライオリティトラストモード： ● **Port**－Portプライオリティトラストモード ● **Dot11e**－802.11eプライオリティトラストモード
QoS priority	ポートプライオリティ。設定範囲は0～7です。

4.1.24 display wlan statistics client

Syntax

display wlan statistics client [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、すべてのクライアントの統計が表示されます。

説明

display wlan statistics client コマンドはクライアントの統計情報を表示します。

例

すべてのクライアントの統計情報を表示します。

<AP> display wlan statistics client

```
MAC address              : 0014-6c8a-43ff
```

```
AP name                 : ap1
Radio ID                : 1
SSID                    : office
BSSID                   : 000f-e2ff-7700
RSSI                    : 31
Sent frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 9/1230 (frames/bytes)
  Video                 : 0/0 (frames/bytes)
  Voice                 : 2/76 (frames/bytes)
Received frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 18/2437 (frames/bytes)
  Video                 : 0/0 (frames/bytes)
  Voice                 : 7/468 (frames/bytes)
Discarded frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 0/0 (frames/bytes)
  Video                 : 0/0 (frames/bytes)
  Voice                 : 5/389 (frames/bytes)
```

表 4-12 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
MAC address	クライアントのMACアドレス
Back ground	AC-BK queue.
Best effort	AC-BE queue.
Video	AC-VI queue.
Voice	AC-VO queue.

4.1.25 display wlan statistics connect-history

Syntax

display wlan statistics connect-history { **ap** { **all** | **name** *ap-name* } | **service-template** *service-template-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap all: すべての AP のクライアント接続履歴を表示します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

service-template *service-template-name*: サービステンプレートを名前で指定します。

説明

display wlan statistics connect-history コマンドはクライアントの接続履歴を表示します。

例

#AP ap1 の接続履歴を表示します。

<AP> display wlan statistics connect-history ap name ap1

```
AP name                 : ap1
Radio ID                : 1
Associations             : 132
Association failures       : 3
Reassociations            : 30
Rejections               : 12
Abnormal disassociations    : 2
Current associations       : 57

AP name                 : ap1
Radio ID                : 2
Associations             : 1004
Association failures       : 35
Reassociations            : 59
Rejections               : 4
Abnormal disassociations    : 22
Current associations       : 300
```

サービステンプレート 1 の接続履歴を表示します。

<AP> display wlan statistics connect-history service-template 1

```
AP name                 : ap1
```

```
Radio ID                : 1
Associations             : 132
Association failures       : 3
Reassociations            : 30
Rejections               : 12
Abnormal disassociations    : 2
Current associations       : 57

AP name                 : ap1
Radio ID                : 2
Associations             : 1004
Association failures       : 35
Reassociations            : 59
Rejections               : 4
Abnormal disassociations    : 22
Current associations       : 300
```

4.1.26 display wlan statistics service-template

Syntax

display wlan statistics service-template *service-template-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。

説明

display wlan statistics service-template コマンドはサービステンプレートの統計情報を表示します。

例

サービステンプレート 1 の統計情報を表示します。

<AP> display wlan statistics service-template 1

```
AP name                  : ap1
Radio ID                 : 1
```

```
Received:
  Frame count              : 1713
  Frame bytes              : 487061
  Data frame count          : 1683
  Data frame bytes          : 485761
  Association request count   : 2
Sent:
  Frame count              : 62113
  Frame bytes              : 25142076
  Data frame count          : 55978
  Data frame bytes          : 22626600
  Association response count  : 2
```

4.1.27 display wlan whitelist

Syntax

display wlan whitelist

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan whitelist コマンドはホワイトリストエントリを表示します。

例

#ホワイトリストエントリを表示します。

<AC> display wlan whitelist

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

4.1.28 inherit exclude service-template

Syntax

inherit exclude service-template *service-template-name*

undo inherit exclude service-template *service-template-name*

デフォルト

AP は、AP グループにバインドされたサービステンプレートを継承します。

View

Radio view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

説明

inherit exclude service-template コマンドは AP グループから指定されたサービステンプレートを継承しないように AP を設定します。

undo inherit exclude service-template コマンドはデフォルトに戻します。

例

AP ap1 を AP グループからサービステンプレート st を継承しないように設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-ap-ap1] radio 1

[AC-ap-ap1-radio-1] inherit exclude service-template st

4.1.29 map-configuration

🕮 メモ：

AP の設定には **remote-configuration** を使用することを推奨します。
remote-configuration で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。なお、**remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

map-configuration *filename*

undo map-configuration

デフォルト

コンフィグレーションファイルなし

View

AP view

AP group AP model view

定義済みユーザロール

network-admin

パラメータ

filename: コンフィグレーションファイル名を指定します。コンフィグレーションファイル名は、1～63 文字の文字列です。大文字と小文字を区別しません。コンフィグレーションファイルが AC の記憶媒体に保管されていることを確認してください。

説明

map-configuration コマンドはコンフィグレーションファイルを AP に展開します。

undo map-configuration コマンドはデフォルトに戻します。

コンフィグレーションファイルは完全なコマンドでなければなりません。

コンフィグレーションファイルは、AC への CAPWAP トンネルが実行状態にあるときに有効になります。AP の再起動後も存続しません。

AP がコンフィグレーションファイルを使用する設定の場合、AP 自身の設定は、AC への CAPWAP トンネルを確立するためにメイン IP アドレスのみを使用します。

例

#コンフィグレーションファイル downconfig.txt を AP ap1 に配置します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] map-configuration downconfig.txt

#コンフィグレーションファイル downconfig.txt を AP グループ apgroup1 のモデル QX-W1020 を持つ AP に配置します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] map-configuration downconfig.txt

4.1.30 nas-id

Syntax

nas-id *nas-id*

undo nas-id

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-id: NAS ID を指定します。NAS ID は、1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-id コマンドはネットワークアクセスサーバ識別子（NAS ID）を設定します。

オンライン後、クライアントは、NAS ID を持つ RADIUS 要求を RADIUS サーバに送信して、ネットワークアクセスサーバを指定します。

装置は、次の優先順位で NAS-ID を選択します。

1.サービステンプレートを無線にバインドする時に指定した NAS-ID パラメータ

2.AP View の設定

3. AP group View の設定

4. wlan global-configuration View の設定

5. ISP ドメイン View の設定

NAS-ID が設定されていない場合、装置はデバイス名を NAS-ID として使用します。例

AP ap1 に NAS ID abc123 を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] nas-id abc123

AP group group1 に NAS ID abc123 を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] nas-id abc123

グローバル NAS ID に abc123 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] nas-id abc123

4.1.31 nas-port-id

Syntax

nas-port-id *nas-port-id*

undo nas-port-id

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-port-id: NAS port ID を指定します。NAS port ID は、1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-port-id コマンドはネットワークアクセスサーバのポート識別子（NAS ポート ID）を設定します。

undo nas-port-id コマンドはデフォルトに戻します。

オンライン後、クライアントは、NAS port ID を持つ RADIUS 要求を RADIUS サーバに送信して、ネットワークアクセスサーバを指定します。

サービステンプレートを無線にバインドするときに NAS port ID を設定します。NAS port ID は、AP view、AP group view、global configuration view に設定できます。これらの設定の優先順位は降順です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 に NAS port ID abcd1234 を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] nas-port-id abcd1234

AP group group1 に NAS port ID abcd1234 を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] nas-port-id abcd1234

グローバル NAS port ID に abcd1234 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] nas-port-id abcd1234

4.1.32 nas-vlan

Syntax

nas-vlan *vlan-id*

undo nas-vlan

デフォルト

NAS VLAN ID が設定されていません。RADIUS サーバに送信された認証要求に NAS VLAN ID フィールドが含まれていません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

vlan-id: NAS VLAN ID を 1～4096 の範囲で指定します。

説明

nas-vlan コマンドはネットワークアクセスサーバ VLAN 識別子（NAS VLAN ID）を設定し、VLAN ID を RADIUS 要求にカプセル化する AC を有効にします。

undo nas-vlan コマンドはデフォルトに戻します。

NAS VLAN ID が設定されると、AC はクライアントのネットワークアクセスサーバを示すために RADIUS サーバに送信される RADIUS 要求に VLAN ID をカプセル化します。

サードパーティのセキュリティアカウンティング管理（SAM）サーバを RADIUS サーバとして使用する場合、NAS VLAN ID を設定します。

例

AP **ap1** の NAS VLAN ID を **1234** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] nas-vlan 1234

4.1.33 quick-association enable

Syntax

quick-association enable

undo quick-association enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

quick-association enable コマンドはクイックアソシエーションを有効にします。

undo quick-association enable コマンドはデフォルトに戻します。

このコマンドは、AP が指定されたサービステンプレートに関連付けられたクライアント上でロードバランシングまたはバンドナビゲーションを実行できないようにします。

例

サービステンプレート **service1** の quick association を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] quick-association enable

4.1.34 region-code

Syntax

region-code *code*

undo region-code

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：JP

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

code: 地域コードを指定します。 地域コードの詳細については、表 4-13 を参照してください。

表 4-13 地域コード一覧

国	地域コード	国	地域コード
Japan	JP	South Africa	ZA

説明

region-code コマンドは地域コードを指定します。

undo region-code コマンドはデフォルトに戻します。

地域コードは、利用可能な周波数、利用可能なチャネル、および送信電力レベルなどの特性を決定します。AP を設定する前に有効な地域コードを設定してください。

AP view、AP group view、および Global configuration view での設定の優先順位は降順です。

例

AP ap1 の地域コードを JP に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] region-code JP

AP group group1.の地域コードを JP に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] region-code US

グローバル地域コードを JP に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] region-code JP

関連コマンド

region-code-lock

4.1.35 region-code-lock

Syntax

region-code-lock { **disable** | **enable** }

undo region-code-lock

デフォルト

AP view：AP group view の設定を使用します。

AP group view：global configuration view の設定を使用します。

global configuration view：ロックしません。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: 地域コードのロックを解除します。

enable: 地域コードをロックします。

説明

region-code-lock enable コマンドは地域コードをロックします。

region-code-lock disable コマンドは地域コードのロックを解除します。

undo region-code-lock コマンドはデフォルトに戻します。

ロックされると地域コードは変更できません。

AP view に地域コードを設定していない場合、AP view で地域コードをロックしても、AP は AP group view または AP group view に設定された地域コードを使用します。AP group view に地域コードが設定していない場合、AP group view で地域コードをロックしても、AP はグローバル地域コードを使用します。

AP view、AP group view、および Global configuration view での設定の優先順位は降順です。

例

AP ap1 の地域コードをロックします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] region-code-lock enable

AP group group1.の地域コードをロックします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] region-code-lock enable

#グローバル地域コードをロックします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] region-code-lock enable

関連コマンド

region-code

4.1.36 reset wlan client

Syntax

reset wlan client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスでクライアントを指定します。

all: すべてのクライアントを指定します。

説明

reset wlan client コマンドはクライアントまたはすべてのクライアントからログオフします。

例

#すべてのクライアントをログオフします。

<AC> reset wlan client all

関連コマンド

display wlan client

4.1.37 reset wlan dynamic-blacklist

Syntax

reset wlan dynamic-blacklist [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスでクライアントを指定します。このオプションを指定しないと、このコマンドはダイナミックブラックリストからすべてのクライアントを削除します。

説明

reset wlan dynamic-blacklist コマンドは指定したクライアントまたはすべてのクライアントをダイナミックブラックリストから削除します。

例

ダイナミックブラックリストからすべてのクライアントを削除します。

<AC> reset wlan dynamic-blacklist

ダイナミックブラックリストから指定したクライアントを削除します。

<AC> reset wlan dynamic-blacklist mac-address b8ca-32a2-df69

関連コマンド

display wlan blacklist

4.1.38 reset wlan statistics client

Syntax

reset wlan statistics client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのクライアントを指定します。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

説明

reset wlan statistics client コマンドはクライアントの統計情報を削除します。

例

すべてのクライアントの統計情報を削除します。

<AC> reset wlan statistics client all

関連コマンド

display wlan statistics

4.1.39 reset wlan statistics service-template

Syntax

reset wlan statistics service-template { **service-template** *service-template-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。

説明

reset wlan statistics service-template コマンドはサービステンプレートの統計情報を削除します。

例

サービステンプレート service1 の統計情報を削除します。

<AP> reset wlan statistics service-template service 1

関連コマンド

display wlan statistics service-template

4.1.40 service-template

Syntax

service-template *service-template-name* [**nas-id** *nas-id* | **nas-port-id** *nas-port-id*] [**ssid-hide**] [**vlan** *vlan-id*]

undo service-template *service-template-name*

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

nas-id *nas-id*: NAS ID を指定します。NAS ID は、1～63 文字のスペースを含まない文字列です。大文字と小文字を区別しません。

nas-port-id *nas-port-id*: NAS port ID を指定します。NAS port ID は、1～63 文字のスペースを含まない文字列です。大文字と小文字を区別しません。

ssid-hide: ビーコンフレームで SSID を非表示にします。

vlan *vlan-id*: VLAN ID によって無線にバインドされる VLAN を指定します。範囲は 1～4094 です。このオプションを指定しない場合、無線はサービステンプレートにバインドされた VLAN を使用します。指定された VLAN が存在しない場合、このコマンドはクライアントがオンラインになったときに VLAN を作成します。

説明

service-template コマンドはサービステンプレートを無線インタフェースまたは無線インタフェースにバインドします。

undo service-template コマンドは無線または無線インタフェースからサービステンプレートをバインド解除します。

サービステンプレートは、無線または無線インタフェースにバインドする前に作成する必要があります。

このコマンドを使用して設定された VLAN ID は、サービステンプレート用に設定された VLAN ID よりも優先されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

サービステンプレート service1 と VLAN group vg1 を radio 1 にバインドします。

<AC> system-view

[AC] wlan ap ap1

[AC-ap-ap1] radio 1

[AC-ap-ap1-radio-1] service-template service1 vlan 10

サービステンプレート service1 と VLAN 10 を AP group apgroup1 の radio 1 にバインドします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] service-template service1 vlan 10

4.1.41 service-template enable

Syntax

service-template enable

undo service-template enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

service-template enable コマンドはサービステンプレートを有効にします。

undo service-template enable コマンドはサービステンプレートを無効にします。

AC 上の BSS（basic service set）の数が制限を超える場合、新しいサービステンプレートを有効にできません。

例

サービステンプレート service1 を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] service-template enable

4.1.42 snmp-agent trap enable wlan client

Syntax

snmp-agent trap enable wlan client

undo snmp-agent trap enable wlan client

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan client コマンドは WLAN アクセスの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan client コマンドはデフォルトに戻します。

この機能を有効にすると、クライアントのステータスが変更されるたびに、装置は NMS にクライアントステータス変更通知を送信します。通知を正しく送信するには、オペレーションマニュアルのセクション 11 *システム管理 "Information Center"* の説明に従って SNMP を設定する必要があります。

例

#WLAN アクセスに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan client

4.1.43 snmp-agent trap enable wlan client-audit

Syntax

snmp-agent trap enable wlan client-audit

undo snmp-agent trap enable wlan client-audit

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan client-audit コマンドはクライアント監査の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan client-audit コマンドはクライアント監査の SNMP 通知を無効にします。

この機能を有効にすると、クライアントがオンラインになったり、オフラインになったり、別の AP にローミングしたり、IP アドレスを取得した場合、装置は NMS にクライアントステータス変更通知を送信します。通知を正しく送信するには、オペレーションマニュアルのセクション 11 *システム管理 “Information Center”* の説明に従って SNMP を設定する必要があります。

例

クライアント監査の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan client-audit

4.1.44 ssid

Syntax

ssid *ssid-name*

undo ssid

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を 1～32 文字の文字列で指定します。SSID 名には、大文字、小文字、数字、特殊文字が使用可能です。大文字と小文字は区別されます。特殊文字については 表 4-14 を参照してください。

表 4-14 使用可能な特殊文字

名称	文字	名称	文字
Tilde	~	Left angle bracket	<
Exclamation point	!	Right angle bracket	>
At sign	@	Hyphen	-
Pound sign	#	Underscore	_
Dollar sign	$	Plus sign	+
Percent sign	%	Equal sign	=
Caret	^	Vertical bar	|
Ampersand sign	&	Backslash	¥
Asterisk	*	Colon	:
Left brace	{	Semi-colon	;
Right brace	}	Quotation marks	"
Left parenthesis	(	Apostrophe	'
Right parenthesis	)	Comma	,
Left bracket	[	Dot	.
Right bracket	]	Slash	/

説明

ssid コマンドはサービステンプレートの SSID を設定します。

undo ssid コマンドはサービステンプレートの SSID を削除します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

QX では、サービステンプレートに個別の SSID を設定することを推奨します。

例

サービステンプレート service1 に SSID lynn を設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] ssid lynn

4.1.45 unknown-client

Syntax

unknown-client { **deauthenticate** | **drop** }

undo unknown-client

デフォルト

AP は未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

deauthenticate: 未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

drop: 未知のクライアントからのパケットを廃棄します。

説明

unknown-client コマンドは AP が未知のクライアントからのトラフィックを処理する方法を設定します。

undo unknown-client コマンドはデフォルトに戻します。

例

AP ap1 サービステンプレート example に未知のクライアントからのパケットを廃棄するが、未知のクライアントの認証は解除しない設定をします。

<AC> system-view

[AC] wlan service-template example

[AC -wlan-st-example] unknown-client drop

4.1.46 user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: ユーザプロファイル名を指定します。設定範囲は 1 から 31 文字です。大文字と小文字を区別します。英字、数字、アンダースコア (_) を使用でき、英字で始まる必要があります。名前は一意である必要があります。

説明

user-profile コマンドはユーザプロファイルを作成し、その view に移行するか、既存のユーザプロファイルの view に移行します。

undo user-profile コマンドはユーザプロファイルを削除します。

例

#ユーザプロファイル a123 を作成し、a123 の View に移行します。

<AC> system view

[AC] user-profile name a123

[AC-user-profile-a123]

4.1.47 vlan

Syntax

vlan *vlan-id*

undo vlan

デフォルト

サービステンプレートを使用してオンラインになった後、クライアントは VLAN 1 に割り当てられます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN を VLAN ID で指定します。VLAN ID の設定範囲は 1～4094 です。指定した VLAN が存在しない場合、このコマンドは、クライアントがオンラインになったときに VLAN を作成します

説明

vlan コマンドはサービステンプレートを使用してオンラインになっているクライアントを VLAN に割り当てます。

undo vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

例

サービステンプレート **service1** を介してオンラインになっているクライアントを VLAN 2 に割り当てます。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] vlan 2

4.1.48 wlan client failure history aging

🕮 メモ：

wlan client failure history aging コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan client failure history aging *time*

undo wlan client failure history aging

デフォルト

72 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

time: クライアントの接続失敗情報を記憶する時間を指定します。設定範囲は 1～720 時間です。

説明

wlan client failure history aging コマンドはクライアントの接続失敗情報を記憶する時間を設定します。

undo wlan client failure history aging コマンドはデフォルト設定に戻します。

例

クライアントの接続失敗情報を記憶する時間を 720 時間に設定します。

<AC> system-view

[AC] wlan client failure history aging 720

4.1.49 wlan client forwarding enable

Syntax

wlan client forwarding enable

undo wlan client forwarding enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan client forwarding enable コマンドはクライアントトラフィックの転送を有効にします。

undo wlan client forwarding enable コマンドはクライアントトラフィックの転送を無効にします。

クライアントトラフィックフォワーダとして AC を設定する場合、この機能を有効にする必要があります。

例

クライアントトラフィック転送を無効にします。

<AC> system-view

[AC] undo wlan client forwarding enable

関連コマンド

client forwarding-location

4.1.50 wlan client reauthentication-period

Syntax

wlan client reauthentication-period [*period-value*]

undo wlan client reauthentication-period

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

period-value: アイドル期間を 1～3600 秒の範囲で指定します。デフォルトでは、アイドル期間は 10 秒です。

説明

wlan client reauthentication-period コマンドはクライアント再認証の前にアイドル期間を設定します。

undo wlan client reauthentication-period コマンドはデフォルトに戻します。

クライアントの再認証の前にアイドル期間を設定して、再認証の失敗を減らします。

WLAN MAC 認証クライアントに対して URL リダイレクトが有効になっている場合、AP は MAC 認証を通過したクライアントからログオフします。次の MAC 認証試行で、クライアントは MAC 認証を通過し、WLAN にアクセスできます。アイドル期間が設定されていると、AP はクライアントをログオフした後にダイナミックブラックリストにクライアントを追加し、指定されたアイドル時間の経過後にクライアントエントリが期限切れになります。

例

クライアント再認証の前にアイドル期間を 100 秒に設定します。

<AC> system-view

[AC] wlan client reauthentication-period 100

4.1.51 wlan dynamic-blacklist active-on-ap

Syntax

wlan dynamic-blacklist active-on-ap

undo wlan dynamic-blacklist active-on-ap

デフォルト

ダイナミックブラックリストは AP に有効です。

View

System view

定義済みユーザロール

network-admin

説明

wlan dynamic-blacklist active-on-ap コマンドはダイナミックブラックリストを AP で有効にするように設定します。

undo wlan dynamic-blacklist active-on-ap コマンドはダイナミックブラックリストを AC に適用するように設定します。

ダイナミックブラックリストを AC に適用するように設定すると、AC に接続されているすべての AP はダイナミックブラックリストのクライアントを拒否します。ダイナミックブラックリストを AP に適用するように設定すると、ダイナミックブラックリスト内のクライアントに関連付けられている AP はクライアントを拒否しますが、クライアントは引き続き AC に接続されている他の AP と関連付けることができます。ダイナミックブラックリストを高密度環境で AC に適用するように設定することを推奨します。

例

ダイナミックブラックリストを AC 上で有効にするように設定します。

<AC> system-view

[AC] undo wlan dynamic-blacklist active-on-ap

4.1.52 wlan dynamic-blacklist lifetime

Syntax

wlan dynamic-blacklist lifetime *lifetime*

undo wlan dynamic-blacklist lifetime

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

lifetime: エージングタイムを指定します。設定範囲は 1～3600 秒です。

説明

wlan dynamic-blacklist lifetime コマンドはダイナミックブラックリストエントリのエージングタイムを設定します。

undo wlan dynamic-blacklist lifetime コマンドはデフォルトに戻します。

設定したエージングタイムは設定後、ダイナミックブラックリストに追加されたエントリから有効です。

例

#ダイナミックブラックリストのエージングタイムを 3600 秒に指定します。

<AC> system-view

[AC] wlan dynamic-blacklist lifetime 3600

4.1.53 wlan link-test

🕮 **メモ：**

wlan link-test コマンドは QX-W1100 シリーズでは利用できません。

Syntax

wlan link-test *mac-address*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

mac-address: H-H-H 形式でクライアント MAC アドレスを指定します。

説明

wlan link-test コマンドはワイヤレスリンクの品質をテストします。

無線リンク品質検出により、AP は無線クライアントへのリンクの品質をテストできます。AP は、各サポートレートでクライアントに空のデータフレームを送信します。次に、クライアントからの応答に基づいて、RSSI、パケット再送信、RTT などのリンク品質情報を計算します。

無線リンク品質検出のタイムアウト時間は 10 秒です。タイムアウト時間内で無線リンク検出が完了しない場合、テスト結果を取得できません。

例

MAC アドレス 60a4-4cda-eff0 のクライアントに対して、無線リンク品質検出を実行します。

<AC> wlan link-test 60a4-4cda-eff0

```
Testing link to 60a4-4cda-eff0. Press CTRL + C to break.
                          Link Status
------------------------------------------------------------------------
MAC address: 60a4-4cda-eff0
```

```
------------------------------------------------------------------------
VHT-MCS  Rate(Mbps)  Tx packets  Rx packets  RSSI  Retries  RTT(ms)
------------------------------------------------------------------------
NSS = 1
------------------------------------------------------------------------
 0       6.5         5           5           54    0        0
 1       13          5           5           51    0        0
 2       19.5        5           5           49    0        0
 3       26          5           5           47    0        0
 4       39          5           5           45    0        0
 5       52          5           5           45    0        0
 6       58.5        5           5           44    0        0
 7       65          5           5           44    0        0
 8       78          5           5           44    0        0
------------------------------------------------------------------------
```

表 4-15 コマンド出力

フィールド	説明
No./MCS/VHT-MCS/HE-MCS	• **No**－802.11a、802.11b、802.11gクライアントのリンク品質テストの速度番号。 • **MCS**－802.11nクライアントのリンク品質テストのMCSインデックス。 • **VHT-MCS**－802.11acクライアントのリンク品質テストのVHT-MCSインデックス。 • **HE-MCS**－802.11axクライアントのリンク品質テストのHE-MCSインデックス。
Rate(Mbps)	APが無線リンク品質検出フレームを送信するレート。
Tx packets	APが送信した無線リンク品質検出フレームの数。
Rx packets	APが受信した無線リンク品質検出フレームの数。
RSSI	APが検出したクライアントのRSSI。
Retries	無線リンク品質検出フレームの再送信の数。
RTT(ms)	APからクライアントへの無線リンク品質検出フレームのラウンドトリップ時間。
NSS	802.11nまたは802.11ac/axクライアントでのリンク品質テスト用の空間ストリームの数。

4.1.54 wlan nas-port-id format

Syntax

wlan nas-port-id format { **2** | **4** }

undo wlan nas-port-id format

View

System view

定義済みユーザロール

network-admin

パラメータ

2: フォーマット 2（*SlotID***00***IfNOVlanID*）を指定します。このフォーマットにおいて、NAS ポート ID は以下の情報を含みます。

- **SlotID**－クライアントがアクセスするスロットの 2 桁の ID です。
- **IfNO**－クライアントがアクセスするインタフェースの 3 桁の番号です。
- **VlanID**－クライアント VLAN の 9 桁の ID です。

4: フォーマット 4（**slot=**;subslot=**;port=**;vlanid=**;vlanid2=****）を指定します。**vlanid2=****は、VLAN ターミネーションが有効なインタフェースで WLAN にアクセスするクライアントに対してのみ使用します。

説明

wlan nas-port-id format コマンドは NAS port ID フォーマットを指定します。

undo wlan nas-port-id format コマンドはデフォルトに戻します。

NAS port ID フォーマットは、NAS port ID が指定されていないときに適用されます。この場合、システムは NAS port ID フォーマットとクライアント情報に基づいて NAS port ID を生成します。NAS port ID が指定されている場合、指定された NAS port ID が使用されます。

例

NAS port ID フォーマットにフォーマット 4 を指定します。

<AC> system-view

[AC] wlan nas-port-id format 4

関連コマンド

nas-port-id

4.1.55 wlan permit-ssid

🕮 メモ：

wlan permit-ssid コマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

wlan permit-ssid *ssid-name*

undo wlan permit-ssid [*ssid-name*]

デフォルト

設定なし

View

User profile view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を指定します。1 から 32 文字で指定します。大文字と小文字は区別されます。

説明

wlan permit-ssid コマンドはクライアントアソシエーションを許可する SSID を設定します。

undo wlan permit-ssid コマンドは許可する SSID を削除します。*ssid-name* パラメータを指定しない場合、許可する SSID 設定を全て削除します。

クライアントアソシエーションを許可する SSID が設定されていない場合、クライアントアソシエーションは制限されません。

クライアントアソシエーションを許可する SSID が設定されている場合、クライアントは許可された SSID を介してのみ WLAN にアクセスできます。

例

クライアントアソシエーションを許可する SSID として SSID 名 ssid 1 を指定します。

<AC> system-view

[AC] user-profile profile1

[AC-user-profile-profile1] wlan permit-ssid ssid1

4.1.56 wlan service-template

Syntax

wlan service-template *service-template-name*

undo wlan service-template *service-template-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

説明

wlan service-template コマンドはサービステンプレートを作成します。

undo wlan service-template コマンドはサービステンプレートを削除します。

指定したサービステンプレートが存在する場合、このコマンドにより service template view に移行します。

無線にバインドされているサービステンプレートは削除できません。

例

サービステンプレート **service1** を作成し、その view に移行します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1]

4.1.57 wlan static-blacklist mac-address

Syntax

wlan static-blacklist mac-address *mac-address*

undo wlan static-blacklist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

wlan static-blacklist mac-address コマンドはスタティックブラックリストにクライアントを追加します。

undo wlan static-blacklist mac-address コマンドはスタティックブラックリストからクライアントを削除します。

スタティックブラックリストにオンラインクライアントを追加すると、クライアントをログオフします。

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

undo コマンドで、**mac-address** *mac-address* オプションを省略した場合、スタティックブラックリストからすべてのクライアントを削除します。

例

スタティックブラックリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<AC> system-view

[AC] wlan static-blacklist mac-address 001c-f0bf-9c92

関連コマンド

display wlan blacklist

4.1.58 wlan web-server api-path

Syntax

wlan web-server api-path *path*

undo wlan web-server api-path

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

path: 1～256 文字の大文字と小文字を区別するパスを指定します。

説明

wlan web-server api-path コマンドはクライアント情報が報告される Web サーバのパスを設定します。

undo wlan web-server api-path コマンドはデフォルトに戻します。

Web サーバは、サーバのホスト名、ポート番号、およびパスが指定されている場合にのみ、クライアント情報を受け入れます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

/wlan/dev-cfg として Web サーバのパスを指定します。

<AC> system-view

[AC] wlan web-server api-path /wlan/dev-cfg

関連コマンド

- **wlan web-server host**
- **wlan web-server max-client-entry**

4.1.59 wlan web-server host

Syntax

wlan web-server host *host-name* **port** *port-number*

undo wlan web-server host

デフォルト

Web サーバのホスト名とポート番号は指定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

host *host-name*: ホスト名を指定します。大文字、小文字を区別しない 3～127 文字です。文字列には、文字、数字、ハイフン（-）、アンダースコア（_）、ドット（.）を使用できます。

port *port-number*: ポート番号を 1～65534 の範囲で指定します。

説明

wlan web-server host コマンドはクライアント情報が報告される Web サーバのホスト名とポート番号を指定します。

undo wlan web-server host コマンドはデフォルトに戻します。

Web サーバは、サーバのホスト名、ポート番号、およびパスが指定されている場合にのみ、クライアント情報を受け入れます。

クライアント情報の変更はリアルタイムで Web サーバに報告されます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

Web サーバのホスト名とポート番号は、それぞれ **www.abc.com** と **668** として指定します。

<AC> system-view

[AC] wlan web-server host www.abc.com port 668

関連コマンド

- **wlan web-server api-path**
- **wlan web-server max-client-entry**

4.1.60 wlan web-server max-client-entry

Syntax

wlan web-server max-client-entry *number*

undo wlan web-server max-client-entry

デフォルト

10

View

System view

定義済みユーザロール

network-admin

パラメータ

number: クライアントエントリの最大数を 1～25 の範囲で指定します。

説明

wlan web-server max-client-entry コマンドは一度に報告するクライアントエントリの最大数を設定します。

undo wlan web-server max-client-entry コマンドはデフォルトに戻します。

例

一度に報告するクライアントエントリの最大数を 12 に設定します。

<AC> system-view

[AC] wlan web-server max-client-entry 12

関連コマンド

- **wlan web-server api-path**
- **wlan web-server host**

4.1.61 wlan whitelist mac-address

Syntax

wlan whitelist mac-address *mac-address*

undo wlan whitelist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

wlan whitelist mac-address コマンドはホワイトリストにクライアントを追加します。

undo wlan whitelist mac-address コマンドはホワイトリストからクライアントを削除します。

最初のクライアントをホワイトリストに追加すると、すべてのオンラインクライアントを切断するかどうかを尋ねるメッセージが表示されます。“Y”と入力するとホワイトリストが作成されます。

ホワイトリストからオンラインクライアントを削除すると、クライアントをログオフします。ホワイトリストからすべてのクライアントを削除すると、オンラインクライアントはログオフされません。

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

undo コマンドで、**mac-address** *mac-address* オプションを省略した場合、ホワイトリストからすべてのクライアントを削除します。

例

ホワイトリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<AC> system-view

[AC] wlan whitelist mac-address 001c-f0bf-9c92

```
This command will disconnect all clients. Continue? [Y/N]:
```

関連コマンド

display wlan whitelist

目次

5 章 WLAN セキュリティ 5-1
5.1 WLAN セキュリティコマンド 5-1
5.1.1 akm mode 5-1
5.1.2 akm sae pwe 5-2
5.1.3 cipher-suite 5-3
5.1.4 enhanced-open enable 5-5
5.1.5 enhanced-open transition-mode service-template 5-6
5.1.6 gtk-rekey client-offline enable 5-7
5.1.7 gtk-rekey enable 5-8
5.1.8 gtk-rekey method 5-8
5.1.9 key-derivation 5-10
5.1.10 pmf 5-11
5.1.11 pmf association-comeback 5-12
5.1.12 pmf saquery retrycount 5-13
5.1.13 pmf saquery retrytimeout 5-13
5.1.14 preshared-key 5-14
5.1.15 ptk-lifetime 5-16
5.1.16 ptk-rekey enable 5-16
5.1.17 security-ie 5-17
5.1.18 snmp-agent trap enable wlan usersec 5-18
5.1.19 tkip-cm-time 5-19
5.1.20 wep key 5-20
5.1.21 wep key-id 5-22
5.1.22 wep mode dynamic 5-23
5.1.23 wpa3 5-24

5章 WLAN セキュリティ

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

5.1 WLANセキュリティコマンド

5.1.1 akm mode

Syntax

akm mode { **dot1x** | **psk** | **anonymous-dot1x** }

undo akm mode

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X を指定します。

psk: PSK を指定します。

anonymous-dot1x: ワイファイアライアンス Anonymous 802.1X を指定します。

説明

akm mode コマンドは AKM（Authentication and Key Management）モードを設定します。

undo akm mode コマンドはデフォルトに戻します。

RSNA ネットワークに AKM モードを設定する必要があります。

WLAN サービステンプレートは AKM モードを 1 つだけサポートします。WLAN サービステンプレートが無効なときだけ AKM モードを設定します。

OSEN IE モデルが使用される場合、ワイファイアライアンス Anonymous 802.1X AKM を設定します。

以下の AKM モードは、いずれも特定の認証モードで使用する必要があります。

- **802.1X AKM—**802.1X 認証モード
- **PSK AKM—**MAC もしくは認証バイパスモード
- ワイファイアライアンス Anonymous **802.1X AKM—**802.1X 認証モード

詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。

例

PSK AKM モードを設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm mode psk

関連コマンド

- **cipher-suite**
- **security-ie**

5.1.2 akm sae pwe

🕮 **メモ：**

- **akm sae pwe** コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
- **both-h2e-hnp** を指定すると **hnp** のみをサポートしたクライアントでローミングに失敗する場合があります。クライアントの問題ですが、ローミング失敗を避けるために" **akm sae pwe hnp**" を設定してください。

Syntax

akm sae pwe { both-h2e-hnp | h2e | hnp }

undo akm sae pwe

デフォルト

both-h2e-hnp

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

both-h2e-hnp: PWE の生成方式として、Hunting-and-Pecking (HnP)と Hash-to-Element (H2E)を指定します。

h2e: PWE の生成方式として、Hash-to-Element (H2E)を指定します。

hnp: PWE の生成方式として、Hunting-and-Pecking (HnP)を指定します。

説明

akm sae pwe コマンドは WPA 3-SAE の SAE 交換時の PWE 生成方式を設定します。

undo akm sae pwe コマンドはデフォルトに戻します。

WPA3-SAE は、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) を使用した PWE の生成をサポートしています。H2E は最新の PWE 生成方法であり、強化されたセキュリティパフォーマンスを提供します。

クライアントが指定された PWE 生成方式をサポートしていない場合、クライアントは WLAN にアクセスできません。クライアントの互換性を向上させる場合は、both-h2e-hnp キーワードを指定します。

例

WPA3-SAE の PWE 生成方式として H2E を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm sae pwe h2e

関連コマンド

wpa3

5.1.3 cipher-suite

🕮 **メモ：**

- QX-W1000 シリーズの AP はソフトウェアバージョン 7.2.19 を含む以降のソフトウェアから **gcmp** パラメータをサポートしています。
- QX-W1100 シリーズの AP はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアから、**gcmp** パラメータをサポートしています。
- QX-W1120 の Radio3 は、**gcmp** パラメータをサポートしていません。
- QX-W1130 の Radio1 は、**gcmp** パラメータをサポートしていません。

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Syntax

cipher-suite { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }

undo cipher-suite { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

ccmp: AES-CCMP 暗号方式を指定します。

gcmp: AES-GCMP 暗号方式を指定します。

tkip: TKIP 暗号方式を指定します。

wep40: WEP40 暗号方式を指定します。

wep104: WEP104 暗号方式を指定します。

wep128: WEP128 暗号方式を指定します。

説明

cipher-suite コマンドはフレーム暗号化に使用する暗号方式を指定します。

undo cipher-suite コマンドは指定した暗号方式を無効にします。

RSNA ネットワークに暗号方式を指定しなければなりません。WLAN サービステンプレートが無効の場合のみ暗号方式を設定します。

RSN IE あるいは WPA IE を設定するとき、TKIP、CCMP、あるいは GCMP 暗号方式を設定します。

WEP 暗号方式には、WEP40、WEP104、WEP128 の 3 タイプ含まれます。各 WLAN サービステンプレートは WEP 暗号方式の 1 タイプのみをサポートします。WEP 暗号方式のタイプを設定したあと、タイプの同じ鍵を作成および適用しなければなりません。

CCMP、TKIP あるいは GCMP 暗号方式が設定されている場合、WEP128 は設定できません。

例

フレーム暗号化用の TKIP 暗号方式を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite tkip

関連コマンド

- **security-ie**
- **wep key**
- **wep key-id**

5.1.4 enhanced-open enable

🕮 **メモ：**

enhanced-open enable コマンドはソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでサポートしています。

Syntax

enhanced-open enable

undo enhanced-open enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

enhanced-open enable コマンドは Enhanced Open システム認証を有効にします。

undo enhanced-open enable コマンドは Enhanced Open システム認証を無効にします。

例

Enhanced Open システム認証を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] enhanced-open enable

関連コマンド

enhanced-open transition-mode service-template

5.1.5 enhanced-open transition-mode service-template

🕮 **メモ：**

enhanced-open transition-mode service-template コマンドはソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでサポートしています。

Syntax

enhanced-open transition-mode service-template *service-template-name*

undo enhanced-open transition-mode service-template

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

service-template-name: 大文字と小文字を区別しない 1~63 文字の文字列でサービステンプレートの名前を指定します。

説明

enhanced-open transition-mode service-template コマンドは移行モードでの推奨サービステンプレートを指定します。

undo enhanced-open transition-mode service-template コマンドはデフォルトに戻します。

このコマンドを複数回実行した場合、最後に実行した設定が反映されます。

例

サービステンプレート **service1** に対して、移行モードでの推奨サービステンプレートとして **service2** を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] enhanced-open transition-mode service-template service2

関連コマンド

- **beacon ssid-hide**
- **enhanced-open enable**

5.1.6 gtk-rekey client-offline enable

Syntax

gtk-rekey client-offline enable

undo gtk-rekey client-offline enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey client-offline enable コマンドは offline-triggered GTK update を有効にします。

undo gtk-rekey client-offline コマンドはデフォルトに戻します。

GTK update が有効な場合のみ offline-triggered GTK update を有効にします。

例

offline-triggered GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey client-offline enable

関連コマンド

gtk-rekey enable

5.1.7 gtk-rekey enable

Syntax

gtk-rekey enable

undo gtk-rekey enable

デフォルト

GTK update のデフォルト値は、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.56 を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey enable コマンドは GTK update を有効にします。

undo gtk-rekey enable コマンドは GTK update を無効にします。

例

GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey enable

5.1.8 gtk-rekey method

Syntax

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

デフォルト

GTK は 86400 秒間隔でアップデートされます。

伝送パケット数のデフォルトは 10000000 です。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

packet-based *packet*: GTK がアップデートされる前に、マルチキャストとブロードキャストを含む伝送パケットの数を指定します。*packet* 引数の値の範囲は 5000~4294967295 です。

time-based *time*: GTK がアップデートされる間隔を指定します。*time* 引数の値の範囲は 180~604800 秒であり、デフォルトは 86400 秒です。

説明

gtk-rekey method コマンドは GTK update 手法を設定します。

undo gtk-rekey method コマンドはデフォルトに戻します。

GTK update が有効な場合のみ GTK update 手法を設定します。

直近のコンフィグレーションは、それ以前のコンフィグレーションを上書きします。例えば、packet に基づく手法を設定した後 time に基づく設定をする場合、time に基づく手法が効力をもちます。

サービステンプレートが有効になった後 GTK update 手法を設定する場合、以下の条件が存在するとき変更点が反映されます。

- GTK update 間隔を変更する場合、すでに設定されていたタイマが終了したとき新たな間隔が反映されます。
- パケット数しきい値を変更する場合、新たなしきい値は即座に反映されます。
- GTK update 手法を packet に基づく設定に変更する場合、タイマが消去されパケット数がしきい値に達したとき新たな設定が反映されます。
- GTK update 手法を time に基づく設定に変更する場合、新たな設定は即座に反映されます。

例

アップデート間隔に基づく GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey method time-based 3600

パケットに基づく GTK update を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] gtk-rekey method packet-based 600000

関連コマンド

gtk-rekey enable

5.1.9 key-derivation

Syntax

key-derivation { **sha1** | **sha1-and-sha256** | **sha256** }

undo key-derivation

デフォルト

sha1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

sha1: HMAC-SHA1 アルゴリズムを KDF として指定します。

sha256: HMAC-SHA256 アルゴリズムを KDF として指定します。

sha1-and-sha256: HMAC-SHA1 アルゴリズムと HMAC-SHA256 アルゴリズムを KDF として指定します。

説明

key-derivation コマンドは KDF（Key Derivation Function）を設定します。

undo key-derivation コマンドはデフォルトに戻します。

KDF は、RSNA メカニズムを使用するネットワークに対してのみ有効です。

管理フレーム保護が有効になっている場合、HMAC-SHA256 アルゴリズムを KDF として構成することをお勧めします。

例

HMAC-SHA256 アルゴリズムを KDF として構成します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] key-derivation sha256

関連コマンド

- **akm mode**

- **cipher-suite**
- **security-ie**

5.1.10 pmf

🕮 **メモ：**

192bit セキュリティなしの WPA3 エンタープライズは WPA2+管理フレーム保護(**pmf**)と同じです。管理フレーム保護を必須(**Mandatory**)として設定をすることで、192bit セキュリティなしの WPA3 エンタープライズと同等の動作をします。
管理フレーム保護を設定する場合は、KDF の設定”key-derivation sha1-and-sha256”をしてください。

Syntax

pmf { **mandatory** | **optional** }

undo pmf

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

mandatory: pmf 必須モードを有効にします。管理フレーム保護をサポートしたクライアントのみ WLAN にアクセスできます。

optional: pmf オプションモードを有効にします。すべてのクライアントが WLAN にアクセスできます。

説明

pmf コマンドは管理フレーム保護を有効にします。

undo pmf コマンドはデフォルトに戻します。

管理フレーム保護は、暗号化規格が RSN かつ暗号化方式が CCMP である RSNA メカニズムを使用するネットワークにのみ適用されます。

例

オプションモードで管理フレーム保護を有効にします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf optional

関連コマンド

- **cipher-suite**
- **security-ie**

5.1.11 pmf association-comeback

Syntax

pmf association-comeback *time*

undo pmf association-comeback

デフォルト

1 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time:アソシエーション復帰時間を指定します。設定範囲は 1~20 秒です。

説明

pmf association-comeback コマンドはアソシエーション復帰時間を設定します。

undo pmf association-comeback コマンドはデフォルトに戻します。

AP がクライアントからのアソシエーション要求もしくは再アソシエーション要求を拒否する場合、AP は要求が拒否されたことと、後でクライアントが接続できることを知らせる応答を送ります。この応答にはアソシエーション復帰時間が含まれています。アソシエーション復帰時間が終了すると、AP はクライアントからのアソシエーション要求もしくは再アソシエーション要求の受信を開始します。

例

association comeback time を 2 秒に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf association-comeback 2

5.1.12 pmf saquery retrycount

Syntax

pmf saquery retrycount *count*

undo pmf saquery retrycount

デフォルト

4 回

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

count: SA クエリ要求の最大試行回数を指定します。設定範囲は 1~16 です。

説明

pmf saquery retrycount コマンドは SA クエリ要求を再伝送する試行回数を最大にします。

undo pmf saquery retrycount コマンドはデフォルトに戻します。

最大試行回数に達した後 AP が SA クエリ要求への確認を受信しない場合、AP はクライアントをオフラインにします。

例

SA クエリ要求への最大試行回数を 3 に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf saquery retrycount 3

関連コマンド

- **pmf**
- **pmf saquery retrytimeout**

5.1.13 pmf saquery retrytimeout

Syntax

pmf saquery retrytimeout *timeout*

undo pmf saquery retrytimeout

デフォルト

200 ミリ秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

timeout: AP が SA クエリ要求を送信する間隔を指定します。設定範囲は 100～500 ミリ秒です。

説明

pmf saquery retrytimeout コマンドは SA クエリ要求を送信する間隔を設定します。

undo pmf saquery retrytimeout コマンドはデフォルトに戻します。

例

SA クエリ要求を送信する間隔を 300 ミリ秒に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf saquery retrytimeout 300

関連コマンド

- **pmf**
- **pmf saquery retrycount**

5.1.14 preshared-key

🕮 **メモ：**

ソフトウェアバージョン 7.2.79 を含む以降のソフトウェアから、**pass-phrase** 文字列で ”?” の文字の使用をサポートしています。

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

pass-phrase:文字列で PSK を設定します。

raw-key: 文字列で PSK を設定します。

cipher: 16 進数で PSK を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、プレーンテキストで指定された鍵は暗号化された形式で保存されます。

string: 鍵の文字列を指定します。この引数は大文字、小文字を区別します。鍵長は鍵タイプにより変わります。

- **pass-phrase(プレーンテキスト)**－8~63 文字
- **pass-phrase(暗号テキスト)**－8~117 文字
- **raw-key(プレーンテキスト)**－16 進数で 64 桁
- **raw-key(暗号テキスト)**－8~117 文字

説明

preshared-key コマンドは PSK を設定します。

undo preshared-key コマンドはデフォルトに戻します。

WLAN サービステンプレートが無効で、AKM モードが PSK のときにのみ PSK を設定します。AKM モードが 802.1X のときに PSK を設定した場合、WLAN サービステンプレートは有効ですが PSK コンフィグレーションは反映されません。

WLAN サービステンプレートに設定できる PSK は 1 つだけです。

例

PSK としてプレーンテキストで文字列 12345678 を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm mode psk

[AC-wlan-st-security] preshared-key pass-phrase simple 12345678

関連コマンド

akm mode

5.1.15 ptk-lifetime

Syntax

ptk-lifetime *time*

undo ptk-lifetime

デフォルト

43200 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: PTK ライフタイムを指定します。設定範囲は 180~604800 秒です。

説明

ptk-lifetime コマンドは PKT ライフタイムを設定します。

undo ptk-lifetime コマンドはデフォルトに戻します。

サービステンプレートが有効なときに PTK ライフタイムを設定する場合、その設定は既定のタイマが終了した後に反映されます。

例

PTK ライフタイムを 200 秒に設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-lifetime 200

5.1.16 ptk-rekey enable

Syntax

ptk-rekey enable

undo ptk-rekey enable

デフォルト

PTK 更新のデフォルト値は、ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.56 を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。

ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

View

WLAN service template view

定義済みユーザロール

network-admin

説明

ptk-rekey enable コマンドは PTK 更新を有効にします。

undo ptk-rekey enable コマンドは PTK 更新を無効にします。

この機能により、設定された PTK の有効期限が切れた後、装置は PTK を更新できます。

例

PTK 更新を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-rekey enable

関連コマンド

ptk-lifetime

5.1.17 security-ie

Syntax

security-ie { **osen** | **rsn** | **wpa** }

undo security-ie { **osen** | **rsn** | **wpa** }

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

osen: AP から送信されたビーコンおよびプローブ応答フレーム内の OSEN IE を有効にします。OSEN IE は、AP の OSEN 機能をアドバタイズします。

rsn: AP から送信されたビーコンおよびプローブ応答フレーム内の RSN IE を有効にします。RSN IE は、AP の RSN 機能をアドバタイズします。

wpa: AP から送信されたビーコンおよびプローブ応答フレーム内の WPA IE を有効にします。WPA IE は、AP の WPA 機能をアドバタイズします。

説明

security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を有効にします。

undo security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を無効にします。

RSNA ネットワークの暗号化規格を設定する必要があります。WLAN サービステンプレートが無効で、CCMP または TKIP 暗号化方式が設定されている場合のみ、暗号化規格を設定できます。

同じ WLAN サービステンプレートに対して WPA IE と RSN IE の両方を設定できます。WPA IE と RSN IE は、WLAN サービステンプレートの OSEN IE と一緒に使用することはできません。

暗号化規格に WPA2 または WPA3 を使用する場合は RSN IE、WPA を使用する場合は WPA IE を設定します。ワイファイアライアンス Anonymous 802.1X AKM の場合、OSEN IE を設定します。

例

ビーコン応答とプローブ応答で RSN IE をイネーブルにします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] security-ie rsn

関連コマンド

- **akm mode**
- **cipher-suite**

5.1.18 snmp-agent trap enable wlan usersec

Syntax

snmp-agent trap enable wlan usersec

undo snmp-agent trap enable wlan usersec

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan usersec コマンドは WLAN セキュリティに対して SNMP 通知を有効にします。

undo snmp-agent trap enable wlan usersec コマンドは WLAN セキュリティに対して SNMP 通知を無効にします

重要な WLAN セキュリティイベントを NMS に報告するために、WLAN セキュリティに対して SNMP 通知を有効にします。WLAN セキュリティイベント通知を正確に送信するため、オペレーションマニュアルのセクション 11 *システム管理 "SNMP"* に記載されているように SNMP の設定も行わなければなりません。

例

WLAN セキュリティに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan usersec

5.1.19 tkip-cm-time

Syntax

tkip-cm-time *time*

undo tkip-cm-time

デフォルト

0 秒

AP は対策をとりません。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: TKIP MIC 失敗ホールド時間を設定します。設定範囲は 0~3600 秒です。

説明

tkip-cm-time コマンドは TKIP MIC 失敗ホールド時間を設定します。

undo tkip-cm-time コマンドはデフォルトに戻します。

暗号化方式に TKIP が設定されているときにのみ TKIP MIC 失敗ホールド時間を設定します。

サービステンプレートが有効なときに MIC 失敗ホールド時間を設定する場合、その設定は既定のタイマが終了したあとに反映されます。

MIC 失敗ホールド時間内に AP が 2 つの MIC 失敗を検出した場合、AP はすべてのクライアントを 60 秒間分離させます。

例

TKIP MIC 失敗ホールド時間を 180 秒に設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] tkip-cm-time 180

関連コマンド

cipher-suite

5.1.20 wep key



重要:

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Syntax

wep key *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo wep key *key-id*

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

key-id: key ID を設定します。設定範囲は 1~4 です。

wep40: WEP40 key を設定します。

wep104: WEP104 key を設定します。

wep128: WEP128 key を設定します。

pass-phrase: WEP key を文字列で設定します。

raw-key: WEP key を 16 進数で設定します。

cipher: 暗号テキストで鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、平文形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵列を指定します。大文字と小文字を区別します。設定範囲は 37~73 文字です。プレーンテキストの鍵の長さは鍵タイプにより異なります。

- **wep40 pass-phrase(プレーンテキスト)**－5 文字
- **wep104 pass-phrase(プレーンテキスト)**－13 文字
- **wep128 pass-phrase(プレーンテキスト)**－16 文字
- **wep40 raw-key(プレーンテキスト)**－16 進数で 10 桁
- **wep104 raw-key(プレーンテキスト)**－16 進数で 26 桁
- **wep128 raw-key(プレーンテキスト)**－16 進数で 32 桁

説明

wep key コマンドは WEP 鍵を設定します。

undo wep key コマンドは設定した WEP 鍵を削除します。

WLAN サービステンプレートが無効で、暗号化方式に WEP が設定されているときにのみ WEP key を設定します。最大で 4 つの WEP key を設定できます。

例

暗号化方式に WEP40 を設定し、WEP key 1 としてプレーンテキスト 12345 を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite wep40

[AC-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345

関連コマンド

- **cipher-suite**
- **wep key-id**

5.1.21 wep key-id

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Syntax

wep key-id { **1** | **2** | **3** | **4** }

undo wep key-id

デフォルト

Key 1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

1: ID が 1 の WEP key を指定します。

2: ID が 2 の WEP key を指定します。

3: ID が 3 の WEP key を指定します。

4: ID が 4 の WEP key を指定します。

説明

wep key-id コマンドは WEP key を適用します。

undo wep key-id コマンドはデフォルトに戻します。

WLAN サービステンプレートが無効のときのみ WEP key を適用します。

RSNA メカニズムでは key 1 が交渉される鍵です。WEP key を適用するために、ID が 1 でない鍵を指定してください。

既存の WEP キーのみを適用できます。

例

暗号化方式に WEP40 を設定し、WEP key 1 としてプレーンテキスト 12345 を設定し、WEP key 1 を適用します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite wep40

[AC-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345

[AC-wlan-st-security] wep key-id 1

関連コマンド

wep key

5.1.22 wep mode dynamic

⚠ **重要**：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Syntax

wep mode dynamic

undo wep mode dynamic

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

wep mode dynamic コマンドはダイナミック WEP メカニズムを有効にします。

undo wep mode dynamic コマンドはダイナミック WEP メカニズムを無効にします。

WLAN サービステンプレートが無効のときのみ WEP メカニズムを有効にします。

ダイナミック WEP メカニズムはユーザアクセス認証のために 802.1X 認証を要求します。

ダイナミック WEP メカニズムが有効な場合、WEP key 4 を適用しないでください。

例

ダイナミック WEP メカニズムを有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wep mode dynamic

関連コマンド

- **cipher-suite**
- **client-security authentication-mode** (コマンドマニュアルのセクション 2 *WLAN "WLAN アクセスの設定"*)
- **wep key**
- **wep key-id**

5.1.23 wpa3

🕮 **メモ**:

- **wpa3** コマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- QX-W1100 シリーズの AP はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアから WPA3 エンタープライズの 192bit セキュリティをサポートしています。
- QX-W1120 の Radio3 は、WPA3 エンタープライズの 192bit セキュリティをサポートしていません。
- QX-W1130 の Radio1 は、WPA3 エンタープライズの 192bit セキュリティをサポートしていません。
- 192bit セキュリティなしの WPA3 エンタープライズについては、管理フレーム保護で実現します。**pmf** を参照してください。
- **enterprise-only-mode** のパラメータはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。
- **enterprise-transition-mode** のパラメータはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。
- **wpa3 enterprise-only-mode** と **wpa3 enterprise-transition-mode** を設定する場合、事前に **pmf** コマンドと **key-derivation** コマンドがサービステンプレートに設定されていないことを確認してください。

Syntax

wpa3 { **enterprise** | **enterprise-only-mode** | **enterprise-transition-mode** | **personal** { **mandatory** | **optional** } }

undo wpa3

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

mdc-admin

パラメータ

enterprise: WPA3 エンタープライズの 192bit セキュリティモードを使用します。

enterprise-only-mode: WPA3 エンタープライズで WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。このパラメータを指定した場合、**pmf mandatory**、**key-derivation sha256** を設定したときと同じ動作となります。

enterprise-transition-mode: WPA3 エンタープライズで WPA3 セキュリティモードを WPA3 移行モードに指定します。このモードでは、WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。このパラメータを指定した場合、**pmf optional**、**key-derivation sha1-and-sha256** を設定したときと同じ動作となります。

personal: WPA3 パーソナルを使用します。

mandatory: WPA3 パーソナルで WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。

optional: WPA3 パーソナルで WPA3 セキュリティモードをオプションモードに指定します。WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。

説明

wpa3 コマンドは WPA3 エンタープライズ(WPA3 必須モード、WPA3 移行モード、192bit セキュリティモード)、または、WPA3 パーソナルを有効にします。

undo wpa3 コマンドは WPA3 エンタープライズ(WPA3 必須モード、WPA3 移行モード、192bit セキュリティモード)、または、WPA3 パーソナルを無効にします。

- WPA3 エンタープライズの 192bit セキュリティモードー暗号化規格を RSN に設定し、暗号化方式を GCMP に設定する必要があります。

- WPA3 エンタープライズ(192bit セキュリティなし)ー暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。管理フレーム保護(**pmf**) 、または、**wpa3 enterprise-only-mode** コマンドか **wpa3 enterprise-transition-mode** コマンドを設定します。。
- WPA3 パーソナルー暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。

WPA3 セキュリティモードを有効にした後、管理フレーム保護を同時に有効にすることを推奨します。

例

WPA3 セキュリティモードをパーソナルレベルの必須モードに設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wpa3 personal mandatory

WPA3 エンタープライズのセキュリティモードを WPA3 必須モードに設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wpa3 enterprise-only-mode

目次

6 章 WLAN 認証 6-1
6.1 WLAN 認証設定コマンド 6-1
6.1.1 client-security accounting-delay time 6-1
6.1.2 client-security accounting-start trigger 6-2
6.1.3 client-security accounting-update trigger 6-4
6.1.4 client-security authentication fail-vlan 6-5
6.1.5 client-security authentication-location 6-6
6.1.6 client-security authentication-mode 6-7
6.1.7 client-security authorization-fail offline 6-9
6.1.8 client-security ignore-authorization 6-10
6.1.9 client-security intrusion-protection action 6-11
6.1.10 client-security intrusion-protection enable 6-12
6.1.11 client-security intrusion-protection timer temporary-block 6-13
6.1.12 client-security intrusion-protection timer temporary-service-stop 6-14
6.1.13 display wlan client-security block-mac 6-15
6.1.14 dot1x domain 6-16
6.1.15 dot1x handshake enable 6-17
6.1.16 dot1x handshake secure enable 6-18
6.1.17 dot1x max-user 6-19
6.1.18 dot1x re-authenticate enable 6-20
6.1.19 fail-permit enable 6-21
6.1.20 fail-permit template 6-23
6.1.21 mac-authentication domain 6-24
6.1.22 mac-authentication fast-connect enable 6-25
6.1.23 mac-authentication max-user 6-26
6.1.24 port-security oui 6-27
6.1.25 radius-server test-profile 6-28
6.2 Web 認証(ポータル認証)設定コマンド 6-30

6章 WLAN 認証

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

6.1 WLAN認証設定コマンド

本章では、WLAN に関する認証コマンドについて説明します。802.1X および MAC アドレス認証コマンドの情報については、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティ "802.1X"、"MAC アドレス認証"* を参照ください。

6.1.1 client-security accounting-delay time

Syntax

client-security accounting-delay time *time* [**no-ip-logoff**]

undo client-security accounting-delay time

デフォルト

装置がクライアントの IP アドレスを学習するとき、装置はアカウンティング開始要求をクライアントに送信します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: クライアントが 802.1X 認証もしくは MAC 認証を通過した後に開始するアカウンティング遅延タイマを指定します。値の範囲は 1～600 秒です。

no-ip-logoff: 遅延タイマ以内にクライアントの IP アドレスを取得できない場合、装置はクライアントをログオフします。このパラメータを指定しない場合、装置は遅延タイマが終了したときアカウンティング開始要求を送信します。

説明

client-security accounting-delay time コマンドはアカウンティング遅延を設定します。

undo client-security accounting-delay time コマンドはデフォルトに戻します。

装置がクライアントの指定されたタイプの IP アドレスを遅延時間内に学習できない場合、装置はクライアントに対して事前に定義されたアクションを実行します。アカウンティング開始権限を持つ IP アドレスのタイプを指定するために、**client-security accounting-start trigger** コマンドを使用します。IP アドレスのタイプを **none** に設定すると、アカウンティング遅延機能は適用されません。

アカウンティング遅延タイマを設定するとき、装置が IP アドレスを取得する時間を考慮してください。ローパフォーマンスなネットワークでは遅延タイマを大きく設定してください。

サービステンプレートが有効な状態でこのコマンドを実行すると、コマンド実行後に接続したクライアントにのみ設定が適用されます。このコマンドが実行される前からオンラインだったクライアントには適用されません。

例

サービステンプレート **service1** で、アカウンティング遅延タイマを 15 秒に設定します。装置がクライアントの IP アドレスを遅延タイマ以内に学習できない場合、クライアントをログオフするように設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security accounting-delay time 15 no-ip-logoff

関連コマンド

client-security accounting-start trigger

6.1.2 client-security accounting-start trigger

Syntax

client-security accounting-start trigger { **ipv4** | **none** }

undo client-security accounting-start trigger

デフォルト

IPv4

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ipv4: IPv4 アドレスタイプを指定します。

none: クライアントが認証をパスしたとき、クライアントにアカウンティング開始要求を送信するように設定します。

説明

client-security accounting-start trigger コマンドはアカウンティング開始権限を持つように IP アドレスタイプを指定します。

undo client-security accounting-start trigger コマンドはデフォルトに戻します。

このコマンドを設定すると、特定の IP アドレスタイプを使用したクライアントのために、装置はアカウンティングサーバにアカウンティング開始要求を送信します。このコマンドは、802.1X 認証あるいは MAC 認証をパスしたクライアントに適用されます。アカウンティングに関する詳細は QX-W1000/W1000 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

アカウンティング開始権限を持つように IP アドレスのタイプを設定するには、IP アドレスタイプの学習を有効にする必要があります。無線クライアント IP アドレス学習に関する詳細は、QX-W1000/W1000 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN IP スヌーピング"* を参照してください。

このコマンドを使用して設定された IP アドレスタイプは、アカウンティングサーバのプロトコル要件を満たす必要があります。

サービステンプレートが有効な状態でこのコマンドを実行すると、コマンド実行後に接続したクライアントにのみ設定が適用されます。このコマンドが実行される前からオンラインだったクライアントには適用されません。

例

サービステンプレート **service1** で、IPv4 アドレスを使用するクライアントに対してのみアカウンティング開始要求を送信するように装置を設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security accounting-start trigger ipv4

関連コマンド

- **client ipv4-snooping arp-learning enable**
- **client-security accounting-delay time**
- **client-security accounting-update trigger**

6.1.3 client-security accounting-update trigger

Syntax

client-security accounting-update trigger ipv4

undo client-security accounting-update trigger

デフォルト

装置は、サーバに割り当てられた、もしくはユーザに定義されたリアルタイムアカウンティング間隔で、アカウンティングアップデート要求をアカウンティングサーバに送信します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ipv4: IPv4 アドレスタイプを指定します。装置は、学習済みのクライアントの IP アドレスが IPv4 アドレスに変更されたときにのみアカウンティングアップデートを引き起こします。

説明

client-security accounting-update trigger コマンドはアカウンティングアップデート権限を持つように IP アドレスタイプを指定します。

undo client-security accounting-update trigger コマンドはデフォルトに戻します。

このコマンドは **client-security accounting-start trigger** コマンドを適用している場合にのみ適用できます。

このコマンドは、定期的なリアルタイムアカウンティング機能の影響を受けません。例えば、アカウンティングアップデートトリガを ipv4 に設定した状態でリアルタイムアカウンティング間隔を 12 分に設定した場合、どちらの設定も適用されます。両方の設定を使用したクライアントに対し、装置はアップデートアカウンティング要求を 12 分おきに送信します。また、クライアントの IP アドレスが IPv4 に変更されるたびに、装置はアカウンティングアップデートします。

リアルタイムアカウンティング間隔を設定するためには、**timer realtime-accounting** コマンドを使用してください。

サービステンプレートが有効な状態でこのコマンドを実行すると、コマンド実行後に接続したクライアントにのみ設定が適用されます。このコマンドが実行される前からオンラインだったクライアントには適用されません。

例

サービステンプレート **service1** で、クライアントの IP アドレスが IPv4 アドレスに変更されると装置がアカウンティングアップデートするように設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security accounting-update trigger ipv4

関連コマンド

- **client-security accounting-start trigger**
- **timer realtime-accounting**

6.1.4 client-security authentication fail-vlan

🕮 **メモ：**

このコマンドは、認証モードが MAC アドレス認証または PSK＋MAC アドレス認証の時に使用することができます。
802.1X 認証、PSK 認証では使用できません。

Syntax

client-security authentication fail-vlan *vlan-id*

undo client-security authentication fail-vlan

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: WLAN 制限 VLAN の ID を指定します。範囲は 1～4094 です。VLAN が作成されていることを確認してください。

説明

client-security authentication fail-vlan コマンドはサービステンプレートで WLAN 制限 VLAN を設定します。

undo client-security authentication fail-vlan コマンドはデフォルトに戻します。

組織のセキュリティ戦略に遵守できずに失敗したことが原因で WLAN 認証に失敗したクライアントに対応するため、クライアントを WLAN の制限 VLAN に収容することができます。例えば、間違ったパスワードやユーザ名を入力したクライアントに制限 VLAN が適応されます。制限 VLAN は認証タイムアウトあるいはネットワークの接続問題のために認証に失敗した WLAN クライアントに適応しません。

本コマンドは、サービステンプレートが無効なときに設定可能であり、サービステンプレートが有効になると適用されます。

例

サービステンプレート 1 で制限 VLAN として VLAN 10 を設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] client-security authentication fail-vlan 10

6.1.5 client-security authentication-location

🕮 **メモ**：

ap パラメータは、ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。

Syntax

client-security authentication-location { **ac** | **ap** }

undo client-security authentication-location

デフォルト

AC が WLAN クライアント認証の認証装置として動作します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac: AC を認証装置として指定します。

ap: AP を認証装置として指定します。

説明

client-security authentication-location コマンドはWLANクライアントの認証装置を指定します。

undo client-security authentication-location コマンドはデフォルトに戻します。

クライアントのデータトラフィックを転送するように AC が設定されている場合は、AP を認証者として指定することはできません(**client forwarding-location** コマンドを使用)。**client forwarding-location** コマンドの詳細については、*コマンドマニュアルの“WLAN アクセスの設定”*を参照してください。

client-security authentication-location コマンドと **client association-location** コマンドでは同一の装置を指定してください。**client association-location** コマンドの詳細については、*コマンドマニュアルの“WLAN アクセスの設定”*を参照してください。

本コマンドは、サービステンプレートが無効なときに設定可能であり、サービステンプレートが有効になると適用されます。

例

サービステンプレート **s1** で WLAN クライアントの認証装置として AC を設定します。

<AC> system-view

[AC] wlan service-template s1

[AC-wlan-st-s1] client-security authentication-location ac

関連コマンド

- **client forwarding-location**
- **client association-location** （*コマンドマニュアルの “WLAN アクセスの設定”*）

6.1.6 client-security authentication-mode

🕮 **メモ**:

- **mac-and-dot1x** パラメータは、ソフトウェアバージョン 7.1.11 を含む以降のソフトウェアからサポートしています。
- **mac-then-dot1x** と **dot1x-then-mac** のパラメータは、EAP relay では使用できません。

Syntax

client-security authentication-mode { **dot1x** | **dot1x-then-mac** | **mac** | **mac-then-dot1x** | **oui-then-dot1x** | **mac-and-dot1x** }

undo client-security authentication-mode

デフォルト

設定なし。装置は認証を実行しません（認証バイパスモード）。クライアントは直接装置にアクセスすることができます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X 認証のみを実行します。

dot1x-then-mac: 最初に 802.1X 認証を実行し、次に MAC アドレス認証を実行します。クライアントが 802.1X 認証を通過した場合、MAC アドレス認証は実行されません。

mac: MAC アドレス認証のみを実行します。

mac-then-dot1x: 最初に MAC アドレス認証を実行し、次に 802.1X 認証を実行します。クライアントが MAC 認証を通過した場合、802.1X 認証は実行されません。

oui-then-dot1x: 最初に OUI 認証を実行し、次に 802.1X 認証を実行します。クライアントが OUI 認証を通過した場合、802.1X 認証は実行されません。

mac-and-dot1x: MAC アドレス認証と 802.1X 認証の２つの認証（マルチステップ認証）を実行します。MAC アドレス認証を最初に実行し、MAC アドレス認証にパスした場合のみ、802.1X 認証を実行します。２つの認証にパスしたクライアントの接続が許可されます。

説明

client-security authentication-mode コマンドは WLAN クライアントの認証モードを設定します。

undo client-security authentication-mode コマンドはデフォルトに戻します。

サービステンプレートはどの認証モードにおいても複数の認証モードへのアクセスを許可します。802.1X クライアントの最大数を設定するには、**dot1x max-user** コマンドを使用します。MAC アドレス認証クライアントの最大数を設定するには、**mac-authentication max-user** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** でサービスにおける WLAN クライアントの認証モードを **mac** に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security authentication-mode mac

6.1.7 client-security authorization-fail offline

Syntax

client-security authorization-fail offline

undo client-security authorization-fail offline

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security authorization-fail offline コマンドは authentication-fail offline 機能を有効にします。

undo client-security authorization-fail offline コマンドは authentication-fail offline 機能を無効にします。

authorization-fail-offline 機能は ACL あるいはユーザプロファイルで許可されていない WLAN クライアントをログオフします。

以下の状況では、クライアントは ACL あるいはユーザプロファイルの許可に失敗します。

- 装置あるいはサーバは、クライアントに指定した ACL あるいはユーザプロファイルの許可に失敗する。
- 許可された ACL あるいはユーザプロファイルが存在しない。

本機能が無効の場合、装置は ACL あるいはユーザプロファイルの許可に失敗した WLAN クライアントをログオフしませんが、装置は失敗ログを残します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** で authorization-fail-offline 機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security authorization-fail offline

6.1.8 client-security ignore-authorization

Syntax

client-security ignore-authorization

undo client-security ignore-authorization

デフォルト

装置はサーバから受け取った認証情報を使用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client-security ignore-authorization コマンドは装置が認証サーバ（RADIUS サーバやローカル装置）から受信した許可情報を無視するよう設定します。

undo client-security ignore-authorization コマンドはデフォルトに戻します。

クライアントが RADIUS あるいはローカル認証を通過した後、サーバはユーザアカウントに設定された許可属性に基づいて許可を実行します。例えば、サーバは VLAN を割り当てることが可能です。装置にこれらのクライアント許可属性を使用させたくない場合、本コマンドを設定してサーバからの許可情報を無視するよう設定します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

例

サービステンプレート **service1** で認証サーバからの許可情報を無視するよう設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security ignore-authorization

6.1.9 client-security intrusion-protection action

Syntax

client-security intrusion-protection action { **service-stop** | **temporary-block** | **temporary-service-stop** }

undo client-security intrusion-protection action

デフォルト

temporary-block

View

Service template view

定義済みユーザロール

network-admin

パラメータ

service-stop: 無線インタフェースの BSS が手動で有効にされるまで、不正フレームが受信された BSS を停止します。

temporary-block: 一定期間、不正フレームの送信元 MAC アドレスをブロック MAC アドレスリストに追加します。期間の設定には **client-security intrusion-protection timer temporary-block** コマンドを使用します。

temporary-service-stop: 一定期間、不正フレームが受信された BSS を停止します。期間の設定には **intrusion-protection timer temporary-service-stop** コマンドを使用します。

説明

client-security authentication-mode コマンドは不正フレームを検出した場合に装置が実施する侵入保護アクションを設定します。

undo client-security intrusion-protection action コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

本コマンドの効果を発生させるには、侵入保護機能を有効にするため、**client-security intrusion-protection enable** コマンドを使用する必要があります。

例

サービステンプレート **service1** で、侵入保護機能が不正フレームを検出した装置で BSS を停止するよう設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

[AC-wlan-st-service1] client-security intrusion-protection action service-stop

関連コマンド

- **client-security intrusion-protection enable**
- **client-security intrusion-protection timer temporary-block**
- **client-security intrusion-protection timer temporary-service-stop**

6.1.10 client-security intrusion-protection enable

Syntax

client-security intrusion-protection enable

undo client-security intrusion-protection enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security intrusion-protection enable コマンドは侵入保護機能を有効にします。

undo client-security intrusion-protection enable コマンドは侵入保護機能を無効にします。

装置が不正なクライアントからの接続要求を受信した場合、要求を受信した BSS で事前定義された保護アクションを実行します。WLAN 認証に失敗した場合、その MAC アドレスのクライアントは不正クライアントになります。保護アクションを設定するには、**client-security intrusion-protection action** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** で、侵入保護機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

関連コマンド

client-security intrusion-protection action

6.1.11 client-security intrusion-protection timer temporary-block

Syntax

client-security intrusion-protection timer temporary-block *time*

undo client-security intrusion-protection timer temporary-block

デフォルト

180 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: MAC アドレスがブロックされる期間を指定します。範囲は 60～300 秒です。

説明

client-security intrusion-protection timer temporary-block コマンドは侵入保護によって MAC アドレスがブロックされる期間を設定します。

undo client-security intrusion-protection timer temporary-block コマンドはデフォルトに戻します。

本コマンドは侵入保護アクションが **temporary-block** の場合のみ有効です。

サービステンプレートを有効にした後にブロック期間を変更した場合、新しい設定は、その後に検出した不正パケットに対して適用されます。

例

サービステンプレート **service1** で、不正 MAC アドレスのブロック期間を 120 秒に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

[AC-wlan-st-service1] client-security intrusion-protection action temporary-block

[AC-wlan-st-service1] client-security intrusion-protection timer temporary-block 120

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection enable**

6.1.12 client-security intrusion-protection timer temporary-service-stop

Syntax

client-security intrusion-protection timer temporary-service-stop *time*

undo client-security intrusion-protection timer temporary-service-stop

デフォルト

20 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: BSS が停止する期間を指定します。範囲は 10～300 秒です。

説明

client-security intrusion-protection timer temporary-service-stop コマンドは侵入保護による BSS 停止期間を設定します。

undo client-security intrusion-protection timer temporary-service-stop コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

サービステンプレートを有効にした後に BSS 停止期間を変更した場合、新しい設定は、その後に検出した不正パケットに対して適用されます。

例

サービステンプレート **service1** で、BSS 停止期間を 30 秒に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client-security intrusion-protection enable

[AC-wlan-st-service1] client-security intrusion-protection action temporary-service-stop

[AC-wlan-st-service1] client-security intrusion-protection timer temporary-service-stop 30

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection enable**

6.1.13 display wlan client-security block-mac

Syntax

display wlan client-security block-mac [**ap** *ap-name* [**radio** *radio-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。オプションを指定しない場合、コマンドはすべてのブロックされた MAC アドレスについての情報を表示します。

radio *radio-id*: 無線を ID で指定します。無線 ID の値の範囲は AP モデルにより異なります。本オプションを指定しない場合、本コマンドは指定された AP のすべての無線についてブロックされた MAC アドレスの情報を表示します。

説明

display wlan client-security block-mac コマンドは WLAN クライアントのブロックされた MAC アドレス情報を表示します。

侵入保護アクションが **temporary-block** である場合、認証に失敗した MAC アドレスがブロック MAC アドレスリストに追加されます。

例

すべてのブロックされた MAC アドレス情報を表示します。

<AC> display wlan client-security block-mac

```
MAC address        AP ID      RADIO ID    BSSID
0002-0002-0002     1          1           00ab-0de1-0001
000d-88f8-0577     1          1           0ef1-0001-02c1
```

```
Total entries: 2
```

表 6-1 コマンド出力

フィールド	説明
MAC address	ブロックされたMACアドレス。（H-H-H形式）
AP ID	ブロックされたMACアドレスのAP ID
RADIO ID	ブロックされたMACアドレスの無線ID
BSSID	ブロックされたMACアドレスのBSS-ID（H-H-H形式）
Total entries	ブロックされたMACアドレスの数

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection timer temporary-block**

6.1.14 dot1x domain

Syntax

dot1x domain *domain-name*

undo dot1x domain

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字小文字を区別ません。

説明

dot1x domain コマンドはサービステンプレートで 802.1X クライアントのための認証ドメインを指定します。

undo dot1x domain コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

802.1X は以下の順番で WLAN クライアントのための認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメイン
2) ユーザ名で指定されたドメイン
3) デフォルト認証ドメイン

例

サービステンプレート **service1** で、802.1X クライアントのための認証ドメインとして **my-domain** を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x domain my-domain

6.1.15 dot1x handshake enable

Syntax

dot1x handshake enable

undo dot1x handshake enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake enable コマンドは 802.1X オンラインユーザハンドシェイク機能を有効にします。

undo dot1x handshake enable コマンドは 802.1X オンラインユーザハンドシェイク機能を無効にします。

オンラインユーザハンドシェイク機能は、定期的にクライアントにハンドシェイクメッセージを送信することにより、オンライン 802.1X クライアントの接続状態を確認します。最大ハンドシェイク試行回数に到達してもハンドシェイクタイマ内にクライアントから応答を受信しない場合、装置はクライアントをオフライン状態にします。ハンドシェイ

クタイマの設定には、**dot1x timer handshake-period** コマンドを使用します。最大ハンドシェイク試行回数の設定には、**dot1x retry** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます

例

サービステンプレート **service1** で、802.1X クライアントのためのオンラインユーザハンドシェイク機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x handshake enable

関連コマンド

- **dot1x handshake secure enable**
- **dot1x retry**（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*）
- **dot1x timer handshake-period**（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*）

6.1.16 dot1x handshake secure enable

Syntax

dot1x handshake secure enable

undo dot1x handshake secure enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake secure enable コマンドは 802.1X オンラインユーザハンドシェイクセキュリティ機能を有効にします。

undo dot1x handshake secure enable コマンドは 802.1X オンラインユーザハンドシェイクセキュリティ機能を無効にします。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に効果が発生します。

オンラインユーザハンドシェイクセキュリティ機能を有効にするには、オンラインユーザハンドシェイク機能が有効になっている必要があります。

オンラインユーザハンドシェイクセキュリティ機能は、認証されたオンラインの 802.1X クライアントのみを保護します。

例

サービステンプレート **service1** で、802.1X クライアントのためのオンラインユーザハンドシェイクセキュリティ機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x handshake enable

[AC-wlan-st-service1] dot1x handshake secure enable

関連コマンド

dot1x handshake enable

6.1.17 dot1x max-user

Syntax

dot1x max-user *count*

undo dot1x max-user

デフォルト

512

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count: 同時接続 802.1X クライアントの最大数を設定します。範囲は 1～512 です。

説明

dot1x max-user コマンドはサービステンプレートで 802.1X クライアントの最大同時接続数を設定します。

undo dot1x max-user コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

最大数に達した場合、サービステンプレートは以降の 802.1X クライアントを拒否します。

メモ：

- 802.1X 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W1100 シリーズは 512、QX-W1000 シリーズは 256 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

例

サービステンプレート **service1** で、802.1X クライアントの最大接続数を 500 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x max-user 500

6.1.18 dot1x re-authenticate enable

Syntax

dot1x re-authenticate enable

undo dot1x re-authenticate enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate enable コマンドはサービステンプレートで 802.1X クライアントの定期的なオンラインユーザ再認証機能を有効にします。

undo dot1x re-authenticate enable コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

定期的再認証により、サービステンプレートにおいてオンラインの 802.1X クライアントを装置が定期的に認証することが可能になります。本機能はオンラインクライアントの接続状態を確認し、サーバによって割り当てられた許可属性をアップデートします。属性には ACL、VLAN ベースのユーザプロファイルが含まれます。

dot1x timer reauth-period コマンドにより、再認証の間隔を設定することができます。

サーバによって割り当てられた RADIUS 属性の Session-Timeout、Termination-Action は、定期的なオンラインユーザの再認証に影響します。サーバによって割り当てられた Session-Timeout、Termination-Action を表示するには、**display dot1x connection** コマンドを使用します（QX-W1000/W1000 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティ “802.1X”* を参照してください）。

- Termination-Action が **Default**（ログオフ）の場合、テンプレート内のオンラインユーザ再認証は、定期的再認証タイマがセッションタイムアウトタイマよりも小さい場合のみ適用されます。
- Termination-Action が **Radius-request** の場合、テンプレート内のオンラインユーザ再認証は動作しません。装置は、セッションタイムアウトタイマの期限切れ後にオンライン 802.1X クライアントを再認証します。

例

サービステンプレート **service1** で、802.1X クライアントの定期的再認証機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] dot1x re-authenticate enable

関連コマンド

dot1x timer（コマンドマニュアルのセクション 9 *セキュリティ “802.1X”*）

6.1.19 fail-permit enable

🕮 **メモ**：

- このコマンドはソフトウェアバージョン 7.2.26 を含む以降のソフトウェアからサポートしています。
- hybrid remote-ap enable コマンドが設定されている AP では、AP が AC と通信不能になっても、失敗許可機能は使用できません

Syntax

fail-permit enable [**keep-online**]

undo fail-permit enable

デフォルト

無効

Views

Service template view

定義済みユーザロール

network-admin

パラメータ

keep-online: 失敗許可機能が動作する際、オンラインのクライアントが切断されるのを防ぎます。

説明

fail-permit enable コマンドは失敗許可機能を有効にします。

undo fail-permit enable コマンドは失敗許可機能を無効にします。

失敗許可機能は以下の目的で使用します。

- **認証失敗許可**—RADIUS サーバもしくは AC と AP が切断されたあと、802.1X 認証、MAC 認証、もしくは PSK 認証クライアントがネットワークにアクセスできるようになります。RADIUS サーバもしくは AC との切断が発生すると、AP はクライアントに対して継続してアクセスサービスを提供し、トラフィックを転送します。

fail-permit enable コマンドは、サービステンプレートが無効になっている場合にのみ実行でき、サービステンプレートが有効になった後に有効になります。

fail-permit enable コマンドと **fail-permit template** コマンドを同一のサービステンプレートに設定しないでください。

例

#サービステンプレートで失敗許可機能を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] fail-permit enable

関連コマンド

fail-permit template

6.1.20 fail-permit template

🕮 メモ：

- このコマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- 失敗許可機能はソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
- 1 つの無線に対して設定できるバックアップ用のサービステンプレート(SSID)は 1 つのみです。

Syntax

fail-permit template

undo fail-permit template

デフォルト

設定なし

Views

Service template view

定義済みユーザロール

network-admin

説明

fail-permit template コマンドはレーダーによる通信停止回避のため、もしくは 802.1X 認証での失敗許可機能のためのバックアップ用サービステンプレートとして指定します。

undo fail-permit template コマンドはレーダーによる通信停止回避のため、もしくは 802.1X 認証での失敗許可機能のためのバックアップ用サービステンプレート指定を削除します。

レーダーによる通信停止回避を行うためには 1 つのサービステンプレートに対して、1 つのバックアップ用のサービステンプレートを用意します。

- バックアップ用サービステンプレートには、**fail-permit service template** コマンドを追加する点を除き、オリジナルのサービステンプレートと同じ設定を含める必要があります。
- バックアップ用サービステンプレートは、オリジナルのサービステンプレートとは異なる無線にバインドする必要があります。

802.1X 認証で失敗許可機能を使用する場合、サービステンプレートを 2 つ設定します。1 つのサービステンプレートには 802.1X 認証の設定および **fail-permit enable** コマンドを設定します。もう一方のサービステンプレートにはバックアップ用に PSK 認証もしく

は 802.1X 認証および **fail-permit template** コマンドを設定します。AP が AC もしくは RADIUS サーバと通信不能になるまではバックアップ用の SSID は表示されません。AP が AC と通信不能になってから、もしくは RADIUS サーバと通信不能になってから数分後に失敗許可機能が動作します。接続済みのクライアントは接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。AC もしくは RADIUS サーバと AP の切断前は、クライアントは 802.1X 認証で認証されます。切断後はバックアップ用の PSK 認証で認証されます。

fail-permit template コマンドは、サービステンプレートが無効になっている場合にのみ実行でき、サービステンプレートが有効になった後に有効になります。

fail-permit enable コマンドと **fail-permit template** コマンドを同一のサービステンプレートに設定しないでください。

例

#サービステンプレートを障害許可サービステンプレートとして指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] fail-permit template

関連コマンド

fail-permit enable

6.1.21 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字と小文字を区別しません。

説明

mac-authentication domain コマンドはサービステンプレートで MAC 認証クライアントのための認証ドメインを指定します。

undo mac-authentication domain コマンドはデフォルトに戻します

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

MAC 認証は以下の順番で WLAN クライアントのための認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメイン
2) ユーザ名で指定されたドメイン
3) デフォルト認証ドメイン

例

サービステンプレート **service1** で、MAC 認証クライアントのための認証ドメインとして **my-domain** を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] mac-authentication domain my-domain

6.1.22 mac-authentication fast-connect enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。

Syntax

mac-authentication fast-connect enable

undo mac-authentication fast-connect enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

mac-authentication fast-connect enable コマンドは、MAC 認証クライアントのための AC 内ローミング高速接続を有効にします。

undo mac-authentication fast-connect enable コマンドは、MAC 認証クライアントのための AC 内ローミング高速接続を無効にします。

本コマンドを有効にすることで、AC で MAC 認証されたクライアントが、同じ AC に管理された別の AP に移動する際、再認証なしでローミングできるようになります。

本機能は MAC 認証を利用する無線クライアントにのみ適用され、authentication-location と association-location はどちらも AC である必要があります。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート **service1** で、MAC 認証クライアントのための AC 内ローミング高速接続を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] mac-authentication fast-connect enable

関連コマンド

- **client-security authentication-mode**
- **client-security authentication-location**
- **client association-location**（コマンドマニュアルの *“4 章 WLAN アクセスの設定”*）

6.1.23 mac-authentication max-user

Syntax

mac-authentication max-user *count*

undo mac-authentication max-user

デフォルト

512

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count: 同時接続 MAC 認証クライアントの最大数を設定します。範囲は 1～512 です。

説明

mac-authentication max-user コマンドはサービステンプレートで MAC 認証クライアントの最大同時接続数を設定します。

undo mac-authentication max-user コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

最大数に達した場合、サービステンプレートは以降の MAC 認証クライアントを拒否します。

🕮 **メモ**:

- MAC アドレス認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W1100 シリーズは 512、QX-W1000 シリーズは 256 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

例

サービステンプレート **service1** で、MAC 認証クライアントの最大接続数を 32 に設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] mac-authentication max-user 32

6.1.24 port-security oui

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

index-value: OUI 値を 1～16 の範囲で設定します。

oui-value: OUI 文字列、すなわち H-H-H フォーマットの 48 ビット MAC アドレスを指定します。システムは、上位 24 ビットのみを OUI 値として使用します。

説明

port-security oui コマンドは OUI 認証用の OUI 値を設定します。

undo port-security oui コマンドは指定した OUI 値を削除します。

OUI（MAC アドレスの最初の 24 バイナリビット）は、IEEE によってデバイスベンダを一意に識別するために割り当てられます。特定の無線デバイスからのパケットが認証を開始できるように装置を設定する場合、このコマンドを使用します。たとえば、企業がイントラネット内のベンダ A の IP 電話だけを許可する場合、このコマンドを使用して、ベンダ A の OUI を指定します。

このコマンドを使用して設定された OUI 値は、認証モードが oui-or-dot1x の場合にのみ適用されます。oui-or-dot1x モードのポートは、1 つの 802.1X 認証ユーザからのフレームと、MAC アドレスが特定の OUI を含む 1 人のユーザからのフレームを許可します。

例

OUI 値 000d2a をセットし、インデックスを 4 に設定します。

<AC> system-view

[AC] port-security oui index 4 mac-address 000d-2a10-003

6.1.25 radius-server test-profile

メモ：

このコマンドはソフトウェアバージョン 7.2.26 を含む以降のソフトウェアからサポートしています。

Syntax

radius-server test-profile *profile-name* **username** *name* [**interval** *interval*]

undo radius-server test-profile *profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: テストプロファイルの名前を指定します。大文字と小文字を区別します。文字数は 1～31 文字です。

username *name*: 検出パケット内のユーザ名を指定します。*name* パラメータは大文字と小文字を区別し、1～253 文字で指定します。

interval *interval*: 検出パケットを送信する間隔を分で設定します。*Interval* パラメータの値の範囲は 1～3600 で、デフォルトは 60 です。

説明

radius-server test-profile コマンドは RADIUS サーバの状態を検出するためのテストプロファイルを設定します。

undo radius-server test-profile コマンドはテストプロファイルを削除します。

装置は、サーバに対して指定されたテストプロファイルが存在する場合にのみ、RADIUS サーバの状態検出を開始します。存在しないテストプロファイルを RADIUS サーバに対して指定した場合、装置上にテストプロファイルを作成するまで、装置はサーバの状態を検出しません。

テストプロファイルを削除すると、装置は削除したテストプロファイルを使用していた RADIUS サーバの状態の検出を停止します。

このコマンドを複数回実行することで、複数のテストプロファイルを設定できます。

例

RADIUS サーバの状態を検出するためにテストプロファイル **abc** を設定します。ユーザ名 **admin** を使用した検出パケットを 10 分ごとに送信します。

<AC> system-view

[AC] radius-server test-profile abc username admin interval 10

関連コマンド

- **primary authentication**（コマンドマニュアルのセクション 9 *セキュリティ “AAA”*）
- **secondary authentication**（コマンドマニュアルのセクション 9 *セキュリティ “AAA”*）

6.2 Web認証(ポータル認証)設定コマンド

Web 認証(ポータル認証)の設定に関するコンフィグについては、別紙の共通マニュアル”*QX-W シリーズ Web 認証(ポータル認証)コマンドマニュアル*”を参照してください。

目次

7 章 WIPS の設定 7-1
7.1 WIPS の設定コマンド 7-1
7.1.1 ap-channel-change 7-1
7.1.2 ap-classification rule 7-2
7.1.3 ap-flood 7-2
7.1.4 ap-impersonation 7-3
7.1.5 apply ap-classification rule 7-4
7.1.6 apply classification policy 7-5
7.1.7 apply countermeasure policy 7-6
7.1.8 apply detect policy 7-7
7.1.9 apply signature policy 7-8
7.1.10 apply signature rule 7-8
7.1.11 ap-rate-limit 7-9
7.1.12 ap-spoofing 7-10
7.1.13 ap-timer 7-11
7.1.14 association-table-overflow 7-12
7.1.15 authentication 7-13
7.1.16 block mac-address 7-14
7.1.17 classification policy 7-15
7.1.18 client-online 7-16
7.1.19 client-rate-limit 7-17
7.1.20 client-spoofing 7-18
7.1.21 client-timer 7-18
7.1.22 countermeasure adhoc 7-20
7.1.23 countermeasure attack all 7-21
7.1.24 countermeasure attack deauth-broadcast 7-21
7.1.25 countermeasure attack disassoc-broadcast 7-22
7.1.26 countermeasure attack honeypot-ap 7-23
7.1.27 countermeasure attack hotspot-attack 7-23
7.1.28 countermeasure attack ht-40-mhz-intolerance 7-24
7.1.29 countermeasure attack malformed-packet 7-25
7.1.30 countermeasure attack man-in-the-middle 7-26
7.1.31 countermeasure attack omerta 7-26
7.1.32 countermeasure attack power-save 7-27
7.1.33 countermeasure attack soft-ap 7-28
7.1.34 countermeasure attack unencrypted-trust-client 7-28
7.1.35 countermeasure attack weak-iv 7-29

7.1.36 countermeasure attack windows-bridge 7-30
7.1.37 countermeasure external-ap 7-31
7.1.38 countermeasure mac-address 7-31
7.1.39 countermeasure misassociation-client 7-32
7.1.40 countermeasure misconfigured-ap 7-33
7.1.41 countermeasure policy 7-34
7.1.42 countermeasure potential-authorized-ap 7-34
7.1.43 countermeasure potential-external-ap 7-35
7.1.44 countermeasure potential-rogue-ap 7-36
7.1.45 countermeasure rogue-ap 7-37
7.1.46 countermeasure unauthorized-client 7-37
7.1.47 countermeasure uncategorized-ap 7-38
7.1.48 countermeasure uncategorized-client 7-39
7.1.49 deauthentication-broadcast 7-39
7.1.50 detect policy 7-40
7.1.51 detect signature 7-41
7.1.52 disassociation-broadcast 7-42
7.1.53 detect dissociate-client enable 7-43
7.1.54 discovered-ap 7-44
7.1.55 display wips sensor 7-45
7.1.56 display wips statistics 7-46
7.1.57 display wips virtual-security-domain countermeasure record 7-51
7.1.58 display wips virtual-security-domain device 7-52
7.1.59 display wlan nat-detect 7-59
7.1.60 flood association-request 7-60
7.1.61 flood authentication 7-61
7.1.62 flood beacon 7-62
7.1.63 flood block-ack 7-63
7.1.64 flood cts 7-64
7.1.65 flood deauthentication 7-65
7.1.66 flood disassociation 7-66
7.1.67 flood eap-failure 7-67
7.1.68 flood eapol-logoff 7-68
7.1.69 flood eapol-start 7-69
7.1.70 flood eap-success 7-70
7.1.71 flood null-data 7-71
7.1.72 flood probe-request 7-72
7.1.73 flood reassociation-request 7-73
7.1.74 flood rts 7-74
7.1.75 frame-type 7-75
7.1.76 honeypot-ap 7-76
7.1.77 hotspot-attack 7-77
7.1.78 ht-40mhz-intolerance 7-78

7.1.79 ht-greenfield 7-79
7.1.80 ignorelist 7-79
7.1.81 import hotspot 7-80
7.1.82 import oui 7-81
7.1.83 invalid-oui-classify illegal 7-82
7.1.84 mac-address 7-83
7.1.85 malformed duplicated-ie 7-84
7.1.86 malformed fata-jack 7-85
7.1.87 malformed illegal-ibss-ess 7-85
7.1.88 malformed invalid-address-combination 7-86
7.1.89 malformed invalid-assoc-req 7-87
7.1.90 malformed invalid-auth 7-88
7.1.91 malformed invalid-deauth-code 7-89
7.1.92 malformed invalid-disassoc-code 7-90
7.1.93 malformed invalid-ht-ie 7-91
7.1.94 malformed invalid-ie-length 7-92
7.1.95 malformed invalid-pkt-length 7-93
7.1.96 malformed large-duration 7-94
7.1.97 malformed null-probe-resp 7-95
7.1.98 malformed overflow-eapol-key 7-96
7.1.99 malformed overflow-ssid 7-97
7.1.100 malformed redundant-ie 7-98
7.1.101 man-in-the-middle 7-99
7.1.102 manual-classify mac-address 7-100
7.1.103 omerta 7-101
7.1.104 oui 7-101
7.1.105 pattern 7-102
7.1.106 permit-channel 7-103
7.1.107 power-save 7-105
7.1.108 prohibited-channel 7-106
7.1.109 report-interval 7-107
7.1.110 reset wips statistics 7-107
7.1.111 reset wips virtual-security-domain 7-108
7.1.112 reset wips virtual-security-domain countermeasure record 7-109
7.1.113 reset wlan nat-detect 7-110
7.1.114 rssi 7-110
7.1.115 rssi-change-threshold 7-111
7.1.116 rssi-threshold 7-112
7.1.117 security 7-113
7.1.118 select sensor all 7-114
7.1.119 seq-number 7-114
7.1.120 signature policy 7-115
7.1.121 signature rule 7-116

7.1.122 soft-ap 7-117
7.1.123 ssid (AP classification rule view) 7-117
7.1.124 ssid (signature view) 7-118
7.1.125 ssid-length 7-119
7.1.126 trust mac-address 7-120
7.1.127 trust oui 7-121
7.1.128 trust ssid 7-122
7.1.129 unencrypted-authorized-ap 7-123
7.1.130 unencrypted-trust-client 7-123
7.1.131 up-duration 7-124
7.1.132 virtual-security-domain 7-125
7.1.133 weak-iv 7-126
7.1.134 windows-bridge 7-127
7.1.135 wips 7-127
7.1.136 wips enable 7-128
7.1.137 wips virtual-security-domain 7-129
7.1.138 wireless-bridge 7-130
7.1.139 wlan nat-detect 7-131

7章 WIPS の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

7.1 WIPSの設定コマンド

7.1.1 ap-channel-change

Syntax

ap-channel-change [**quiet** *quiet-value*]

undo ap-channel-change

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がチャネル変更のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にチャネル変更を検出してもアラームを引き起こしません。

説明

ap-channel-change コマンドはチャネル変更の設定をします。

undo ap-channel-change コマンドはチャネル変更の検出を無効にします。

例

チャネル変更の検出を有効にし、遅延時間を 5 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-channel-change quiet 5

7.1.2 ap-classification rule

Syntax

ap-classification rule *rule-id*

undo ap-classification rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。値の範囲は 1～65535 です。

説明

ap-classification rule コマンドは AP 分類ルールを作成し、その view に移行します。AP 分類ルールがすでに存在する場合、**ap-classification rule** コマンドで AP classification rule view に移行します。

undo ap-classification rule コマンドは AP 分類ルールを削除します。

例

AP classification rule 1 を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

7.1.3 ap-flood

Syntax

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

undo ap-flood

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

apnum *apnum-value*: AP 数しきい値を指定します。値の範囲は 10～200 です。デフォルト値は 80 です。

exceed *exceed-value*: 超過を許可された AP の最大数を指定します。*exceed-value* 引数の値の範囲は 10～200 です。デフォルト値は 80 です。AP の数が、AP 数しきい値と、超過を許可された AP の最大数の合計を超える場合、WIPS は AP フラッド攻撃アラームを引き起こします。

quiet *quiet-value*: WIPS が AP フラッド攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP フラッド攻撃を検出してもアラームを引き起こしません。

説明

ap-flood コマンドは AP フラッド攻撃検出を設定します。

undo ap-flood コマンドは AP フラッド攻撃検出を無効にします。

例

AP フラッド攻撃検出を有効にし、*apnum-value*、*exceed-value*、*quiet-value* をそれぞれ 50、50、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-flood apnum 50 exceed 50 quiet 100

7.1.4 ap-impersonation

Syntax

ap-impersonation [**quiet** *quiet-value*]

undo ap-impersonation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP なりすまし攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP なりすまし攻撃を検出してもアラームを引き起こしません。

説明

ap-impersonation コマンドは AP なりすまし攻撃検出を設定します。

undo ap-impersonation コマンドはデフォルトに戻します。

例

AP なりすまし攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-impersonation quiet 360

7.1.5 apply ap-classification rule

Syntax

apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

undo apply ap-classification rule *rule-id*

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。ID の値の範囲は 1～65535 です。

authorized-ap: 許可された AP として AP 分類ルールに一致する AP を指定します。

external-ap: 外部 AP

misconfigured-ap: 不良コンフィグレーション AP として AP 分類ルールに一致する AP を指定します。

rogue-ap: 不正な AP として AP 分類ルールに一致する AP を指定します。

level: AP 分類ルールに一致する AP に対して重大度レベルを指定します。レベルの範囲は 1～100 です。デフォルトレベルは 50 です。

説明

apply ap-classification rule コマンドは分類ポリシに AP 分類ルールを設定します。

undo apply ap-classification rule コマンドはデフォルトに戻します。

例

分類ポリシ **home** に AP classification rule 1 を設定します。不正な AP として AP classification rule 1 に一致する AP を指定します。重大度レベルを 80 に設定します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] apply ap-classification rule 1 rogue-ap severity-level 80

関連コマンド

ap-classification rule

7.1.6 apply classification policy

Syntax

apply classification policy *policy-name*

undo apply classification policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply classification policy コマンドは分類ポリシを VSD（Virtual Security Domain）に適用します。

undo apply classification policy コマンドは VSD から分類ポリシを削除します。

例

分類ポリシ **policy1** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply classification policy policy1

7.1.7 apply countermeasure policy

Syntax

apply countermeasure policy *policy-name*

undo apply countermeasure policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 対策ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply countermeasure policy コマンドは対策ポリシを VSD（Virtual Security Domain）に適用します。

undo apply countermeasure policy コマンドは VSD から対策ポリシを削除します。

例

対策ポリシ **policy2** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply countermeasure policy policy2

7.1.8 apply detect policy

Syntax

apply detect policy *policy-name*

undo apply detect policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply detect policy コマンドは攻撃検出ポリシを VSD に適用します。

undo apply detect policy コマンドは VSD から攻撃検出ポリシを削除します。

例

攻撃検出ポリシ **policy2** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply detect policy policy2

7.1.9 apply signature policy

Syntax

apply signature policy *policy-name*

undo apply signature policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply signature policy コマンドは署名ポリシを VSD に適用します。

undo apply signature policy コマンドはデフォルトに戻します。

例

署名ポリシ **policy1** を VSD **home** に適用します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain home

[AC-wips-vsd-home] apply signature policy policy1

7.1.10 apply signature rule

Syntax

apply signature rule *rule-id*

undo apply signature rule *rule-id*

デフォルト

設定なし

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で署名を指定します。値の範囲は 1～65535 文字です。

説明

apply signature rule コマンドは署名ポリシに署名を設定します。

undo apply signature rule コマンドはデフォルトに戻します。

例

signature 1 を署名ポリシ **office** に設定します。

<AC> system-view

[AC] wips

[AC-wips] signature policy office

[AC-wips-sig-office] apply signature rule 1

7.1.11 ap-rate-limit

Syntax

ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo ap-rate-limit

デフォルト

学習した AP エントリのための統計値収集間隔：60 秒

遅延時間：1200 秒

AP エントリしきい値：64

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習した AP エントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS が AP エントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: AP エントリ攻撃アラームを引き起こす AP エントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

ap-rate-limit コマンドは AP エントリの学習を制限します。

undo ap-rate-limit コマンドはデフォルトに戻します。

例

AP エントリの学習を制限します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-rate-limit interval 60 quiet 1600 threshold 100

7.1.12 ap-spoofing

Syntax

ap-spoofing [**quiet** *quiet-value*]

undo ap-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP スプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時

間は 600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こしません。

説明

ap-spoofing コマンドは AP スプーフィング攻撃を有効にします。

undo ap-spoofing コマンドは AP スプーフィング攻撃を無効にします。

例

AP スプーフィング検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-spoofing quiet 360

7.1.13 ap-timer

🕮 **メモ：**

inactive-value 引数と aging-value 引数の下限値が Version 7.1.13 を含む以降のソフトウェアから変更されました。

Syntax

ap-timer [**inactive** *inactive-value* **aging** *aging-value*]

undo ap-timer

デフォルト

非アクティブ時間：300 秒

エージングタイマ：600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。指定された非アクティブ時間内に AP がフレームを送受信しない場合、WIPS は AP を非アクティブ状態に設定します。

Version 7.1.13 を含む以降のソフトウェア

inactive-value 引数の値の範囲は 1～1200 秒です。

Version 7.1.11 を含む以前のソフトウェア

inactive-value 引数の値の範囲は 60～1200 秒です。

aging *aging-value*: エージングタイマを指定します。指定されたエージングタイマ内に AP がフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

Version 7.1.13 を含む以降のソフトウェア

aging-value 引数の値の範囲は 1～86400 秒です。

Version 7.1.11 を含む以前のソフトウェア

aging-value 引数の値の範囲は 120～86400 秒です。

説明

ap-timer コマンドは AP エントリタイマを設定します。

undo ap-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-timer inactive 120 aging 360

7.1.14 association-table-overflow

Syntax

association-table-overflow [**quiet** *quiet-value*]

undo association-table-overflow

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がアソシエーション/再アソシエーション DoS 攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にアソシエーション/再アソシエーション DoS 攻撃を検出してもアラームを引き起こしません。

説明

association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を設定します。

undo association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を無効にします。

例

アソシエーション/再アソシエーション DoS 攻撃検出を有効にし、遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] association-table-overflow quiet 100

7.1.15 authentication

Syntax

authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

undo authentication

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定された認証モードと等しい認証モードを整合します。

include: 指定された認証モードを含む認証モードを整合します。

802.1x: 802.1X 認証モードを指定します。

none: 認証モードは指定されません。

other: 802.1X と PSK 以外の認証モードを指定します。

psk: PSK 認証モードを指定します。

説明

authentication コマンドは AP の認証モードを整合するために AP 分類ルールを設定します。

undo authentication コマンドはデフォルトに戻ります。

例

PSK 認証モードを使用する AP を整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] authentication equal psk

7.1.16 block mac-address

Syntax

block mac-address *mac-address*

undo block mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての MAC アドレスを指定します。

説明

block mac-address コマンドはスタティック禁止装置リストに MAC アドレスを追加します。

undo block mac-address コマンドはスタティック禁止装置リストから 1 つもしくはすべての MAC アドレスを削除します。

例

スタティック禁止装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] block mac-address 78AC-C0AF-944F

7.1.17 classification policy

Syntax

classification policy *policy-name*

undo classification policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

classification policy コマンドは分類ポリシを作成し、その view に移行します。

undo classification policy コマンドは分類ポリシを削除します。

例

分類ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home]

7.1.18 client-online

Syntax

client-online *value1* [**to** *value2*]

undo client-online

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP に紐付けられたクライアント数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

client-online コマンドは AP に紐付いたクライアント数を整合するために AP 分類ルールを設定します。

undo client-online コマンドはデフォルトに戻します。

例

20～40 のクライアントに紐付いた AP を整合するために、AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] client-online 20 to 40

7.1.19 client-rate-limit

Syntax

client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo client-rate-limit

デフォルト

学習したクライアントエントリのための統計値収集間隔：60 秒

遅延時間：1200 秒

クライアントエントリしきい値：512

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習したクライアントエントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS がクライアントエントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内にクライアントエントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: クライアントエントリ攻撃アラームを引き起こすクライアントエントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

client-rate-limit コマンドはクライアントエントリの学習を制限します。

undo client-rate-limit コマンドはデフォルトに戻します。

例

クライアントエントリの学習を制限します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-rate-limit interval 80 quiet 1600 threshold 100

7.1.20 client-spoofing

Syntax

client-spoofing [**quiet** *quiet-value*]

undo client-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がクライアントスプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にクライアントスプーフィング攻撃を検出してもアラームを引き起こしません。

説明

client-spoofing コマンドはクライアントスプーフィング攻撃検出を有効にします。

undo client-spoofing コマンドはクライアントスプーフィング攻撃検出を無効にします。

例

クライアントスプーフィング攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-spoofing quiet 360

7.1.21 client-timer

メモ：

inactive-value 引数と aging-value 引数の下限値が Version 7.1.13 を含む以降のソフトウェアから変更されました。

Syntax

client-timer inactive *inactive-value* **aging** *aging-value*

undo client-timer

デフォルト

非アクティブ時間：300 秒

エージングタイマ：600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。指定された非アクティブ時間内にクライアントがフレームを送受信しない場合、WIPS はクライアントを非アクティブ状態に設定します。

Version 7.1.13 を含む以降のソフトウェア

inactive-value 引数の値の範囲は 1～1200 秒です。

Version 7.1.11 を含む以前のソフトウェア

inactive-value 引数の値の範囲は 60～1200 秒です。

aging *aging-value*: エージングタイマを指定します。指定されたエージングタイマ内にクライアントがフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

Version 7.1.13 を含む以降のソフトウェア

aging-value 引数の値の範囲は 1～86400 秒です。

Version 7.1.11 を含む以前のソフトウェア

aging-value 引数の値の範囲は 120～86400 秒です。

説明

client-timer コマンドでクライアントエントリタイマを設定します。

undo client-timer コマンドでデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-timer inactive 120 aging 360

7.1.22 countermeasure adhoc

Syntax

countermeasure adhoc

undo countermeasure adhoc

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure adhoc コマンドはアドホック装置に対策を講じるために WIPS を有効にします。

undo countermeasure adhoc コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure adhoc

7.1.23 countermeasure attack all

Syntax

countermeasure attack all

undo countermeasure attack all

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack all コマンドはすべての攻撃者に対策を講じるために WIPS を有効にします。

undo countermeasure attack all コマンドはデフォルトに戻します。

例

すべての攻撃者に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack all

7.1.24 countermeasure attack deauth-broadcast

Syntax

countermeasure attack deauth-broadcast

undo countermeasure attack deauth-broadcast

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack deauth-broadcast コマンドは認証取り消しアタックをブロードキャストする装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack deauth-broadcast コマンドはデフォルトに戻します。

例

認証取り消しアタックをブロードキャストする装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack deauth-broadcast

7.1.25 countermeasure attack disassoc-broadcast

Syntax

countermeasure attack disassoc-broadcast

undo countermeasure attack disassoc-broadcast

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack disassoc-broadcast コマンドはアソシエーション解除フレームをブロードキャストする装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack disassoc-broadcast コマンドはデフォルトに戻します。

例

#アソシエーション解除フレームをブロードキャストする装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack disassoc-broadcast

7.1.26 countermeasure attack honeypot-ap

Syntax

countermeasure attack honeypot-ap

undo countermeasure attack honeypot-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack honeypot-ap コマンドはハニーポット AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack honeypot-ap コマンドはデフォルトに戻します。

例

ハニーポット AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack honeypot-ap

7.1.27 countermeasure attack hotspot-attack

Syntax

countermeasure attack hotspot-attack

undo countermeasure attack hotspot-attack

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack hotspot-attack コマンドはホットスポット攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack hotspot-attack コマンドはデフォルトに戻します。

例

ホットスポット攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack hotspot-attack

7.1.28 countermeasure attack ht-40-mhz-intolerance

Syntax

countermeasure attack ht-40-mhz-intolerance

undo countermeasure attack ht-40-mhz-intolerance

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack ht-40-mhz-intolerance コマンドは 40MHz 帯域幅モードが無効の装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack ht-40-mhz-intolerance コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack ht-40-mhz-intolerance

7.1.29 countermeasure attack malformed-packet

Syntax

countermeasure attack malformed-packet

undo countermeasure attack malformed-packet

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack malformed-packet コマンドは不正パケットを送信する装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack malformed-packet コマンドはデフォルトに戻します。

例

不正パケットを送信する装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack malformed-packet

7.1.30 countermeasure attack man-in-the-middle

Syntax

countermeasure attack man-in-the-middle

undo countermeasure attack man-in-the-middle

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack man-in-the-middle コマンドは MITM 攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack man-in-the-middle コマンドはデフォルトに戻します。

例

MITM 攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack man-in-the-middle

7.1.31 countermeasure attack omerta

Syntax

countermeasure attack omerta

undo countermeasure attack omerta

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack omerta コマンドは Omerta 攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack omerta コマンドはデフォルトに戻します。

例

Omerta 攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack omerta

7.1.32 countermeasure attack power-save

Syntax

countermeasure attack power-save

undo countermeasure attack power-save

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack power-save コマンドはパワーセーブ攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack power-save コマンドはデフォルトに戻します。

例

パワーセーブ攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack power-save

7.1.33 countermeasure attack soft-ap

Syntax

countermeasure attack soft-ap

undo countermeasure attack soft-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack soft-ap コマンドはソフト AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack soft-ap コマンドはデフォルトに戻します。

例

ソフト AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack soft-ap

7.1.34 countermeasure attack unencrypted-trust-client

Syntax

countermeasure attack unencrypted-trust-client

undo countermeasure attack unencrypted-trust-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack unencrypted-trust-client コマンドは未暗号化のフレームを送信する許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure attack unencrypted-trust-client コマンドはデフォルトに戻します。

例

未暗号化フレームを送信する許可クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack unencrypted-trust-client

7.1.35 countermeasure attack weak-iv

Syntax

countermeasure attack weak-iv

undo countermeasure attack weak-iv

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack weak-iv コマンドは Weak IV を使用する装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack weak-iv コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack weak-iv

7.1.36 countermeasure attack windows-bridge

Syntax

countermeasure attack windows-bridge

undo countermeasure attack windows-bridge

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack windows-bridge コマンドは Windows ブリッジ攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack windows-bridge コマンドはデフォルトに戻します。

例

Windws ブリッジ攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack windows-bridge

7.1.37 countermeasure external-ap

Syntax

countermeasure external-ap

undo countermeasure external-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure external-ap コマンドは外部の AP に対策を講じるために WIPS を有効にします。

undo countermeasure external-ap コマンドはデフォルトに戻します。

例

#外部の AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure external-ap

7.1.38 countermeasure mac-address

Syntax

countermeasure mac-address *mac-address*

undo countermeasure mac-address { *mac-address* | **all** }

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての AP とクライアントを指定します。

説明

countermeasure mac-address コマンドは指定された MAC アドレスを持つ装置に対策を講じるために WIPS を有効にします。

undo countermeasure mac-address コマンドは設定を削除します。

countermeasure mac-address コマンドを複数回設定することで、複数の装置に対策を講じるように WIPS を有効化できます。

例

MAC アドレス **2a11-1fa1-141f** を持つ装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure mac-address 2a11-1fa1-141f

7.1.39 countermeasure misassociation-client

Syntax

countermeasure misassociation-client

undo countermeasure misassociation-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misassociation-client コマンドは間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure misassociation-client コマンドはデフォルトに戻します。

例

間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure misassociation-client

7.1.40 countermeasure misconfigured-ap

Syntax

countermeasure misconfigured-ap

undo countermeasure misconfigured-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misconfigured-ap コマンドは未設定 AP に対策を講じるために WIPS を有効にします。

undo countermeasure misconfigured-ap コマンドはデフォルトに戻します。

例

未設定 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure misconfigured-ap

7.1.41 countermeasure policy

Syntax

countermeasure policy *policy-name*

undo countermeasure policy *policy-name*

Default

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 対策ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

countermeasure policy コマンドは対策ポリシを作成し、その view に移行します。

undo countermeasure policy コマンドは対策ポリシを削除します。

例

対策ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home]

7.1.42 countermeasure potential-authorized-ap

Syntax

countermeasure potential-authorized-ap

undo countermeasure potential-authorized-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-authorized-ap コマンドは潜在的許可 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-authorized-ap コマンドはデフォルトに戻します。

例

潜在的許可 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-authorized-ap

7.1.43 countermeasure potential-external-ap

Syntax

countermeasure potential-external-ap

undo countermeasure potential-external-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-external-ap コマンドは潜在的外部 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-external-ap コマンドはデフォルトに戻します。

例

潜在的外部 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-external-ap

7.1.44 countermeasure potential-rogue-ap

Syntax

countermeasure potential-rogue-ap

undo countermeasure potential-rogue-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-rogue-ap コマンドは潜在的不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-rogue-ap コマンドはデフォルトに戻します。

例

潜在的不正 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-rogue-ap

7.1.45 countermeasure rogue-ap

Syntax

countermeasure rogue-ap

undo countermeasure rogue-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure rogue-ap コマンドは不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure rogue-ap コマンドはデフォルトに戻します。

例

不正 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure rogue-ap

7.1.46 countermeasure unauthorized-client

Syntax

countermeasure unauthorized-client

undo countermeasure unauthorized-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure unauthorized-client コマンドは無許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure unauthorized-client コマンドはデフォルトに戻します。

例

無許可クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure unauthorized-client

7.1.47 countermeasure uncategorized-ap

Syntax

countermeasure uncategorized-ap

undo countermeasure uncategorized-ap

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-ap コマンドは未分類 AP に対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-ap コマンドはデフォルトに戻します。

例

未分類 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure uncategorized-ap

7.1.48 countermeasure uncategorized-client

Syntax

countermeasure uncategorized-client

undo countermeasure uncategorized-client

Default

対策なし

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-client コマンドは未分類クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-client コマンドはデフォルトに戻します。

例

未分類クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure uncategorized-client

7.1.49 deauthentication-broadcast

Syntax

deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo deauthentication-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こすブロードキャスト認証取り消しの数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を設定します。

undo deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] deauthentication-broadcast interval 100 threshold 100 quiet 360

7.1.50 detect policy

Syntax

detect policy *policy-name*

undo detect policy *policy-name*

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

policy-name: 攻撃検出ポリシの名前を指定します。大文字と小文字を区別します。設定範囲は 1～63 文字です。

説明

detect policy コマンドは攻撃検出ポリシを作成し、その view に移行します。

undo detect policy コマンドは攻撃検出ポリシを削除します。

例

攻撃検出ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home]

7.1.51 detect signature

Syntax

detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo detect

デフォルト

有効

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 署名に一致するパケットのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が user-defined 攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内に user-defined 攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: user-defined 攻撃アラームを引き起こす、署名に一致したパケット数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

detect signature コマンドは署名に基づく user-define 攻撃検出を有効にします。

undo detect signature コマンドは署名に基づく user-define 攻撃検出を無効にします。

例

署名に基づく user-define 攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、60、100、360 に設定します。

<AC> system-view

[AC] wips

[AC-wips] signature policy home

[AC-wips-sig-home] detect signature interval 60 threshold 100 quiet 360

7.1.52 disassociation-broadcast

Syntax

disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo disassociation-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こす、ブロードキャスト認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を有効にします。

undo disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] disassociation-broadcast interval 100 threshold 100 quiet 360

7.1.53 detect dissociate-client enable

Syntax

detect dissociate-client enable

undo detect dissociate-client enable

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

detect dissociate-client enable コマンドは関連付けられていないクライアントの検出を有効にします。

undo detect dissociate-client enable コマンドは関連付けられていないクライアントの検出を有効にします。

例

関連付けられていないクライアントの検出を有効にします。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] detect dissociate-client enable

7.1.54 discovered-ap

Syntax

discovered-ap *value1* [**to** *value2*]

undo discovered-ap

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP を検出するセンサの数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 1～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

discovered-ap コマンドは AP を検出するセンサの数を整合するために AP 分類ルールを設定します。

undo discovered-ap コマンドはデフォルトに戻します。

例

10～128 のセンサに検出された AP を整合するために、AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] discovered-ap 10 to 128

7.1.55 display wips sensor

Syntax

display wips sensor

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wips sensor コマンドはすべてのセンサに関する情報を表示します。

例

すべてのセンサに関する情報を表示します。

<AC> display wips sensor

```
Total number of sensors: 1
Sensor ID    Sensor name              VSD name             Radio ID   Status
3            ap1                      aaa                  1          Active
```

表 7-1 コマンド出力

フィールド	説明
VSD name	APが属するVSDの名前

フィールド	説明
Radio ID	WIPSで有効化された無線の名前
Status	センサの状態 ● **Active**－センサはWIPSで有効にされます。 ● **Inactive**－センサはWIPSで有効にされません。

7.1.56 display wips statistics

Syntax

display wips statistics [**receive** | **virtual-security-domain** *vsd-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

receive: すべての VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

virtual-security-domain *vsd-name*: 指定された VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

説明

display wips statistics コマンドはセンサから収集した攻撃検出情報を表示します。

例

すべての VSD のセンサから収集した攻撃検出統計値情報を表示します。

<AC> display wips statistics receive

```
Information from sensor 3
 Information about attack statistics:
   Detected association-request flood messages: 0
   Detected authentication flood messages: 0
   Detected beacon flood messages: 0
   Detected block-ack flood messages: 0
   Detected cts flood messages: 0
   Detected deauthentication flood messages: 0
   Detected disassociation flood messages: 0
   Detected eapol-start flood messages: 0
```

```
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected eapol-logoff flood messages: 0
Detected eap-failure flood messages: 0
Detected eap-success flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected signature rule messages: 0
Detected 40MHZ messages: 0
Detected power save messages: 0
Detected omerta messages: 0
Detected windows bridge messages: 0
Detected soft AP messages: 0
Detected broadcast disassoc messages: 2
Detected broadcast deauth messages: 0
Detected AP impersonate messages: 0
Detected HT greenfield messages: 0
Detected association table overflow messages: 0
Detected wireless bridge messages: 0
```

```
Detected AP flood messages: 11
```

表 7-2 コマンド出力

フィールド	説明
Information from sensor n	センサnから収集した情報。nはセンサのIDをあらわします。
Detected association-request flood messages	紐付け要求フラッドアタック攻撃に対して検出したメッセージの数。
Detected authentication flood messages	認証要求フラッド攻撃に対して検出したメッセージの数。
Detected beacon flood messages	ビーコンフラッド攻撃に対して検出したメッセージの数。
Detected block-ack flood messages	ブロックアクトフラッド攻撃に対して検出したメッセージの数。
Detected cts flood messages	CTSフラッド攻撃に対して検出したメッセージの数。
Detected deauthentication flood messages	認証取り消しフラッド攻撃に対して検出したメッセージの数。
Detected disassociation flood messages	紐付け取り消しフラッド攻撃に対して検出したメッセージの数。
Detected eapol-start flood messages	EAPOLスタートフラッド攻撃に対して検出したメッセージの数。
Detected null-data flood messages	ヌルデータフラッド攻撃に対して検出したメッセージの数。
Detected probe-request flood messages	プローブ要求フラッド攻撃に対して検出したメッセージの数。
Detected reassociation-request flood messages	再紐付け要求フラッド攻撃に対して検出したメッセージの数。
Detected rts flood messages	RTSフラッド攻撃に対して検出したメッセージの数。
Detected eapol-logoff flood messages	EAPOLログオフフラッド攻撃に対して検出したメッセージの数。
Detected eap-failure flood messages	EAPOL失敗フラッド攻撃に対して検出したメッセージの数。
Detected eap-success flood messages	EAPOL成功フラッド攻撃に対して検出したメッセージの数。
Detected duplicated-ie messages	複製されたIEをもつ異常パケットに対して検出したメッセージの数。
Detected fata-jack messages	FATAジャック異常パケットに対して検出したメッセージの数。
Detected illegal-ibss-ess messages	異常なIBSSとESS設定をもつ異常パケットに対して検出したメッセージの数。

フィールド	説明
Detected invalid-address-combination messages	無効な送信元アドレスをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-assoc-req messages	異常な紐付け要求に対して検出したメッセージの数。
Detected invalid-auth messages	異常な認証要求に対して検出したメッセージの数。
Detected invalid-deauth-code messages	無効な認証取り消しコードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-disassoc-code messages	無効な紐付け取り消しコードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-ht-ie messages	異常なHT IEをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-ie-length messages	無効なIE長をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-pkt-length messages	無効なパケット長をもつ異常パケットに対して検出したメッセージの数。
Detected large-duration messages	オーバーサイズの期間をもつ異常パケットに対して検出したメッセージの数。
Detected null-probe-resp messages	異常なプローブ要求フレームに対して検出したメッセージの数。
Detected overflow-eapol-key messages	オーバーサイズのEAPOL鍵をもつ異常パケットに対して検出したメッセージの数。
Detected overflow-ssid messages	オーバーサイズなSSIDをもつ異常パケットに対して検出したメッセージの数。
Detected redundant-ie messages	冗長なIEをもつ異常パケットに対して検出したメッセージの数。
Detected AP spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs AP)
Detected AP spoof client messages	クライアントスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs client)
Detected AP spoof ad-hoc messages	アドホックスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs Ad hoc)
Detected ad-hoc spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(Ad hoc spoofs AP)
Detected client spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(client spoofs AP)
Detected weak IV messages	ウィークIVに対して検出したメッセージの数。
Detected excess AP messages	APエントリ攻撃に対して検出したメッセージの数。

フィールド	説明
Detected excess client messages	クライアントエントリ攻撃に対して検出したメッセージの数。
Detected 40MHZ messages	40Hz帯モードで無効化されるクライアントに対して検出したメッセージの数。
Detected power save messages	電力節約攻撃に対して検出したメッセージの数。
Detected omerta messages	Omerta攻撃に対して検出したメッセージの数。
Detected windows bridge messages	Windowsブリッジに対して検出したメッセージの数。
Detected soft AP messages	ソフトAPに対して検出したメッセージの数。
Detected broadcast disassoc messages	ブロードキャスト紐付け取り消し攻撃に対して検出したメッセージの数。
Detected broadcast deauth messages	ブロードキャスト認証取り消し攻撃に対して検出したメッセージの数。
Detected AP impersonate messages	APなりすまし攻撃に対して検出したメッセージの数。
Detected HT greenfield messages:	HTグリーンフィールドAPの検出メッセージ数
Detected association table overflow messages	アソシエーション/再アソシエーションのDoS攻撃に対する検出メッセージ数
Detected wireless bridge messages	無線ブリッジの検出メッセージ数。
Detected AP flood messages	APフラッドアタックの検出メッセージ数

指定された VSD のセンサから収集された攻撃検出情報を表示します。

<AC> display wips statistics virtual-security-domain 111

```
Information from VSD 111
Information about attack statistics:
  Detected hotspot attack messages: 1
  Detected unencrypted authorized AP messages: 0
  Detected unencrypted trust client messages: 0
  Detected honeypot AP messages: 1
  Detected man in the middle messages: 1
  Detected AP channel change messages: 0
```

表 7-3 コマンド出力

フィールド	説明
Detected hotspot attack messages	ホットスポット攻撃の検出メッセージ数。
Detected unencrypted authorized AP messages	暗号化されていない許可APの検出メッセージ数。
Detected unencrypted trust client messages	暗号化されていない許可クライアントの検出メッセージ数。
Detected honeypot AP messages	ハニーポットAPの検出メッセージ数。
Detected man in the middle messages	MITM攻撃の検出されたメッセージ数
Detected AP channel change messages	チャネル変更のために検出されたメッセージの数。

関連コマンド

reset wips statistics

7.1.57 display wips virtual-security-domain countermeasure record

Syntax

display wips virtual-security-domain *vsd-name* **countermeasure record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

display wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に実行している対策の情報を表示します。

例

VSD **office** で WIPS が対策を実行している不正な装置に関する情報を表示します。

<AC> display wips virtual-security-domain office countermeasure record

```
Total 3 times countermeasure, current 3 countermeasure record in
virtual-security-domain office

Reason: Attack; Ass - associated; Black - blacklist;
       Class - classification; Manu - manual;

MAC address    Type   Reason   Countermeasure AP    Radio ID   Time
1000-0000-00e3 AP     Manu     ap1                  1          2016-05-03/09:32:01
1000-0000-00e4 AP     Manu     ap2                  1          2016-05-03/09:32:11
2000-0000-f282  Client  Black       ap3                                  1
2016-05-03/09:31:56
```

表 7-4 コマンド出力

フィールド	説明
Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain office	成功した対策の数。このフィールドは1024まで表示できます。
MAC Address	WIPSが対策した無線装置のMACアドレス。
Type	無線装置のタイプ：APもしくはクライアント
Reason	WIPSが無線装置に対策した理由。 ● **Attack**－無線装置がアタッカーです。 ● **Ass**－無線装置が関連付いたAPに対して対策します。 ● **Black**－クライアントに対策後にAPに関連付くと、クライアントをブラックリストに追加します。 ● **Class**－装置のタイプに基づいて対策を実施します。 ● **Manu**－MACアドレスに基づいて対策を実施します。
Countermeasure AP	無線装置に対策を実行したセンサの名前。
Radio ID	無線装置に対策を実行したセンサのラジオID。
Time	無線装置に対策を実行した時間。

7.1.58 display wips virtual-security-domain device

Syntax

display wips virtual-security-domain *vsd-name* **device** [**ap** [**ad-hoc** | **authorized** | **external** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue**

| **rogue**] | **client** [[**dissociative-client**] | [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 無線装置の情報を表示します。

ap: AP の情報を表示します。

ad-hoc: アドホックモードで動作する AP に関する情報を表示します。

authorized: 許可 AP に関する情報を表示します。

external: 外部 AP に関する情報を表示します。

misconfigured: 間違って設定された AP に関する情報を表示します。

potential-authorized: 潜在的に許可された AP に関する情報を表示します。

potential-external: 潜在的外部 AP に関する情報を表示します。

potential-rogue: 潜在的な不正 AP に関する情報を表示します。

rogue: 不正な AP に関する情報を表示します。

client: クライアント情報を表示します。

dissociative-client: 紐付けられていないクライアント情報を表示します。

authorized: 許可クライアントに関する情報を表示します。

misassociation: 間違って紐付けられたクライアントに関する情報を表示します。

unauthorized: 未許可クライアントに関する情報を表示します。

uncategorized: 分類されていないクライアントに関する情報を表示します。

mac-address *mac-address*: 特定の無線装置に関する情報を表示します。*mac-address* 引数は無線装置の MAC アドレスを表し、H-H-H 形式です。

verbose: 詳細な装置情報を表示します。

説明

display wips virtual-security-domain device コマンドは VSD で検出された無線装置に関する情報を表示します。

例

VSD **office** で検出された無線装置に関する情報を表示します。

<AC> display wips virtual-security-domain office device

```
Total 200 detected devices in virtual-security-domain office

Class: Auth - authorization; Ext - external; Mis - mistake;
      Unauth - unauthorized; Uncate - uncategorized;
      (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Duration    Sensors Channel Status
1000-0000-0000 AP     Ext(P)   00h 10m 46s 1       11      Active
1000-0000-0001 AP     Ext(P)   00h 10m 46s 1       6       Active
1000-0000-0002 AP     Ext(P)   00h 10m 46s 1       1       Active
```

表 7-5 コマンド出力

フィールド	説明
Type	無線装置タイプ : AP、Client、またはMesh
Class	無線装置のカテゴリ
Duration	無線装置が現在の状態に移行してからの期間
Sensors	無線装置を検出したセンサの数
Channel	直近で無線装置が検出されたチャネル
Status	APもしくはクライアントの状態 • **Active**－APもしくはクライアントはアクティブです。 • **Inactive**－APもしくはクライアントは非アクティブです。

VSD **a** で検出された無線装置に関する詳細な情報を表示します。

<AC> display wips virtual-security-domain a device verbose

```
Total 2 detected devices in virtual-security-domain a

 AP: 1000-0000-0000
   Mesh Neighbor: None
   Classification: Mis(C)
   Severity level: 0
   Classify way: Auto
   Status: Active
   Status duration: 00h 27m 57s
```

```
    Vendor: Not found
    SSID: service
    Radio type: 802.11g
    Countermeasuring: No
    Security: None
    Encryption method: None
    Authentication method: None
    Broadcast SSID: Yes
    QoS supported: No
    Ad-hoc: No
    Beacon interval: 100 TU
    Up duration: 00h 27m 57s
  Channel band-width supported: 20MHZ
    Hotspot AP: No
    Soft AP: No
    Honeypot AP: No
    Total number of reported sensors: 1
      Sensor 1:
        Sensor ID: 3
        Sensor name: 1
        Radio ID: 1
        RSSI: 15
        Channel: 64
        First reported time: 2014-06-03/09:05:51
        Last reported time: 2014-06-03/09:05:51
    Total number of associated clients: 1
      01: 2000-0000-0000
Client: 2000-0000-0000
  Last reported associated AP: 1000-0000-0000
  Classification: Uncate
  Severity level: 0
  Classify way: Auto
  Dissociative status: No
  Status: Active
  Status duration: 00h 00m 02s
  Vendor: Not found
  Radio type: 802.11a
  40mhz intolerance: No
  Countermeasuring: No
  Man in the middle: No
  Total number of reported sensors: 1
    Sensor 1:
      Sensor ID: 2
```

```
Sensor name: 1
Radio ID: 1
RSSI: 50
Channel: 64
First reported time: 2014-06-03/14:52:56
Last reported time: 2014-06-03/14:52:56
Reported associated AP: 1000-0000-0000
```

表 7-6 コマンド出力

フィールド	説明
AP	APのMACアドレス
Mesh Neighbor	メッシュAPのネイバのMACアドレス
Client	クライアントのMACアドレス
Last reported associated AP	クライアントが直近で報告した、紐付けられたAPのMACアドレス

Classification	APもしくはクライアントのカテゴリ
	• APカテゴリオプション
	  • ad_hoc
	  • authorized
	  • rogue
	  • misconfigured
	  • external
	  • potential-authorized
	  • potential-rogue
	  • potential-external
	  • uncategorized
	• クライアントカテゴリオプション
	  • authorized
	  • unauthorized
	  • misassociated
	  • uncategorized

Severity level	装置の重大度レベル

フィールド	説明
Classify way	APもしくはクライアント分類方法 ● **Manual**－手動分類 ● **Invalid OUI**－無効なOUIリストに追加 ● **Block List**－禁止装置リストに追加 ● **Associated**－ACに接続されたAP ● **Trust List**－許可装置リストに追加 ● **User Define**－ユーザが定義した分類 ● **Auto**－自動分類
Dissociative status	クライアントが紐付けられたものではないかどうかをあらわします。
Status	APもしくはクライアントの状態 ● **Active**－APもしくはクライアントはアクティブです。 ● **Inactive**－APもしくはクライアントは非アクティブです。
Status duration	無線装置が現在の状態に移行してからの期間
Vendor	装置のOUI。装置のOUIが、インポートされたOUIと一致する場合、このフィールドは装置のOUIを表示します。装置にOUIが設定されていない場合、あるいは装置のOUIが、インポートされたいずれのOUIとも一致しない場合、このフィールドは**Not found**を表示します。
SSID	APに提供された無線装置のSSID
Radio Type	無線装置の無線モード
40mhz intolerance	クライアントが40MHz帯をサポートするかどうかをあらわします。
Countermeasuring	WIPSが無線装置に対策を講じるかをあらわします。 ● **No** ● **Yes**
Man in the middle	MITM攻撃を検出するかどうかをあらわします。
Security	セキュリティ方式。 ● **None** ● **WEP** ● **WPA** ● **WPA 2**

フィールド	説明
Encryption method	データ暗号方式。 • **TKIP** • **CCMP** • **WEP** • **None**
Authentication method	認証方式。 • **None** • **PSK** • **802.1X** • **Others**－PSK認証と802.1X認証以外の認証方式
Broadcast SSID	APがSSIDをブロードキャストするかどうかをあらわします。APがSSIDをブロードキャストしない場合、このフィールドは何も表示しません。
QoS supported	無線装置がQoSをサポートするかどうかをあらわします。
Ad-hoc	無線装置がアドホックモードかどうかをあらわします。
Beacon interval	TUにおけるビーコン間隔です。1つのTUは1024マイクロ秒に等しいです。
Channel band-width supported	サポートされたチャネル帯域幅モード • 20/40/80MHZ • 20/40MHz • 20MHz
Hotspot AP	APがホットスポット攻撃APであるかどうかをあらわします。
Soft AP	APがソフトAPであるかどうかをあらわします。
Honeypot AP	APがハニーポットAPであるかどうかをあらわします。
Sensor n	無線装置を検出したセンサです。nはシステムに割り当てられたIDをあらわします。
Channel	センサが直近で無線装置を検出したチャネルです。
First reported time	センサが最初に無線装置を検出した時間です。
Last reported time	センサが直近で無線装置を検出した時間です。
n: H-H-H	APに紐付けられたMACアドレスです。nはシステムに割り当てられたIDをあらわします。
Reported associated AP	センサが報告した、紐付けられたAPのMACアドレスです。

関連コマンド

reset wips virtual-security-domain device

7.1.59 display wlan nat-detect

Syntax

display wlan nat-detect [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、検出されたすべての NAT 構成クライアントに関する情報が表示されます。

説明

display wlan nat-detect コマンドは NAT が設定されたクライアントに関する情報を表示します。

例

検出されたすべての NAT 構成クライアントに関する情報を表示します。

<AC> display wlan nat-detect

```
Total 1 detected clients with NAT configured

MAC address    Last report        First report        Duration
0a98-2044-0000 2015-08-24/11:05:23 2015-08-24/10:05:23  01h 15m 00s
```

表 7-7 コマンド出力

フィールド	説明
Total number detected clients with NAT configured	検出されたNAT構成クライアントの数
MAC address	検出されたクライアントのMACアドレス

フィールド	説明
Last report	クライアントが直近に検出された時刻
First report	クライアントが最初に検出された時刻
Duration	クライアントがNAT設定されてからの期間

関連コマンド

reset wlan nat-detect

7.1.60 flood association-request

Syntax

flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood association-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け要求フラッド攻撃アラームを引き起こす紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood association-request コマンドは紐付け要求フラッド攻撃検出を設定します。

undo flood association-request コマンドはデフォルトに戻します。

例

紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood association-request interval 100 threshold 100 quiet 360

7.1.61 flood authentication

Syntax

flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood authentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証要求フラッド攻撃アラームを引き起こす認証要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood authentication コマンドは認証要求フラッド攻撃検出を設定します。

undo flood authentication コマンドはデフォルトに戻します。

例

認証要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood authentication interval 100 threshold 100 quiet 360

7.1.62 flood beacon

Syntax

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood beacon

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ビーコンフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がビーコンフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にビーコンフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ビーコンフラッド攻撃アラームを引き起こすビーコンフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood beacon コマンドはビーコンフラッド攻撃検出を設定します。

undo flood beacon コマンドはデフォルトに戻します。

例

ビーコンフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood beacon interval 100 threshold 100 quiet 360

7.1.63 flood block-ack

Syntax

flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood block-ack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロックアクトフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロックアクトフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にブロックアクトフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロックアクトフラッド攻撃アラームを引き起こすブロックアクトフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood block-ack コマンドはブロックアクトフラッド攻撃検出を設定します。

undo flood block-ack コマンドはデフォルトに戻します。

例

ブロックアクトフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood block-ack interval 100 threshold 100 quiet 360

7.1.64 flood cts

Syntax

flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood cts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: CTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が CTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に CTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: CTS フラッド攻撃アラームを引き起こす CTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood cts コマンドは CTS フラッド攻撃検出を設定します。

undo flood cts コマンドはデフォルトに戻します。

例

CTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood cts interval 100 threshold 100 quiet 360

7.1.65 flood deauthentication

Syntax

flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood deauthentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証取り消しフラッド攻撃アラームを引き起こす認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood deauthentication コマンドは認証取り消しフラッド攻撃検出を設定します。

undo flood deauthentication コマンドはデフォルトに戻します。

例

認証取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood deauthentication interval 100 threshold 100 quiet 360

7.1.66 flood disassociation

Syntax

flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood disassociation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け取り消しフラッド攻撃アラームを引き起こす紐付け取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood disassociation コマンドは紐付け取り消しフラッド攻撃検出を設定します。

undo flood disassociation コマンドはデフォルトに戻します。

例

紐付け取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood disassociation interval 100 threshold 100 quiet 360

7.1.67 flood eap-failure

Syntax

flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-failure

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 失敗フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 失敗フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 失敗フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 失敗フラッド攻撃アラームを引き起こす EAP 失敗フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-failure コマンドは EAP 失敗フラッド攻撃検出を設定します。

undo flood eap-failure コマンドはデフォルトに戻します。

例

EAP 失敗フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eap-failure interval 100 threshold 100 quiet 360

7.1.68 flood eapol-logoff

Syntax

flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-logoff

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL ログオフフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL ログオフフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL ログオフフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL ログオフフラッド攻撃アラームを引き起こす EAPOL ログオフフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-logoff コマンドは EAPOL ログオフフラッド攻撃検出を設定します。

undo flood eapol-logoff コマンドはデフォルトに戻します。

例

EAPOL ログオフフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eapol-logoff interval 100 threshold 100 quiet 360

7.1.69 flood eapol-start

Syntax

flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-start

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL スタートフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL スタートフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL スタートフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL スタートフラッド攻撃アラームを引き起こす EAPOL スタートフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-start コマンドは EAPOL スタートフラッド攻撃検出を設定します。

undo flood eapol-start コマンドはデフォルトに戻します。

例

EAPOL スタートフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eapol-start interval 100 threshold 100 quiet 360

7.1.70 flood eap-success

Syntax

flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-success

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 成功フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 成功フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 成功フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 成功フラッド攻撃アラームを引き起こす EAP 成功フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-success コマンドは EAP 成功フラッド攻撃検出を設定します。

undo flood eap-success コマンドはデフォルトに戻します。

例

EAP 成功フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eap-success interval 100 threshold 100 quiet 360

7.1.71 flood null-data

Syntax

flood null-data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood null-data

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ヌルデータフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がヌルデータフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にヌルデータフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ヌルデータフラッド攻撃アラームを引き起こすヌルデータフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood null-data コマンドはヌルデータフラッド攻撃検出を設定します。

undo flood null-data コマンドはデフォルトに戻します。

例

ヌルデータフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood null-data interval 100 threshold 100 quiet 360

7.1.72 flood probe-request

Syntax

flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood probe-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: プローブ要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がプローブ要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にプローブ要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: プローブ要求フラッド攻撃アラームを引き起こすプローブ要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood probe-request コマンドはプローブ要求フラッド攻撃検出を設定します。

undo flood probe-request コマンドはデフォルトに戻します。

例

プローブ要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood probe-request interval 100 threshold 100 quiet 360

7.1.73 flood reassociation-request

Syntax

flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood reassociation-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 再紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が再紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に再紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 再紐付け要求フラッド攻撃アラームを引き起こす再紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood reassociation-request コマンドは再紐付け要求フラッド攻撃検出を設定します。

undo flood reassociation-request コマンドはデフォルトに戻します。

例

再紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood reassociation-request interval 100 threshold 100 quiet 360

7.1.74 flood rts

Syntax

flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood rts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: RTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が RTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に RTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: RTS フラッド攻撃アラームを引き起こす RTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood rts コマンドは RTS フラッド攻撃検出を設定します。

undo flood rts コマンドはデフォルトに戻します。

例

RTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood rts interval 100 threshold 100 quiet 360

7.1.75 frame-type

Syntax

frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

undo frame-type

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

control: 制御フレームと整合します。

data: データフレームと整合します。

management: 管理フレームと整合します。

frame-subtype: フレームサブタイプを指定します。

association-request: 紐付け要求フレームと整合します。

association-response: 紐付け応答フレームと整合します。

authentication: 認証フレームと整合します。

beacon: ビーコンフレームと整合します。

deauthentication: 認証取り消しフレームと整合します。

disassociation: 紐付け取り消しフレームと整合します。

probe-request: プローブ要求フレームと整合します。

説明

frame-type コマンドはフレームのフレームタイプと整合するためにサブ署名を設定します。

undo frame-type コマンドはデフォルトに戻します。

例

データフレームと一致するように signature 1 に対してサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] frame-type data

7.1.76 honeypot-ap

Syntax

honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

undo honeypot-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

similarity *similarity-value*: ハニーポット AP アラームを引き起こす類似のしきい値を指定します。値の範囲は 70～100%です。デフォルト値は 80%です。AP の SSID と適合 AP の SSID との間の類似点がしきい値に達すると、AP はハニーポット AP とみなされます。

quiet *quiet-value*: WIPS がハニーポット AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット AP を検出してもアラームを引き起こしません。

説明

honeypot-ap コマンドはハニーポット AP 検出を設定します。

undo honeypot-ap コマンドはハニーポット AP 検出を無効にします。

例

ハニーポット AP 検出を有効にします。類似のしきい値と遅延時間をそれぞれ、90%、10 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] honeypot-ap similarity 90 quiet 10

7.1.77 hotspot-attack

Syntax

hotspot-attack [**quiet** *quiet-value*]

undo hotspot-attack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がハニーポット攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット攻撃を検出してもアラームを引き起こしません。

説明

hotspot-attack コマンドはハニーポット攻撃検出を設定します。

undo hotspot-attack コマンドはハニーポット攻撃検出を無効にします。

例

ハニーポット攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] hotspot-attack quiet 100

7.1.78 ht-40mhz-intolerance

Syntax

ht-40mhz-intolerance [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が 40MHz の帯域幅モードを使用禁止にしたクライアントを検出するアラームを開始した後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を設定します。

undo ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を無効にします。

例

40MHz の帯域幅モードを使用禁止にしたクライアント検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ht-40mhz-intolerance quiet 100

7.1.79 ht-greenfield

Syntax

ht-greenfield [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が HT グリーンフィールド AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-greenfield コマンドは HT グリーンフィールド検出を設定します。

undo ht-greenfield コマンドは HT グリーンフィールド検出を無効にします。

例

HT グリーンフィールド AP 検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ht-greenfield quiet 100

7.1.80 ignorelist

Syntax

ignorelist mac-address *mac-address*

undo ignorelist mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを H-H-H 形式で指定します。

all: アラームを無視する装置リスト内のすべてのすべての MAC アドレスを指定します。

説明

ignorelist コマンドはアラームを無視する装置リストに MAC アドレスを追加します。

undo ignorelist コマンドはアラームを無視する装置リストから特定の、もしくはすべての MAC アドレスを削除します。

WIPS は、アラームを無視する装置リスト内の無線装置のみを監視しますが、アラームはあげません。

例

アラームを無視する装置リストに MAC アドレス **2a11-1fa1-1311** を追加します。

<AC> system-view

[AC] wips

[AC-wips] ignorelist mac-address 2a11-1fa1-1311

7.1.81 import hotspot

Syntax

import hotspot *file-name*

undo import hotspot

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import hotspot コマンドはコンフィグレーションファイルからホットスポットをインポートします。

undo import hotspot コマンドはコンフィグレーションファイルを削除します。

1 つのコンフィグレーションファイルからのみホットスポットをインポートできます。

例

コンフィグレーションファイル **hotspot_cfg** からホットスポットをインポートします。

<AC> system-view

[AC] wips

[AC-wips] import hotspot hotspot_cfg

7.1.82 import oui

Syntax

import oui *file-name*

undo import oui

デフォルト

インポートなし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import oui コマンドはコンフィグレーションファイルから OUI をインポートします。

undo import oui コマンドはコンフィグレーションを削除します。

IEEE ウェブサイトからコンフィグレーションファイルをダウンロードできます。

1 つのコンフィグレーションファイルからのみ OUI をインポートできます。

例

コンフィグレーションファイル **oui_import_cfg** から OUI をインポートします。

<AC> system-view

[AC] wips

[AC-wips] import oui oui_import_cfg

関連コマンド

invalid-oui-classify illegal

7.1.83 invalid-oui-classify illegal

Syntax

invalid-oui-classify illegal

undo invalid-oui-classify

デフォルト

無効

View

Classification policy view

定義済みユーザロール

network-admin

説明

invalid-oui-classify illegal コマンドは無効な OUI で装置を不正な装置として分類するように WIPS を有効にします

undo invalid-oui-classify コマンドはデフォルトに戻します。

例

無効な OUI で装置を不正な装置として分類するように WIPS を設定します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] invalid-oui-classify illegal

関連コマンド

import oui

7.1.84 mac-address

Syntax

mac-address { **bssid** | **destination** | **source** } *mac-address*

undo mac-address

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

bssid: 指定された BSSID と整合します。

destination: 指定された送信元 MAC アドレスと整合します。

source: 指定された送信元 MAC アドレスと整合します。

mac-address: MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドはフレームが送信元 MAC アドレスと整合するようにサブ署名を設定します。

undo mac-address コマンドはデフォルトに戻します。

例

フレームが送信元 MAC アドレス **000f-e201-0101** と整合するように signature 1 に対してサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] mac-address source 000f-e201-0101

7.1.85 malformed duplicated-ie

Syntax

malformed duplicated-ie [**quiet** *quiet-value*]

undo malformed duplicated-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が複製された IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に複製された IE を検出してもアラームを引き起こしません。

説明

malformed duplicated-ie コマンドは複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。

undo malformed duplicated-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。複製された IE をパケットが持つ場合、WIPS はパケットを異常とみなします。この検出はベンダに定義された IE には適用できません。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed duplicated-ie quiet 360

7.1.86 malformed fata-jack

Syntax

malformed fata-jack [**quiet** *quiet-value*]

undo malformed fata-jack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が FATA ジャック異常パケットアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に FATA ジャック異常パケットを検出してもアラームを引き起こしません。

説明

malformed fata-jack コマンドは FATA ジャック異常パケットを検出するように、WIPS を有効にします。

undo malformed fata-jack コマンドはデフォルトに戻します。

この機能は認証フレームに適用できます。認証アルゴリズム番号の値が 2 である場合、WIPS は認証フレームを異常とみなします。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed fata-jack quiet 360

7.1.87 malformed illegal-ibss-ess

Syntax

malformed illegal-ibss-ess [**quiet** *quiet-value*]

undo malformed illegal-ibss-ess

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 IBSS および ESS 設定のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 IBSS および ESS 設定を検出してもアラームを引き起こしません。

説明

malformed illegal-ibss-ess コマンドは異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed illegal-ibss-ess コマンドはデフォルトに戻します。

この機能はビーコンフレームおよびプローブ応答フレームに適用できます。IBSS と ESS がフレーム内でともに 1 に設定されている場合、WIPS はフレームを異常とみなします。

例

異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed illegal-ibss-ess quiet 360

7.1.88 malformed invalid-address-combination

Syntax

malformed invalid-address-combination [**quiet** *quiet-value*]

undo malformed invalid-address-combination

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な送信元アドレスのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な送信元アドレスを検出してもアラームを引き起こしません。

説明

malformed invalid-address-combination コマンドは無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-address-combination コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- フレームの TO DS が 1 の場合。（フレームがクライアントにより AP に送信されたことを示します）
- フレームの送信元 MAC アドレスがマルチキャストアドレスもしくはブロードキャストアドレスの場合。

例

無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-address-combination quiet 360

7.1.89 malformed invalid-assoc-req

Syntax

malformed invalid-assoc-req [**quiet** *quiet-value*]

undo malformed invalid-assoc-req

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常紐付け要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常紐付け要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-assoc-req コマンドは異常紐付け要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-assoc-req コマンドはデフォルトに戻します。

この機能は紐付け要求フレームに適用できます。フレーム内の SSID 長が 0 である場合、WIPS はフレームを異常とみなします。

例

異常紐付け要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-assoc-req quiet 360

7.1.90 malformed invalid-auth

Syntax

malformed invalid-auth [**quiet** *quiet-value*]

undo malformed invalid-auth

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常認証要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常認証要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-auth コマンドは異常認証要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-auth コマンドはデフォルトに戻します。

この機能は認証要求フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- 認証アルゴリズム番号が 802.11 プロトコルと一致せず、3 より大きい場合。
- 認証トランザクションシーケンス番号が 1 であり、状態コードが 0 で無い場合。（認証トランザクションシーケンス番号は、クライアントと AP 間の認証処理を示します。）
- 認証トランザクションシーケンス番号が 4 より大きい場合。

例

異常認証要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-auth quiet 360

7.1.91 malformed invalid-deauth-code

Syntax

malformed invalid-deauth-code [**quiet** *quiet-value*]

undo malformed invalid-deauth-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な認証取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な認証取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-deauth-code コマンドは無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-deauth-code コマンドはデフォルトに戻します。

この機能は認証取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-deauth-code quiet 360

7.1.92 malformed invalid-disassoc-code

Syntax

malformed invalid-disassoc-code [**quiet** *quiet-value*]

undo malformed invalid-disassoc-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な紐付け取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な紐付け取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-disassoc-code コマンドは無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-disassoc-code コマンドはデフォルトに戻します。

この機能は紐付け取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-disassoc-code quiet 360

7.1.93 malformed invalid-ht-ie

Syntax

malformed invalid-ht-ie [**quiet** *quiet-value*]

undo malformed invalid-ht-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 HT IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 HT IE を検出してもアラームを引き起こしません。

説明

malformed invalid-ht-ie コマンドは異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ht-ie コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ応答フレーム、紐付け応答フレーム、再紐付け応答フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- HT ケーパビリティ IE の SM 電力節約値が 2 である場合。
- HT オペレーション IE のセカンダリチャネルオフセット値が 2 である場合。

例

異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-ht-ie quiet 360

7.1.94 malformed invalid-ie-length

Syntax

malformed invalid-ie-length [**quiet** *quiet-value*]

undo malformed invalid-ie-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な IE 長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な IE 長を検出してもアラームを引き起こしません。

説明

malformed invalid-ie-length コマンドは無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ie-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE 長が 802.11 プロトコルと一致しない場合、WIPS はフレームを異常とみなします。

例

無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-ie-length quiet 360

7.1.95 malformed invalid-pkt-length

Syntax

malformed invalid-pkt-length [**quiet** *quiet-value*]

undo malformed invalid-pkt-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効なパケット長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効なパケット長を検出してもアラームを引き起こしません。

説明

malformed invalid-pkt-length コマンドは無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-pkt-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。パケットペイロード解析後に IE の残存長が 0 で無い場合、WIPS はフレームを異常とみなします。

例

無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed invalid-pkt-length quiet 360

7.1.96 malformed large-duration

Syntax

malformed large-duration [**quiet** *quiet-value* | **threshold** *value*]

undo malformed large-duration

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな期間のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな期間を検出してもアラームを引き起こしません。

threshold *threshold-value*: WIPS がオーバーサイズな期間を判断し、アラームをあげるために、期間のサイズを指定します。*value* 引数の値の範囲は 1～32767 です。デフォルト値は 5000 です。

説明

malformed large-duration コマンドはオーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed large-duration コマンドはデフォルトに戻します。

この機能はユニキャスト管理フレーム、ユニキャストデータフレーム、RTS フレーム、CTS フレーム、ACK フレームに適用できます。フレーム内の期間の値が指定されたしきい値より大きい場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed large-duration quiet 360

7.1.97 malformed null-probe-resp

Syntax

malformed null-probe-resp [**quiet** *quiet-value*]

undo malformed null-probe-resp

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常プローブ応答フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常プローブ応答フレームを検出してもアラームを引き起こしません。

説明

malformed null-probe-resp コマンドは異常プローブ応答フレームを検出するように、WIPS を有効にします。

undo malformed null-probe-resp コマンドはデフォルトに戻します。

この機能はプローブ応答フレームに適用できます。フレームがメッシュフレームでなく、SSID 長が 0 である場合、WIPS はフレームを異常とみなし、パケットは異常パケットとみなします。

例

異常プローブ応答フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed null-probe-resp quiet 360

7.1.98 malformed overflow-eapol-key

Syntax

malformed overflow-eapol-key [**quiet** *quiet-value*]

undo malformed overflow-eapol-key

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな EAPOL 鍵のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな EAPOL 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-eapol-key コマンドはオーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-eapol-key コマンドはデフォルトに戻します。

この機能は EAPOL 鍵フレームに適用できます。フレーム内の TO DS が 1 で、鍵長が 0 より大きい場合、WIPS はフレームを異常とみなします。悪意ある EAPOL 鍵フレームにより DOS 攻撃を受ける恐れがあります。

例

オーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed overflow-eapol-key quiet 360

7.1.99 malformed overflow-ssid

Syntax

malformed overflow-ssid [**quiet** *quiet-value*]

undo malformed overflow-ssid

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな SSID のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな SSID 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-ssid コマンドはオーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-ssid コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ要求フレーム、プローブ応答フレーム、紐付け要求フレームに適用できます。フレーム内の SSID 長が 32 より大きく、802.11 プロトコルに一致していない場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed overflow-ssid quiet 360

7.1.100 malformed redundant-ie

Syntax

malformed redundant-ie [**quiet** *quiet-value*]

undo malformed redundant-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が冗長な IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に冗長な IE を検出してもアラームを引き起こしません。

説明

malformed redundant-ie コマンドは冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed redundant-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE がフレームにとって必要な IE でも予備の IE でもない場合、WIPS はフレームを異常とみなします。

例

冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] malformed redundant-ie quiet 360

7.1.101 man-in-the-middle

Syntax

man-in-the-middle [**quiet** *quiet-value*]

undo man-in-the-middle

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が MITM（Man-In-The-Middle）攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に MITM 攻撃を検出してもアラームを引き起こしません。

説明

man-in-the-middle コマンドは MITM 攻撃検出を有効にします。

undo man-in-the-middle コマンドは MITM 攻撃検出を無効にします。

MITM 攻撃検出を有効にする前にハニーポット AP 検出を有効にしてください。

例

MITM 攻撃検出を有効にします。

```
<AC> system-view
[AC] wips
[AC-wips] detect policy home
[AC-wips-dtc-home] honeypot-ap
[AC-wips-dtc-home] man-in-the-middle
```

7.1.102 manual-classify mac-address

Syntax

manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

undo manual-classify mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

authorized-ap: AP を許可された AP として指定します。

external-ap: AP を外部 AP として指定します。

misconfigured-ap: AP を間違って設定された AP として指定します。

rogue-ap: AP を不正な AP として指定します。

all: すべての AP を指定します。

説明

manual-classify mac-address コマンドは AP に対してカテゴリを設定します。

undo manual-classify mac-address コマンドはデフォルトに戻します。

例

MAC アドレスが 000f-00e2-0001 の AP を許可された AP として設定します。

```
<AC> system-view
[AC] wips
```

[AC-wips] classification policy home

[AC-wips-cls-home] manual-classify mac-address 000f-00e2-0001 authorized-ap

7.1.103 omerta

Syntax

omerta [**quiet** *quiet-value*]

undo omerta

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Omerta 攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に Omerta 攻撃を検出してもアラームを引き起こしません。

説明

omerta コマンドは Omerta 攻撃検出を有効にします。

undo omerta コマンドは Omerta 攻撃検出を無効にします。

例

Omerta 攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] omerta quiet 100

7.1.104 oui

Syntax

oui *oui-info*

undo oui

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

oui-info: OUI 情報を XXXXXX 形式で指定します。大文字と小文字を区別しません。16 進数で指定します。

説明

oui コマンドは AP の OUI 情報と整合するように AP 分類ルールを設定します。

undo oui コマンドはデフォルトに戻します。

例

AP を OUI **000fe4** と整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] oui 000fe4

7.1.105 pattern

Syntax

pattern *pattern-number* **offset** *offset-value* **mask** *mask value1* [**to** *value2*] [**from-payload**]

undo pattern { *pattern-number* | **all** }

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

pattern-number: 0～65535 の範囲の数字で指定されたフレームのビットと一致するサブ署名を指定します。

offset *offset-value*: 指定されたビットから参照ビットまでのオフセットを指定します。*offset-value* 引数の値の範囲は 0～2346 ビットです。参照ビットは、フレームヘッド（デフォルト）もしくはフレームペイロードの最初のビットになることができます。

mask *mask*: 指定されたビットで AND 演算に使用される 2 バイトマスクを指定します。マスクは 16 進数形式です。マスクの値の範囲は 0～ffff です。

value1 [**to** *value2*]: ビット数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～65535 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

from-payload: 参照ビットとしてフレームペイロードの最初のビットを指定します。このキーワードを指定しない場合、フレームヘッドの最初のビットは参照ビットになります。

説明

pattern コマンドは指定されたフレームのビットと整合するようにサブ署名を設定します。

undo pattern コマンドはデフォルトに戻します。

例

フレームヘッドの第 2 ビットと第 3 ビットが整合するようにサブ署名を設定します。フレームの第 2 ビットと第 3 ビットの値が 0x0015～0x0020 の範囲内の場合、フレームはサブ署名と整合します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] pattern 1 offset 8 mask ffff 15 to 20

7.1.106 permit-channel

Syntax

permit-channel *channel-id-list*

undo permit-channel { *channel-id-list* | **all** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

channel-id-list: 許可された 10 個までのチャネルアイテムの空間分離リストを指定します。各アイテムは、*value1* **to** *value2* の形式でチャネル番号もしくはチャネル番号の範囲を指定します。チャネル番号の範囲は 1～224 です。*value2* 引数の値は *value1* 引数の値以上でなければなりません。

all: 許可されたすべてのチャネルを指定します。

説明

permit-channel コマンドは許可されたチャネルリストに 1 つあるいは複数のチャネルを追加します。

undo permit-channel コマンドは許可されたチャネルリストから指定されたチャネルあるいはすべてのチャネルを削除します。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、このコマンドを使用して許可されたチャネルリストを設定します。

例

チャネル 1 を許可されたチャネルリストに追加します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] permit-channel 1

関連コマンド

prohibited-channel

7.1.107 power-save

Syntax

power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

undo power-save

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: パワーセーブフレームのための統計値収集間隔を指定します。*interval-value* 引数の値は 1～3600 秒です。デフォルト値は 10 秒です。

minoffpacket *packet-value*: パワーセーブ攻撃分析を引き起こすパワーセーブ off フレームの数のしきい値を指定します。クライアントからの off フレームの数がしきい値の達すると、WIPS はパワーセーブ攻撃が発生したかどうか判断するために、パワーセーブフレームを分析します。値の範囲は 10～150 です。デフォルト値は 50 です。

onoffpercent *percent-value*: クライアントからのパワーセーブ on フレームと off フレームの比率のしきい値を指定します。しきい値に達すると WIPS はパワーセーブ攻撃のアラームを引き起こします。値の範囲は 0～100 です。デフォルト値は 80 です。

quiet *quiet-value*: WIPS がパワーセーブ攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にパワーセーブ攻撃を検出してもアラームを引き起こしません。

説明

power-save コマンドはパワーセーブ攻撃検出を有効にします。

undo power-save コマンドはパワーセーブ攻撃検出を無効にします。

例

パワーセーブ攻撃検出を有効にします。*interval-value*、*packet-value*、*percent-value*、*quiet-value* の値をそれぞれ、20、20、90、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] power-save interval 20 minoffpacket 20 onoffpercent 90 quiet 100

7.1.108 prohibited-channel

Syntax

prohibited-channel [**quiet** *quiet-value*]

undo prohibited-channel

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が禁止されたチャネルのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に禁止されたチャネルを検出してもアラームを引き起こしません。

説明

prohibited-channel コマンドは禁止されたチャネル検出を有効にします。

undo prohibited-channel コマンドは禁止されたチャネル検出を無効にします。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、**permit-channel** コマンドを使用して許可されたチャネルリストを設定します。

例

禁止されたチャネル検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] prohibited-channel quiet 100

関連コマンド

permit-channel

7.1.109 report-interval

Syntax

report-interval *interval*

undo report-interval

デフォルト

30000 ミリ秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval: センサが AC に検出した装置の情報を通知する間隔を指定します。設定範囲は 1000～300000 ミリ秒です。

説明

report-interval コマンドはセンサが AC に検出した装置の情報を通知する間隔を設定します。

undo report-interval コマンドはデフォルトに戻します。

例

センサが AC に検出した装置の情報を通知する間隔を 10000 ミリ秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] report-interval 10000

7.1.110 reset wips statistics

Syntax

reset wips statistics

View

User view

定義済みユーザロール

network-admin

説明

reset wips statistics コマンドはすべてのセンサから収集した情報を削除します。

例

すべてのセンサから収集した情報を消去します。

<AC> reset wips statistics

関連コマンド

display wips statistics receive

7.1.111 reset wips virtual-security-domain

Syntax

reset wips virtual-security-domain *vsd-name* **device** { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 装置のエントリを消去します。

ap: AP のエントリを消去します。

all: すべての AP のエントリを消去します。

mac-address *mac-address*: AP のエントリを消去します。*mac-address* 引数は AP の MAC アドレスをあらわします。

client: クライアントのエントリを消去します。

all: すべてのクライアントのエントリを消去します。

mac-address *mac-address*: クライアントのエントリを消去します。*mac-address* 引数はクライアントの MAC アドレスをあらわします。

all: すべての AP とクライアントのエントリを消去します。

説明

reset wips virtual-security-domain コマンドは VSD にある学習した AP もしくはクライアントのエントリを削除します。

例

VSD **aaa** にある学習した AP とクライアントのエントリを消去します。

<AC> reset wips virtual-security-domain aaa device all

関連コマンド

display wips virtual-security-domain device

7.1.112 reset wips virtual-security-domain countermeasure record

Syntax

reset wips virtual-security-domain *vsd-name* **countermeasure record**

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

reset wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に対して講じた対策に関する情報を削除します。

例

VSD **aaa** のために WIPS が不正な装置に対して講じた対策に関する情報を消去します。

<AC> reset wips virtual-security-domain aaa countermeasure record

関連コマンド

display wips virtual-security-domain countermeasure record

7.1.113 reset wlan nat-detect

Syntax

reset wlan nat-detect

View

User view

定義済みユーザロール

network-admin

network-operator

説明

reset wlan nat-detect コマンドは NAT を設定したクライアントに関する情報を消去します。

例

NAT を構成したクライアントに関する情報をクリアします。

<AC> reset wlan nat-detect

関連コマンド

display wlan nat-detect

7.1.114 rssi

Syntax

rssi *value1* [**to** *value2*]

undo rssi

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の RSSI の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、

どちらも 0～100 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

rssi コマンドで、AP の RSSI と整合するように AP 分類ルールを設定します。

undo rssi コマンドでデフォルトに戻します。

例

AP が 20～40 の RSSI と整合するように AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] rssi 20 to 40

7.1.115 rssi-change-threshold

Syntax

rssi-change-threshold *threshold-value*

undo rssi-change-threshold

デフォルト

20

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

threshold-value: 装置検出の RSSI 相違のしきい値を指定します。設定範囲は 1～100 です。

説明

rssi-change-threshold コマンドは装置検出の RSSI 相違のしきい値を設定します。

undo rssi-change-threshold コマンドはデフォルトに戻します。

例

装置検出の RSSI 相違のしきい値を 80 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] rssi-change-threshold 80

7.1.116 rssi-threshold

Syntax

rssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

undo rssi-threshold { **ap** | **client** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

ap *ap-rssi-value*: AP の RSSI しきい値を指定します。設定範囲は 1～100 です。

client *client-rssi-value*: クライアントの RSSI しきい値を指定します。設定範囲は 1～100 です。

説明

rssi-threshold コマンドは装置検出の RSSI しきい値を設定します。

undo rssi-threshold コマンドはデフォルトに戻します。

例

信号強度が 80 を超過している AP を検出するために WIPS を設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] rssi-threshold ap 80

7.1.117 security

Syntax

security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

undo security

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定されたセキュリティモードと等しいセキュリティモードと整合します。

include: 指定されたセキュリティモードを含むセキュリティモードと整合します。

clear: 消去するセキュリティモードを指定します。

wep: WEP セキュリティモードを指定します。

wpa: WPA セキュリティモードを指定します。

wpa2: WPA 2 セキュリティモードを指定します。

説明

security コマンドは AP に使用されるセキュリティモードと整合するように AP 分類ルールを設定します。

undo security コマンドはデフォルトに戻します。

例

WEP セキュリティモードを使用する AP と整合するように AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] security equal wep

7.1.118 select sensor all

Syntax

select sensor all

undo select sensor all

デフォルト

直近で攻撃者を検出したセンサのみ、その攻撃者に対して対策を講じます。

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

select sensor all コマンドは攻撃者を検出するすべてのセンサを有効にします。

undo select sensor all コマンドは設定を削除します。

例

攻撃者に対して対策を講じるために、攻撃者を検出するすべてのセンサを有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-ctm-home] select sensor all

7.1.119 seq-number

Syntax

seq-number *seq-value1* [**to** *seq-value2*]

undo seq-number

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

seq-value1 [**to** *seq-value2*]: フレームのシーケンス番号の範囲を指定します。*seq-value1* 引数と *seq-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*seq-value1* 引数と *seq-value2* 引数の値の範囲は、どちらも 0～4095 です。ただし、*seq-value2* 引数の値は *seq-value1* 引数の値より大きくなければなりません。

説明

seq-number コマンドはシーケンス番号をもつフレームと整合するサブ署名を設定します。

undo seq-number コマンドはデフォルトに戻します。

例

シーケンス番号 100 をもつフレームと整合するサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] seq-number 100

7.1.120 signature policy

Syntax

signature policy *policy-name*

undo signature policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 署名ポリシの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

signature policy コマンドは署名ポリシを作成し、その view に移行します。指定された署名ポリシがすでに存在する場合、signature policy view に移行します。

undo signature policy コマンドは署名ポリシを削除します。

例

署名ポリシ **home** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] signature policy home

7.1.121 signature rule

Syntax

signature rule *rule-id*

undo signature rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: 署名の ID を指定します。範囲は 1～65535 です。

説明

signature rule コマンドは署名を作成し、その view に移行します。指定された署名がすでに存在する場合、signature view に移行します。

undo signature rule コマンドは署名を削除します。

例

signature 1 を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

7.1.122 soft-ap

Syntax

soft-ap [**convert-time** *time-value*]

undo soft-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

convert-time *time-value*: ソフト AP がクライアントと AP の役割を切り替える間隔を指定します。*time-value* 引数の値の範囲は 5～600 秒です。デフォルト値は 10 秒です。

説明

soft-ap コマンドはソフト AP 検出を有効にします。

undo soft-ap コマンドはソフト AP 検出を無効にします。

例

ソフト AP 検出を有効にします。*time-value* 引数の値を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] soft-ap convert-time 100

7.1.123 ssid (AP classification rule view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

undo ssid

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

ssid-string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドは AP に対して無線装置の SSID を整合するように AP 分類ルールを設定します。

undo ssid コマンドはデフォルトに戻します。

例

SSID **abc** の無線サービスを使用した AP を整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] ssid equal abc

7.1.124 ssid (signature view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *string*

undo ssid

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドはフレームの SSID を整合するためにサブ署名を設定します。

undo ssid コマンドはデフォルトに戻します。

例

signature 1 に対して SSID **office** のフレームを整合するためにサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-rule-1] ssid equal office

7.1.125 ssid-length

Syntax

ssid-length *length-value1* [**to** *length-value2*]

undo ssid-length

デフォルト

設定なし

View

Signature rule

定義済みユーザロール

network-admin

パラメータ

length-value1 [**to** *length-value2*]: SSID 長の値の範囲を指定します。*length-value1* 引数と *length-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*length-value1* 引数と *length-value2* 引数の値の範囲は、どちらも 1～32 です。ただし、*length-value2* 引数の値は *length-value1* 引数の値より大きくなければなりません。

説明

ssid-length コマンドはフレームの SSID 長を整合するためにサブ署名を設定します。

undo ssid-length コマンドはデフォルトに戻します。

例

SSID 長が 10 のフレームを整合するためにサブ署名を設定します。

<AC> system-view

[AC] wips

[AC-wips] signature rule 1

[AC-wips-sig-1] ssid-length 10

7.1.126 trust mac-address

Syntax

trust mac-address *mac-address*

undo trust mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを指定します。

all: すべての MAC アドレスを指定します。

説明

trust mac-address コマンドは許可された装置リストに AP もしくはクライアントの MAC アドレスを追加します。

undo trust mac-address コマンドは許可された装置リストから 1 つあるいはすべての MAC アドレスを削除します。

例

許可された装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] trust mac-address 78AC-C0AF-944F

7.1.127 trust oui

Syntax

trust oui *oui*

undo trust oui { *oui* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

oui: OUI の名前を指定します。大文字と小文字を区別しません。文字数は 6 文字です。

all: すべての OUI を指定します。

説明

trust oui コマンドは信頼された OUI リストに OUI を追加します。

undo trust oui コマンドは信頼された OUI リストから 1 つあるいはすべての OUI を削除します。

例

信頼された OUI リストに OUI **000fe4** と **000fe5** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] trust oui 000fe4

[AC-wips-cls-home] trust oui 000fe5

7.1.128 trust ssid

Syntax

trust ssid *ssid-name*

undo trust ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID の名前を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

all: すべての SSID を指定します。

説明

trust ssid コマンドは信頼された SSID リストに SSID を追加します。

undo trust ssid コマンドは信頼された SSID リストから 1 つあるいはすべての SSID を削除します。

例

信頼された SSID リストに SSID **flood1** を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] trust ssid flood1

7.1.129 unencrypted-authorized-ap

Syntax

unencrypted-authorized-ap [**quiet** *quiet-value*]

undo unencrypted-authorized-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可 AP を検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可 AP を検出してもアラームを引き起こしません。

説明

unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を有効にします。

undo unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を無効にします。

例

暗号化されていない許可 AP 検出を有効にします。遅延時間を 10 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] unencrypted-authorized-ap quiet 10

7.1.130 unencrypted-trust-client

Syntax

unencrypted-trust-client [**quiet** *quiet-value*]

undo unencrypted-trust-client

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可クライアントを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可クライアントを検出してもアラームを引き起こしません。

説明

unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を有効にします。

undo unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を無効にします。

例

暗号化されていない許可クライアント検出を有効にします。遅延時間を 10 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] unencrypted-trust-client quiet 10

7.1.131 up-duration

Syntax

up-duration *value1* [**to** *value2*]

undo up-duration

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の動作時間の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～2592000 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

up-duration コマンドは AP の動作時間と整合するように AP 分類ルールを設定します。

undo up-duration コマンドはデフォルトに戻します。

例

2000～40000 秒の動作時間の AP と整合するように AP 分類ルールを設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] up-duration 2000 to 40000

7.1.132 virtual-security-domain

Syntax

virtual-security-domain *vsd-name*

undo virtual-security-domain *vsd-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

virtual-security-domain コマンドは VSD を作成し、その view に移行します。

undo virtual-security-domain コマンドは VSD を削除します。

例

VSD **office** を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] virtual-security-domain office

[AC-wips-vsd-office]

7.1.133 weak-iv

Syntax

weak-iv [**quiet** *quiet-value*]

undo weak-iv

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がウィーク IV のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にウィーク IV を検出してもアラームを引き起こしません。

説明

weak-iv コマンドはウィーク IV 検出を有効にします。

undo weak-iv コマンドはデフォルトに戻します。

例

ウィーク IV 検出を有効にします。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] weak-iv

7.1.134 windows-bridge

Syntax

windows-bridge [**quiet** *quiet-value*]

undo windows-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Windows ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に Windows ブリッジを検出してもアラームを引き起こしません。

説明

windows-bridge コマンドは Windows ブリッジ検出を有効にします。

undo windows-bridge コマンドは Windows ブリッジを無効にします。

例

Windows ブリッジ検出を有効にします。遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] windows-bridge quiet 360

7.1.135 wips

Syntax

wips

undo wips

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

説明

wips コマンドは WIPS view に移行します。

undo wips コマンドは WIPS view 内の設定をすべて削除します。

例

WIPS view に移行します。

<AC> system-view

[AC] wips

[AC-wips]

7.1.136 wips enable

Syntax

wips enable

undo wips enable

デフォルト

Radio view では、無線が AP group radio view で設定を使用します。

AP group radio view では、WIPS は無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

wips enable コマンドは WIPS を有効にし、Radio を WISP センサにします。

undo wips enable コマンドはデフォルトに戻します。

無線通信と WIPS センサは同じ Radio 上での併用をサポートしています。

無線通信と WIPS センサを併用している Radio の WIPS スキャンは、通信への影響を与えないために、端末との通信のないタイミングで行われます。

また、無線通信と WIPS センサが有効な Radio に対する通信、および端末の接続に対しては、通信を優先するため WIPS 検出はできません。

例

AP **ap1** の無線 1 に対して WIPS を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] wips enable

AP group **apgroup1** のモデル **QX-W1020** を持つ AP の無線 1 に対して WIPS を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] wips enable

7.1.137 wips virtual-security-domain

Syntax

wips virtual-security-domain *vsd-name*

undo wips virtual-security-domain

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP グループは VSD に追加されません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

wips virtual-security-domain コマンドは AP を VSD に追加します。

undo wips virtual-security-domain コマンドは AP を VSD から削除します。

例

VSD **office** に AP を追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] wips virtual-security-domain office

AP group **apgroup1** を VSD **office** に追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] wips virtual-security-domain office

7.1.138 wireless-bridge

Syntax

wireless-bridge [**quiet** *quiet-value*]

undo wireless-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無線ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に無線ブリッジを検出してもアラームを引き起こしません。

説明

wireless-bridge コマンドは無線ブリッジ検出を有効にします。

undo wireless-bridge コマンドは無線ブリッジを無効にします。

例

無線ブリッジ検出を有効にします。遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] wireless-bridge quiet 100

7.1.139 wlan nat-detect

Syntax

wlan nat-detect { **disable** | **enable** }

undo wlan nat-detect

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、NAT を設定したクライアントの検出は無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: NAT が設定されているクライアントの検出を無効にします。

enable: NAT が設定されているクライアントの検出を有効にします。

説明

wlan nat-detect enable コマンドは NAT を設定したクライアント検出を有効にします。

wlan nat-detect disable コマンドは NAT を設定したクライアント検出を無効にします。

undo wlan nat-detect コマンドはデフォルトに戻します。

装置は、NAT で設定されたクライアントを検出するとアラームを生成します。検出された NAT 設定クライアントに関する情報を表示するには、**display wlan nat-detect** コマンドを使用します。

例

AP **ap1** 用に NAT が設定されているクライアントの検出を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] wlan nat-detect enable

AP group **aaa** の AP 用に NAT が設定されているクライアントの検出を有効にします。

<AC> system-view

[AC] wlan ap-group aaa

[AC-wlan-ap-group-aaa] wlan nat-detect enable

目次

8 章 WLAN QoS の設定 8-1
8.1 WLAN QoS の設定コマンド 8-1
8.1.1 atf 8-1
8.1.2 bandwidth-guarantee 8-2
8.1.3 bandwidth-guarantee service-template 8-4
8.1.4 cac policy 8-5
8.1.5 client-rate-limit (radio view/AP group radio view) 8-7
8.1.6 client-rate-limit (service template view) 8-8
8.1.7 display wlan wmm 8-9
8.1.8 edca client (ac-be | ac-bk) 8-13
8.1.9 edca client (ac-vi | ac-vo) 8-14
8.1.10 edca radio 8-16
8.1.11 mu-edca client 8-18
8.1.12 qos priority 8-20
8.1.13 qos trust 8-21
8.1.14 reset wlan wmm 8-21
8.1.15 svp map-ac 8-22
8.1.16 u-apsd enable 8-23
8.1.17 wlan client-rate-limit 8-24
8.1.18 wlan max-bandwidth 8-26
8.1.19 wmm 8-27

8章 WLAN QoS の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

8.1 WLAN QoSの設定コマンド

8.1.1 atf

🕮 メモ：

atf コマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。
atf コマンドは QX-W1100 シリーズの AP でのみサポートしています。

Syntax

atf { **disable** | **enable** }

undo atf

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view では、Air Time Fairness は無効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: Air Time Fairness を無効にします。

enable: Air Time Fairness を有効にします。

説明

atf enable コマンドは Air Time Fairness を有効にします。

atf disable コマンドは Air Time Fairness を無効にします。

undo atf コマンドはデフォルトに戻します。

このコマンドを使用すると、高速クライアントでワイヤレスリソースを使用する機会が増えます。これにより、ネットワーク全体の転送効率が向上しますが、低速クライアントの転送効率が低下する可能性があります。

この機能を設定する場合は、アクセスクライアントの数と高速クライアントの転送効率を考慮してください。

この機能でネットワークの転送効率が向上するのは、AP からクライアント方向の通信のみです。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** の Radio 1 で Air Time Fairness を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] atf enable

AP group **apgroup1** の AP の Radio1 で Air Time Fairness を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] atf enable

8.1.2 bandwidth-guarantee

Syntax

bandwidth-guarantee { **disable** | **enable** }

undo bandwidth-guarantee

デフォルト

radio view は以下の通りです。

- AP group view のサービステンプレート設定が使用されている場合、AP は AP group view 内の設定を使用します。
- サービステンプレートが手動で無線に紐づけられている場合、帯域幅保証は無効になります。

AP group radio view では、帯域幅保証は無効です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 帯域保証を無効にします。

enable: 帯域保証を有効にします。

説明

bandwidth-guarantee enable コマンドは帯域保証を有効にします。

bandwidth-guarantee disable コマンドは帯域保証を無効にします。

undo bandwidth-guarantee コマンドはデフォルトに戻します。

このコマンドを使用すると、ネットワークが輻輳しているときに、同じ無線に関連付けられたクライアントが保証帯域幅を取得できるようになります。保証帯域幅を設定するには、**bandwidth-guarantee service-template** コマンドを使用します。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP **ap1** の帯域保証を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] service-template 1

[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee enable

AP group **apgroup1** の帯域保証を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] bandwidth-guarantee enable

関連コマンド

bandwidth-guarantee service-template

8.1.3 bandwidth-guarantee service-template

Syntax

bandwidth-guarantee service-template *service-template-name* **percent** *percent*

undo bandwidth-guarantee { **all** | **service-template** *service-template-name* }

デフォルト

radio view は以下の通りです。

- AP group view のサービステンプレート設定が使用されている場合、AP は AP group view 内の設定を使用します。
- サービステンプレートが手動で無線に紐づけられている場合、サービステンプレートに保証された帯域幅の割合は設定されません。

AP group radio view では、サービステンプレートに保証帯域幅の割合が設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。大文字と小文字を区別しない 1～63 文字です。指定したサービステンプレートが無線に紐づけられていることを確認してください。

percent *percent*: 総帯域幅に対する保証帯域幅の割合を指定します。*percent* 引数の値の範囲は 1～100 です。合計帯域幅は、無線の最大帯域幅を示します。保証帯域幅は、サービステンプレートに対応する BSS の最小帯域幅を示します。

all: すべてのサービステンプレートを指定します。

説明

bandwidth-guarantee service-template コマンドは指定されたサービステンプレートの保証帯域幅の割合を設定します。

undo bandwidth-guarantee service-template コマンドは指定されたサービステンプレートの保証帯域幅設定をキャンセルします。

このコマンドを有効にするには、帯域保証機能が有効になっていることを確認してください。

同じ無線に紐づけられているすべてのサービステンプレートで、保証帯域幅の合計が100%を超えることはできません。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

radio view でサービステンプレート 1 の保証帯域幅の割合を 30%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] service-template 1

[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee service-template 1 percent 30

[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee enable

AP group radio view で、サービステンプレート 1 の保証帯域幅の割合を 30%に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] bandwidth-guarantee enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] service-template 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] bandwidth-guarantee service-template 1 percent 30

関連コマンド

- **bandwidth-guarantee enable**
- **wlan mac-bandwidth**

8.1.4 cac policy

Syntax

cac policy { **channelutilization** [*channelutilization-value*] | **client** [*client-number*] }

undo cac policy

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view では、クライアントベースのアドミッションポリシが使用され、許可されるクライアントの最大数は 20 です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channelutilization: チャネル使用率に基づくアドミッションポリシを指定します。

channelutilization-value: 最大チャネル使用率を 0～100%の範囲で指定します。最大チャネル使用率は、一定の時間内に受信された AC-VO および AC-VI トラフィックの有効時間に対する中間時間を参照します。有効時間とは、データの送受信に使用可能な時間を指します。デフォルトでは、最大チャネル使用率は 65%です。

client: クライアントベースのアドミッションポリシを指定します。

client-number: 接続できるクライアントの最大数を 0～64 の範囲で指定します。クライアントは、AC-VO および AC-VI の両方のキューを使用している場合、1 つのクライアントとしてカウントされます。

説明

cac policy コマンドは Connect Admission Control（CAC）ポリシを設定します。

undo cac policy コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

CAC ポリシは、AC-VO キューおよび AC-VI キューでのみ有効です。

例

CAC のチャネル使用率に基づくアドミッションポリシを設定し、最大チャネル使用率を 70%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] cac policy channelutilization 70

CAC のチャネル使用に基づくアドミッションポリシを設定し、AP group **apgroup1** の最大チャネル使用率を 70%に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] cac policy channelutilization 70

8.1.5 client-rate-limit (radio view/AP group radio view)

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*

undo client-rate-limit { **inbound** | **outbound** }

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、無線ベースのクライアントレート制限は設定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

dynamic: 動的レート制限モードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

static: 静的レート制限モードを指定します。各クライアントの最大レートは固定です。

cir *cir*: CIR を Kbps で指定します。*cir* 引数の値は 16～1700000 の範囲です。このオプションは、静的レート制限モードの場合は各クライアントの最大レートを設定し、動的レート制限モードの場合はすべてのクライアントの最大レートを設定します。

説明

client-rate-limit コマンドは無線ベースのクライアントレート制限を設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドを有効にするには、無線ベースのクライアントレート制限が有効になっていることを確認します。

このコマンドを複数回繰り返して、受信トラフィックと送信トラフィックの両方のレートを制限できます。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

radio view で無線 1 のクライアントレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定し、すべてのクライアントの送信トラフィックに対して CIR を 89 Kbps に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-1] client-rate-limit inbound mode static cir 567

[AC-wlan-ap-ap1-1] client-rate-limit outbound mode dynamic cir 89

AP group radio view で無線 1 のクライアントレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定し、すべてのクライアントの送信トラフィックに対して CIR を 89 Kbps に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client-rate-limit inbound mode static cir 567

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client-rate-limit outbound mode dynamic cir 89

8.1.6 client-rate-limit (service template view)

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*

undo client-rate-limit { **inbound** | **outbound** }

デフォルト

サービステンプレートベースのクライアントレート制限は設定されていません。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

dynamic: 動的レート制限モードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

static: 静的レート制限モードを指定します。各クライアントの最大レートは固定です。

cir *cir*: CIR を Kbps で指定します。cir 引数の値は 16～1700000 の範囲です。このオプションは、静的レート制限モードの場合は各クライアントの最大レートを設定し、動的レート制限モードの場合はすべてのクライアントの最大レートを設定します。

説明

client-rate-limit コマンドはサービステンプレートベースのクライアントレート制限を設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドを有効にするには、サービステンプレートベースのクライアントレート制限が有効になっていることを確認します。

このコマンドを複数回繰り返して、受信トラフィックと送信トラフィックの両方のレートを制限できます。

例

サービステンプレート 1 のレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] client-rate-limit inbound mode static cir 567

8.1.7 display wlan wmm

Syntax

display wlan wmm { **radio** { **all** | **ap** *ap-name* } | **client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* } }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての無線またはすべてのクライアントを指定します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

説明

display wlan wmm radio コマンドは無線の WMM 統計情報を表示します。

display wlan wmm client コマンドはクライアントの WMM 統計情報を表示します。

例

AP **test** の無線の WMM 統計情報を表示します。

<AC> display wlan wmm radio ap test

```
AP ID : 4   AP name : test

Radio : 1
Client EDCA updates : 0
QoS mode  : WMM
WMM status : Enabled
Radio max AIFSN    : 15              Radio max ECWmin : 10
Radio max TXOPLimit : 32767            Radio max ECWmax : 10
CAC information
Clients accepted                 : 0
  Voice                          : 0
  Video                          : 0
Total request mediumtime(μs)       : 0
  Voice(μs)                      : 0
  Video(μs)                      : 0
Calls rejected due to insufficient resources  : 0
Calls rejected due to invalid parameters     : 0
Calls rejected due to invalid mediumtime     : 0
Calls rejected due to invalid delaybound     : 0

Radio : 2
Client EDCA updates : 0
QoS mode : WMM
WMM status: Disabled
Radio max AIFSN    : 15              Radio max ECWmin : 10
Radio max TXOPLimit : 32767            Radio max ECWmin : 10
CAC information
Client accepted                  : 0
  Voice                          : 0
  Video                          : 0
Total request mediumtime(μs)       : 0
  Voice(μs)                      : 0
  Video(μs)                      : 0
Calls rejected due to insufficient resources  : 0
Calls rejected due to invalid parameters     : 0
```

```
Calls rejected due to invalid mediumtime     : 0
Calls rejected due to invalid delaybound     : 0
```

表 8-1 コマンド出力

フィールド	説明
Client EDCA	クライアントのEDCAパラメータが更新された回数です。
QoS mode	• WMM
WMM status	• Enable • Disable
Radio max AIFSN	無線がサポートする最大AIFSNです。
Radio max ECWmin	無線がサポートする最大ECWminです。
Radio max TXOPLimit	無線がサポートする最大TXOPLimitです。
Radio max ECWmax	無線がサポートする最大ECWmaxです。
Total request mediumtime	AC-VOおよびAC-VIキューの合計要求中間時間(マイクロ秒単位)です。

#すべてのクライアントの WMM 統計情報を表示します。

<AC> display wlan wmm client all

```
MAC address : 000f-e23c-0001           SSID : service
QoS mode : WMM
APSD information :
  Max SP length : 7
  L: Legacy    T: Trigger      D: Delivery
  AC           AC-BK    AC-BE   AC-VI    AC-VO
  Assoc State   T|D     L      T|D      T|D
Statistics information :
  Uplink packets     : 0          Downlink packets  : 0
  Uplink bytes       : 0          Downlink bytes    : 0
  Downgrade packets      : 0          Discarded packets      : 0
  Downgrade bytes        : 0          Discarded bytes        : 0
TS information:
  AC                 : AC-VO       User priority            : 7
  TID                : 1           Direction                : Bidirectional
  PSB                : 0           Surplus bandwidth allowance : 1.0000
  Medium time (μs)     : 39          MSDU size (bytes)          : 1500
  Mean data rate (Kbps) : 10.000      Minimum PHY rate (Mbps)     : 11.000
  TS creation time     : 0h:0m:5s
```

```
TS updating time      : 0h:0m:5s
Uplink TS packets     : 0           Downlink TS packets        : 0
Uplink TS bytes       : 0           Downlink TS bytes          : 0
```

表 8-2 コマンド出力

フィールド	説明
QoS mode	**WMM**はQoSモードを表します。 QoSモードが利用できない場合、このフィールドには**N/A**が表示されます。
Max SP length	最大サービス期間(SP)の長さです。
AC	• AC-VO • AC-VI • AC-BE • AC-BK
Assoc state	ACキューのAPSD属性です。 • **T**－ACキューがtrigger-enabledです。 • **D**－ACキューがdelivery-enabledです。 • **T	D**－ACキューは、trigger-enabledとdelivery-enabledの両方です。 • **L**－ACはレガシ属性のものです。
User priority	有線ネットワークからのパケットのユーザ優先度です。
TID	トラフィック識別子です。範囲は0～15です。
Direction	トラフィック方向です。 • Uplink • Downlink • Bidirectional
PSB	省電力動作です。 • **1**－U-APSD省電力モードです。 • **0**－従来の省電力モードです。
Surplus bandwidth allowance	余剰帯域幅のパーセンテージです。
Medium time	許容される中間時間(マイクロ秒)です。
MSDU size	平均MSDUサイズ(バイト)です。
Mean data rate	平均データ転送速度(Kbps)です。
Minimum PHY rate	最小物理伝送速度(Mbps)です。

関連コマンド

reset wlan wmm

8.1.8 edca client (ac-be | ac-bk)

Syntax

edca client { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-be** | **ac-bk** }

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view で使用される、クライアントの AC-BE キューと AC-BK キューのデフォルトの EDCA パラメータ値を表 8-3 に示します。

表 8-3 クライアントの AC-BE キューと AC-BK キューのデフォルト EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

noack: No ACK ポリシを使用するように AC キューを設定します。デフォルトでは、No ACK ポリシが使用されます。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットしか送信できません。

説明

edca client コマンドはクライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定します。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

すべてのクライアントが 802.11b クライアントである場合、AC-BE キューと AC-BK キューのそれぞれに対して TXOP Limit 値を 0 に設定することを推奨します。

802.11b と 802.11g の両方のクライアントが WLAN に存在する場合、AC-BK と AC-BE のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-BE キューの AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca client ac-be aifsn 5

AP group **apgroup1** の AC-BE キューに対して AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca client ac-be aifsn 5

8.1.9 edca client (ac-vi | ac-vo)

Syntax

edca client { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-vi** | **ac-vo** }

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view で使用される、クライアントの AC-VI キューと AC-VO キューのデフォルトの EDCA パラメータ値を表 8-4 に示します。

表 8-4 クライアントの AC-BE キューと AC-BK キューのデフォルト EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

cac: CAC を指定します。AC-VO および AC-VI キューは CAC をサポートします。CAC はデフォルトで無効になっています。

disable: CAC を無効にします。

enable: CAC を有効にします。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットしか送信できません。

説明

edca client コマンドはクライアントの AC-VI または AC-VO キューの EDCA パラメータを設定します。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

すべてのクライアントが 802.11b クライアントである場合、AC-VI および AC-VO キューの TXOPLimit 値をそれぞれ 188 と 102 に設定することを推奨します。

802.11b と 802.11g のそれぞれのクライアントが WLAN に存在する場合、AC-VI と AC-VO のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-VO キューの AIFSN を 3 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca client ac-vo aifsn 3

AP group **apgroup1** の AC-VO キューの AIFSN を 3 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca client ac-vo aifsn 3

8.1.10 edca radio

Syntax

edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **noack** | **txoplimit** *txoplimit-value* } *

undo edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** }

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、デフォルトの EDCA パラメータ値を表 8-5 に示します。

表 8-5 EDCA パラメータのデフォルト値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	6	0
AC-VI	1	3	4	94
AC-VO	1	2	3	47

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

ack-policy: AC キューの ACK ポリシを指定します。

noack: No ACK ポリシ（デフォルト）を指定します。

normalack: Normal ACK ポリシを指定します。

aifsn *aifsn-value*: AIFSN（Arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）の指数形式を指定します。*ecwmin-value* 引数の値の範囲は 0～10 です。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）の指数形式を指定します。*ecwmax-value* 引数の値の範囲は 0～10 です。ECWmax の値は ECWmin の値より小さくすることはできません。

txopimit *txoplimit-value*: TXOP Limit（Transmission opportunity limit）の値を 32 マイクロ秒単位で指定します。*txoplimit-value* 引数の値の範囲は 0～32767 です。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットのみを送信できます。

説明

edca radio コマンドは EDCA パラメータを設定します。

undo edca radio コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

802.11b 無線の場合、AC-BK、AC-BE、AC-VI、AC-VO キューの TXOP 制限値をそれぞれ 0、0、188、102 に設定することを推奨します。

例

無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] edca radio ac-vo aifsn 2

AP group **apgroup1** の無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] edca radio ac-vo aifsn 2

8.1.11 mu-edca client

🕮 メモ：

mu-edca client コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
mu-edca client コマンドは QX-W1100 シリーズの AP でのみサポートしています。

Syntax

mu-edca client { ac-be | ac-bk | ac-vi | ac-vo } { aifsn *aifsn-value* **| ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* **| muedcatimer** *muedcatimer-value* **} ***

undo mu-edca client { ac-be | ac-bk | ac-vi | ac-vo }

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view では、MU EDCA パラメータは指定されていません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 2～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

muedcatimer *muedcatimer-value*: MU EDCA パラメータのタイムアウトを 1 から 255 TU (1 TU=1024 us) の範囲で指定します。

説明

mu-edca client コマンドは MU EDCA パラメータを設定します。

undo mu-**edca client** コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

この機能を使用すると、802.11ax 無線と非 802.11 ax 無線の両方が存在する場合に、クライアントは 802.11ax パケットに対して異なる EDCA パラメータセットを使用して、非 802.11 ax パケットの公平な伝送を保証できます。

MU EDCA パラメータを設定すると、関連付けられた AP が 802.11 ax クライアントをトリガーしてデータを送信するときに、クライアントは MU EDCA パラメータの使用を選択できます。EDCA パラメータと比較して、MU EDCA パラメータは、より大きな aifsn、ecwmin、および ecwmax 値が指定され、待機時間と平均バックオフ時間を増やして 802.11 ax パケットの優先度を下げます。

システムは MU EDCA パラメータを使用するためのタイマーを設定します。タイマーの期限が切れる前に AP がクライアントにデータを送信するようにトリガーすると、タイマーはリセットされます。タイマーの期限が切れると、MU EDCA パラメータの代わりに、EDCA パラメータが 802.11 ax パケットに再び使用されます。

例

AC-BE キューの AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mu-edca client ac-be aifsn 5

AP group **apgroup1** の AC-BE キューに対して AIFSN を 5 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1120

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] mu-edca client ac-be aifsn 5

8.1.12 qos priority

Syntax

qos priotity *priority-value*

undo qos priotity

デフォルト

0

View

Service template view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティを 0～7 の範囲で指定します。値が大きいほど優先度が高くなります。

説明

qos priority コマンドはポートプライオリティを設定します。

undo qos priority コマンドはデフォルトに戻します。

ポートトラステッドモードが有効な場合、AP はポートプライオリティをサービステンプレートのすべてのパケットに割り当てます。

パケットトラステッドモードが有効な場合、このコマンドは有効になりません。

例

サービステンプレート 1 のポートプライオリティを 2 に設定します。

<AC> system

[AC] wlan service-template 1

[AC-wlan-st-1] qos priority 2

関連コマンド

qos trust

8.1.13 qos trust

Syntax

qos trust {**dot11e** | **dscp** }

undo qos trust

デフォルト

ポートプライオリティを信頼する

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11e: 優先度マッピングのためにパケット内で運ばれる 802.11e 優先度を使用します。
dscp: 優先度マッピングのためにパケット内で運ばれる DSCP 優先度を使用します。

説明

qos trust コマンドはパケットトラステッドモードを有効にします。

undo qos trust コマンドはデフォルトに戻します。

この機能は、アップリンクパケットでのみ有効です。

例

プライオリティマッピングのためにパケットで伝送される 802.11e プライオリティを使用するようにサービステンプレート 1 を設定します。

<AC> system

[AC] wlan service-template 1

[AC-wlan-st-1] qos trust dot11e

関連コマンド

qos priority

8.1.14 reset wlan wmm

Syntax

reset wlan wmm { **client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* } | **radio** { **all** | **ap** *ap-name* } }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

client: クライアントの WMM 統計情報を削除します。

all: すべての無線またはクライアントの WMM 統計情報を削除します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

radio: 無線の WMM 統計情報を削除します。

説明

reset wlan wmm コマンドは WMM 統計情報を削除します。

例

すべての無線の WMM 統計情報を削除します。

<AC> reset wlan wmm radio all

関連コマンド

display wlan wmm

8.1.15 svp map-ac

Syntax

svp map-ac { **ac-vi** | **ac-vo** }

svp map-ac disable

undo svp map-ac

デフォルト

radio view は、AP group view の設定を使用します。

AP group radio view は、SVP マッピングが無効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

説明

svp map-ac コマンドは指定された AC キューへの SVP マッピングを有効にします。

svp map-ac disable コマンドは SVP マッピングを無効にします。

undo svp map-ac コマンドはデフォルトに戻します。

SVP マッピングは、WMM 以外のクライアントでのみ有効です。

radio view の設定は、AP group radio view の設定よりも優先されます。

例

SVP パケットを AC-VO キューにマッピングします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] svp map-ac ac-vo

AP group **apgroup1** の SVP パケットを AC-VO キューにマッピングします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] svp map-ac ac-vo

8.1.16 u-apsd enable

🕮 **メモ：**

u-apsd enable コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。

Syntax

u-apsd enable

undo u-apsd enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

u-apsd enable コマンドは U-APSD を有効にします。

undo u-apsd enable コマンドは U-APSD を無効にします。

Unscheduled automatic power-save delivery (U-APSD) は、クライアントの電力を節約するために WMM によって定義された節電方法です。

U-APSD は、WMM を有効にすると自動的に有効になります。

クライアントが U-APSD をサポートしている場合、この機能を有効にして節電機能を向上させることを推奨します。

この機能を設定するにはサービステンプレートが無効になっていることを確認してください。

例

U-APSD を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] u-apsd enable

8.1.17 wlan client-rate-limit

Syntax

wlan client-rate-limit { **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]

undo wlan client-rate-limit [{ **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } [**inbound** | **outbound**]]

デフォルト

クライアントタイプベースのクライアントレート制限は設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a クライアントを指定します。

dot11ac: 802.11ac クライアントを指定します。

dot11ax: 802.11ax クライアントを指定します。

dot11an: 802.11an クライアントを指定します。

dot11b: 802.11b クライアントを指定します。

dot11g: 802.11g クライアントを指定します。

dot11gac: 802.11gac クライアントを指定します。

dot11gn: 802.11gn クライアントを指定します。

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

cir *cir*: 各クライアントの CIR を Kbps 単位で指定します。*cir* 引き数の値は 1～2097152 の範囲です。

cbs *cbs*: 各クライアントの CBS をバイト単位で指定します。*cbs* 引数の値は 1～268435456 の範囲です。このオプションを指定しない場合、CBS の値は CIR の値から自動的に計算されます。

説明

wlan client-rate-limit コマンドはクライアントタイプベースのクライアントレート制限を設定します。

undo wlan client-rate-limit コマンドは設定を削除します。

クライアントレート制限のために、異なるレート制限方式とレート制限モードを設定することができ、すべての設定が有効になります。これらの設定間のうちレート制限の最小値が各クライアントに適用されます。

例

802.11an クライアントの受信トラフィックのレート制限を 20480 Kbps に設定します。

<AC> system-view

[AC] wlan client-rate-limit dot11an inbound cir 20480

8.1.18 wlan max-bandwidth

Syntax

wlan max-bandwidth { **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } *bandwidth*

undo wlan max-bandwidth [**dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn**]

デフォルト

次の最大帯域幅設定が適用されます。

- dot11a と dot11g に対して 30000 Kbps
- dot11an、dot11gn と dot11gac に対して 250000 Kbps
- dot11ac と dot11ax では 500000 Kbps
- dot11b では 7000 Kbps

View

System view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11an: 802.11an 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gac: 802.11gac 無線モードを指定します。

dot11gn: 802.11gn 無線モードを指定します。

bandwidth: 最大帯域幅を Kbps 単位で指定します。値の範囲は、無線の種類によって次のように変化します。

- dot11a と dot11g は 16～30000 です。
- dot11an、dot11gn と dot11gac は 16～250000 です。
- dot11ac と dot11ax は 16～500000 です。
- dot11b は 16～7000 です。

説明

wlan max-bandwidth コマンドは無線タイプごとの最大帯域幅を設定します。

undo wlan max-bandwidth コマンドは指定した無線タイプのデフォルト設定またはすべての無線タイプのデフォルト設定を復元します。

最大帯域幅は、保証された帯域幅を計算するために使用されます。

例

802.11ac の最大帯域幅を 2000 Kbps に設定します。

<AC> system-view

[AC] wlan max-bandwidth dot11ac 2000

8.1.19 wmm

Syntax

wmm { **disable** | **enable** }

undo wmm

デフォルト

radio view は、AP group view で設定を使用します。

AP group radio view は、WMM が有効になっています。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: WMM を無効にします。

enable: WMM を有効にします。

説明

wmm enable コマンドは WMM を有効にします。

wmm disable コマンドは WMM を無効します。

undo wmm コマンドはデフォルトに戻します。

radio view の設定は、AP group radio view の設定よりも優先されます。

すべての 802.11n クライアントは WLAN QoS をサポートしている必要があります。802.11n クライアントが関連する AP と通信するために、無線が 802.11an または 802.11gn モードで動作しているときに WMM を有効にしてください。

例

WMM を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] wmm disable

AP group **apgroup1** の WMM を無効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] wmm disable

目次

9 章 WLAN ローミングの設定 9-1
9.1 WLAN ローミングの設定コマンド 9-1
9.1.1 authentication-mode 9-1
9.1.2 display wlan mobility 9-2
9.1.3 display wlan mobility group 9-4
9.1.4 display wlan mobility roam-track mac-address 9-5
9.1.5 group enable 9-6
9.1.6 member 9-7
9.1.7 snmp-agent trap enable wlan mobility 9-8
9.1.8 source 9-9
9.1.9 tunnel-type 9-10
9.1.10 wlan mobility group 9-11
9.1.11 wlan mobility-group-isolation enable 9-12
9.2 WLAN 802.11r コマンド 9-13
9.2.1 ft enable 9-13
9.2.2 ft method 9-14
9.2.3 ft mobility-domain-id 9-15
9.2.4 ft reassociation-timeout 9-16
9.3 WLAN 802.11v コマンド 9-17
9.3.1 bss transition-management disassociation 9-17
9.3.2 bss transition-management enable 9-18
9.3.3 sacp anti-sticky 9-19

9章 WLAN ローミングの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

9.1 WLANローミングの設定コマンド

9.1.1 authentication-mode

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

authentication-mode *authentication-mode* **[cipher | simple]** *authentication-key*

undo authentication-mode

デフォルト

IACTP 制御メッセージの認証モードは設定されていません。AC は IACTP 制御メッセージの完全性を検証しません。

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

authentication-mode: 認証モードを指定します。128 ビット MD 5 認証モードのみサポートします。

cipher: 暗号テキストの認証キーを指定します。

simple: プレーンテキストの認証キーを指定します。

authentication-key: 認証キーの文字列を設定します。大文字と小文字を区別します。**simple** を指定した場合、プレーンテキストで 1～16 の文字列でなくてはなりません。**cipher** を設定した場合、33～53 文字の暗号テキストでなければなりません。セキュリティのため、プレーンテキストのキーを含むすべてのキーは暗号化されて保存されます。

説明

authentication-mode コマンドは IACTP 制御メッセージの認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

例

#モビリティグループ aaa の 認証モードを MD5 に設定し、認証キー12345 をプレーンテキストで設定します。

<AC> system-view

[AC] wlan mobility group aaa

[AC] authentication-mode md5 simple 12345

9.1.2 display wlan mobility

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan mobility { roam-in | roam-out } [member ip *ipv4-address* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

roam-in: 別の AC からローミングしたクライアントに関する情報を表示します。

roam-out: 別の AC にローミングしたクライアントに関する情報を表示します。

member ip *ipv4-address*: メンバ AP の IPv4 アドレスを指定します。

説明

display wlan mobility コマンドは AC 間でローミングしたクライアントに関する情報を表示します。

例

AC にローミングしたすべてのクライアントに関する情報を表示します。

<AC> display wlan mobility roam-in

```
Total entries: 1
MAC address    BSSID         VLAN ID  HA IP address
5250-0012-0411  cbab-abab-abab  1       192.168.0.101
```

指定されたメンバ AC にローミングしたクライアントに関する情報を表示します。

<AC> display wlan mobility roam-in member ip 192.168.0.101

```
Total entries: 1
MAC address    BSSID         VLAN ID
5250-0012-0411  cbab-abab-abab  1
```

#別の AC にローミングしたすべてのクライアントに関する情報を表示します。

<AC> display wlan mobility roam-out

```
Total entries: 1
MAC address    BSSID         VLAN ID  Online time      FA IP address
5250-0012-0411  cbab-abab-abab  1       00hr 01min 39sec  192.168.0.102
```

#指定されたメンバ AC から別の AC にローミングしたクライアントに関する情報を表示します。

[AC] display wlan mobility roam-out member ip 192.168.0.102

```
Total entries: 1
MAC address    BSSID         VLAN ID  Online time
5250-0012-0411  cbab-abab-abab  1       00hr 03min 02sec
```

表 9-1 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
BSSID	クライアントが関連付けられているAPのBSSID
VLAN ID	クライアントのVLAN ID
Online time	クライアントのオンライン時間
HA IP address	クライアントのローミング元APのIPアドレス
FA IP address	クライアントのローミング先APのIPアドレス

9.1.3 display wlan mobility group

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan mobility group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan mobility group コマンドはモビリティグループ情報を表示します。

例

#モビリティグループ情報を表示します。

<AC> display wlan mobility group

```
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 172.16.220.101
 Source IPv6: Not configured
 Authentication method: Not configured
 Mobility group status: Enabled
 Member entries: 2
 IP address                      State        Online time
 172.16.220.102                   Down         00hr 00min 00sec
 172.16.220.105                   Up           00hr 36min 27sec
```

表 9-2 コマンド出力

フィールド	説明
Tunnel type	モビリティグループのIACTPトンネルタイプです。 • IPv4 • IPv6
Source IPv4	IACTPトンネルの確立に使用する送信元IPv4アドレスです。

フィールド	説明
Source IPv6	IACTP トンネルの確立に使用する送信元IPv6アドレスです。
Authentication method	モビリティグループに使用される認証方式です。
Mobility group status	モビリティグループのステータスです。 • enable • disable
IP address	メンバAPのIPアドレスです。
State	IACTP トンネルのステータスです。 • UP • DOWN
Online time	メンバAPのオンライン時間です。

9.1.4 display wlan mobility roam-track mac-address

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan mobility roam-track mac-address *mac-address*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを指定します。

説明

display wlan mobility roam-track mac-address コマンドはホーム AC 上のクライアントのローミング情報を表示します。最新のローミングトラック情報が最初に表示されます。

例

#ホーム AC 上の指定されたクライアントのローミング情報を表示します。

<AC> display wlan mobility roam-track mac-address 5250-0012-0411

```
Total entries: 2
BSSID         Created at          Online time      AP IP address  RID  AP name
3ce5-a68d-2280  2017-03-14 11:12:28  00hr 48min 46sec  192.168.0.2    2    ap1
3ce5-a608-1150  2017-03-14 11:12:05  00hr 40min 46sec  127.0.0.1      2    ap2
```

表 9-3 コマンド出力

フィールド	説明
BSSID	クライアントが関連付けられているAPのBSSIDです。
Created at	クライアントのローミングトラックエントリが作成された日時。
Online time	クライアントのオンライン時間。
AC IP address	クライアントが関連付けられているACのIPアドレスです。
RID	クライアントが関連付けられている無線のIDです。
AP name	クライアントが関連付けられているAPの名前です。

9.1.5 group enable

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

group enable

undo group enable

デフォルト

無効

View

Mobility group view

定義済みユーザロール

network-admin

説明

group enable コマンドはモビリティグループを有効にします。

undo group enable コマンドはモビリティグループを無効にします。

例

#モビリティグループ floor 1 を有効にします。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] tunnel-type ipv4

[AC-wlan-mg-floor1] source ip 192.168.0.1

[AC-wlan-mg-floor1] member ip 192.168.0.2

[AC-wlan-mg-floor1] group enable

関連コマンド

- **member**
- **source**
- **tunnel-type**
- **wlan mobility group**

9.1.6 member

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

member ip *ip-address*

undo member [**ip** *ip-address*]

デフォルト

メンバ AC の設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: メンバ AC の IPv4 アドレスを指定します。

説明

member コマンドはモビリティグループメンバを追加します。

undo member コマンドはモビリティグループメンバを削除します。

モビリティグループが無効の場合のみ、メンバの追加・削除が可能です。

モビリティグループのメンバは、IACTP トンネルの確立に使用される IP アドレスによって識別されます。

AC は 1 つのモビリティグループだけに属することが出来ます。

モビリティグループには、最大 31 のモビリティグループメンバを追加できます。

undo member コマンドの使用時に、IP アドレスを省略した場合、モビリティグループ内のすべてのメンバを削除します。

例

#モビリティグループ floor 1 にメンバ 192.168.1.55 を追加します。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] member ip 192.168.1.55

9.1.7 snmp-agent trap enable wlan mobility

Syntax

snmp-agent trap enable wlan mobility

undo snmp-agent trap enable wlan mobility

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan mobility コマンドは WLAN ローミングの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan mobility コマンドは WLAN ローミングの SNMP 通知を無効にします。

重要な WLAN ローミングイベントを NMS に送信するには、WLAN ローミングの SNMP 通知を有効にします。WLAN ローミングイベント通知を正しく送信するには、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 11 *システム管理 "SNMP"* の説明に従って SNMP も設定する必要があります。

例

WLAN ローミングの SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan mobility

9.1.8 source

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

source ip *ip-address*

undo source

デフォルト

送信元 IPv4 アドレスの設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

source コマンドは IACTP トンネルを確立するための送信元 IPv4 アドレスを設定します。

undo source コマンドは IACTP トンネルを確立するための送信元 IPv4 アドレスを削除します。

モビリティグループが無効の場合のみ、送信元 IPv4 アドレスの設定・削除が可能です。

1 つの送信元 IPv4 アドレスだけ設定することができます。

例

#IACTP トンネルを確立するための送信元 IPv 4 アドレス 192.168.1.55 を設定します。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] source ip 192.168.1.55

関連コマンド

- **group enable**
- **member**

9.1.9 tunnel-type

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

tunnel-type ipv4

undo tunnel-type

デフォルト

IPv4

View

Mobility group view

定義済みユーザロール

network-admin

説明

tunnel-type コマンドは IACTP トンネルの IP アドレスタイプを設定します。

undo tunnel-type コマンドはデフォルトに戻します。

例

#モビリティグループ floor1 の IACTP トンネルの IP アドレスタイプとして IPv4 を設定します。

<AC> system-view

[AC] wlan mobility group floor1

[AC-wlan-mg-floor1] tunnel-type ipv4

9.1.10 wlan mobility group

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

wlan mobility group *group-name*

undo wlan mobility group *group-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: モビリティグループ名を指定します。モビリティグループ名は、1～15 文字の文字列です。大文字と小文字を区別します。

説明

wlan mobility group コマンドはモビリティグループを作成します。

undo wlan mobility group コマンドはモビリティグループを削除します。

メンバ AC に設定するモビリティグループは、同じ名前である必要があります。

1 つの AC に作成できるモビリティグループは 1 つだけです。

例

#モビリティグループ **office** を作成し、その view に移行します。

<AC>system-view

[AC] wlan mobility group office

[AC-wlan-mg-office]

9.1.11 wlan mobility-group-isolation enable

メモ：

この章のコマンドはソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

Syntax

wlan mobility-group-isolation enable

undo wlan mobility-group-isolation enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネル分離を有効にします。

undo wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネル分離を無効にします。

このコマンドは、モビリティグループ内の AP 間にループが存在する場合に必要です。このコマンドにより、AP はモビリティグループ内のトンネル間でパケットを転送できなくなり、ブロードキャストストームが回避されます。

例

#モビリティグループのトンネル分離をイネーブルにします。

<AC>system-view

[AC] wlan mobility-group-isolation enable

9.2 WLAN 802.11rコマンド

🕮 **メモ：**

この章のコマンドはソフトウェアバージョン 7.2.52 を含む以降のソフトウェアからサポートしています。

9.2.1 ft enable

Syntax

ft enable

undo ft enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

ft enable コマンドは FT（Fast BSS Transition）を有効にします。

undo ft enable コマンドは FT を無効にします。

FT により、クライアントが BSS から同一 ESS の別の BSS にローミングする際の遅延が短縮されます。802.11r FT を使用すると、クライアントはローミング先の AP とメッセージを交換する必要があります。FT は 2 つのメッセージ交換方法を提供します。

FT を有効にする場合、サービステンプレートが無効であることを確認してください。

FT を有効にするサービステンプレートは、security-ie rsn、client association-location ac を使用し、WPA3 と enhanced-open が無効である必要があります。

例

FT を有効にします。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft enable

9.2.2 ft method

Syntax

ft method { **over-the-air** | **over-the-ds** }

undo ft method

デフォルト

over-the-air

View

Service template view

定義済みユーザロール

network-admin

パラメータ

over-the-air: Over-the-air FT を指定します。この方法では、クライアントは事前ローミング認証のためにローミング先の AP と直接通信できます。

over-the-DS: Over-the-DS FT を指定します。この方法では、クライアントは事前ローミング認証のために現在接続している AP を経由してローミング先の AP と通信します。

説明

ft method コマンドは FT 方法を設定します。

undo ft method コマンドはデフォルトに戻します。

FT 方法を設定する場合、サービステンプレートが無効であることを確認してください。

このコマンドは FT が有効の場合にのみ適用されます。

例

FT 方法を Over-the-DS に設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft method over-the-ds

関連コマンド

ft enable

9.2.3 ft mobility-domain-id

メモ：

このコマンドはソフトウェアバージョン 7.2.56 を含む以降のソフトウェアからサポートしています。

Syntax

ft mobility-domain-id *mobility-domain-id*

undo ft mobility-domain-id

デフォルト

設定無し

View

Service template view

定義済みユーザロール

network-admin

パラメータ

mobility-domain-id：モビリティドメイン ID を 1 から 65535 の範囲で指定します。

説明

ft mobility-domain-id コマンドはモビリティドメイン ID を設定します。

undo ft mobility-domain-id コマンドはデフォルトに戻します。

クライアントが異なる AP 間を移動するときに、クライアントのアクセス時間を短縮するには、この機能を設定します。

この機能を設定すると、クライアントは、2 つの AP が同じモビリティドメイン ID を持つ場合に限り、802.11r FT(fast BSS transition) を介して異なる AP 間をローミングできます。

クライアントが、FT が有効なっていてもモビリティグループに含まれていない AP 間を移動する場合、クライアントは AP 間の FT ローミングを使用する場合があります。ただし、AP は同じモビリティグループに属していないため、ローミングは失敗します。次に、クライアントはアソシエーションを使用して新しい AP に切り替えます。

AP に異なるモビリティドメイン ID を設定することで、クライアントは AP 間の FT ローミングを試行せずに新しい AP に直接関連付けができるようになります。その結果、AP 間の FT ローミング処理が省略されるため、サービス切り替え時間が短縮されます。サービステンプレートを有効にする前に、この機能を設定します。この機能は、FT が有効の場合にだけ有効です。

例

AC にモビリティドメイン ID666 を設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft mobility-domain-id 666

関連コマンド

ft enable

9.2.4 ft reassociation-timeout

Syntax

ft reassociation-timeout *timeout*

undo ft reassociation-timeout

デフォルト

20 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

timeout: 再関連付けタイムアウトタイマを 1～100 秒の範囲で指定します。

説明

ft reassociation-timeout コマンドは再関連付けタイムアウトタイマを設定します。

undo ft reassociation-timeout コマンドはデフォルトに戻します。

再関連付けタイムアウトタイマを設定する場合、サービステンプレートが無効であることを確認してください。

このコマンドは FT が有効の場合のみ適用されます。

タイムアウトタイマが終了する前にクライアントが再関連付け要求を送信しない場合、ローミングプロセスは終了されます。

例

再関連付けタイムアウトタイマを 30 秒に設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] ft reassociation-timeout 30

関連コマンド

ft enable

9.3 WLAN 802.11vコマンド

🕮 **メモ：**

- この章のコマンドは V7.2.52 を含む以降のバージョンからサポートしています。
- 802.11v の設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

9.3.1 bss transition-management disassociation

Syntax

bss transition-management disassociation { **forced** | **recommended** } [**timer** *time*]

undo bss transition-management disassociation

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

パラメータ

forced: アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はそのクライアントを強制的にログオフします。

recommended: アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はクライアントを強制的にログオフしません。

time: アソシエーション解除タイマを 0～180 秒の範囲で指定します。デフォルトのタイマは 90 秒です。このタイマを 0 に設定すると、bss transition-management disassociation forced が有効の場合、AP は BTM 要求をクライアントに送信した直後に、そのクライアントを強制的にログオフします。bss transition-management disassociation

recommended が有効の場合、AP はクライアントに BTM 要求を送信した後、そのクライアントからログオフしません。

説明

bss transition-management disassociation コマンドは BTM アソシエーション解除を設定します。

undo bss transition-management disassociation コマンドはデフォルトに戻します。

BTM のアソシエーション解除を有効にするには、まず BTM を有効にします。BTM アソシエーション解除を設定する場合、サービステンプレートが無効であることを確認してください。

BTM アソシエーション解除が設定されている場合、AP はクライアントから BTM query ーを受信すると BTM request をクライアントに送信し、BSS 移行のためにクライアントを案内します。

bss transition-management disassociation forced を設定すると、アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合に、クライアントが強制的にログオフされます。この機能は慎重に使用してください。

例

BTM のアソシエーション解除(forced)を有効にし、タイマを 60 秒に設定します

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] bss transition-management disassociation forced timer 60

関連コマンド

- **bss transition-management enable**
- **sacp anti-sticky**

9.3.2 bss transition-management enable

Syntax

bss transition-management enable

undo bss transition-management enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

bss transition-management enable コマンドは BTM を有効にします。

undo bss transition-management enable コマンドはデフォルトに戻します。

BTM を使用すると、接続中の AP の信号強度が低い場合や、より優れた AP が検出された場合に、クライアントは最適な AP にローミングできます。

client anti-sticky が無効の場合、AP はクライアントの信号強度がしきい値よりも低いかどうかを調べず、unsolicited BTM をトリガしません。

この作業を行う前に、サービステンプレートが無効になっていることを確認してください。

例

BTM を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] bss transition-management enable

関連コマンド

- **bss transition-management forced-disassociation**
- **sacp anti-sticky**

9.3.3 sacp anti-sticky

🕮 **メモ：**

forced-logoff のパラメータはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

Syntax

sacp anti-sticky { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }

undo sacp anti-sticky

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view ではクライアント anti-sticky は有効です

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*: RSSI しきい値を 5～100(dbm)の範囲で設定します。デフォルトのしきい値は 20dbm です。

interval *interval*: 検出間隔を 3～10(秒)の範囲で設定します。デフォルトの検出間隔は 3 秒です。

forced-logoff: 信号強度が RSSI しきい値よりも低い非 802.11v クライアントをログオフします。

説明

sacp anti-sticky enable コマンドはクライアント anti-sticky を有効にします。

sacp anti-sticky disable コマンドはクライアント anti-sticky を無効にします。

undo sacp anti-sticky コマンドはデフォルトに戻します。

この機能により、AP は指定された間隔でクライアントの信号強度を調べることができます。802.11v クライアントの場合、クライアントの信号強度が RSSI しきい値より低いと、関連付けられた AP が BSS 移行をトリガして、クライアントをより適切な BSS に導きます。802.11v 以外のクライアントの場合、アクションは実行されません。

例

AP1 の radio1 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

AP グループ 1 のモデル QX-W1120 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-model-QX-W1120] radio 2

[AC-wlan-ap-group-1-model-QX-W1120-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

関連コマンド

- **bss transition-management disassociation**
- **bss transition-management enable**

目次

10 章 WLAN ロードバランスの設定 10-1
10.1 WLAN ロードバランスの設定コマンド 10-1
10.1.1 ap radio 10-1
10.1.2 description 10-2
10.1.3 display wlan load-balance group 10-3
10.1.4 display wlan load-balance status service-template 10-4
10.1.5 snmp-agent trap enable wlan load-balance 10-6
10.1.6 wlan load-balance access-denial 10-6
10.1.7 wlan load-balance enable 10-7
10.1.8 wlan load-balance group 10-8
10.1.9 wlan load-balance mode bandwidth 10-9
10.1.10 wlan load-balance mode session 10-10
10.1.11 wlan load-balance mode traffic 10-10
10.1.12 wlan load-balance rssi-threshold 10-11

10章 WLAN ロードバランスの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

10.1 WLANロードバランスの設定コマンド

10.1.1 ap radio

Syntax

ap name *ap-name* **radio** *radio-id*

undo ap { **name** *ap-name* [**radio** *radio-id*] | **all** }

デフォルト

なし

View

Load balancing group view

定義済みユーザロール

network-admin

パラメータ

ap-name: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

radio-id: 名前で無線を指定します。この引数の範囲は AP のモデルにより異なります。

all: すべての無線を指定します。

説明

ap radio コマンドはロードバランスグループに無線を追加します。

undo ap コマンドはロードバランスグループから 1 つもしくはすべての無線を取り除きます。

1 つのロードバランスグループにのみ無線を追加できます。

undo ap コマンド内で無線を指定しない場合、このコマンドは指定された AP のすべての無線をロードバランスグループから取り除きます。

例

AP 1 の無線 2 をロードバランスグループ 10 に追加します。

<AC> system-view

[AC] wlan load-balance group 10

[AC-wlan-lb-group-10] ap name ap1 radio 2

10.1.2 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Load balancing group view

定義済みユーザロール

network-admin

パラメータ

text: ロードバランスグループに対する記述を指定します。1~63 の文字列です。大文字、小文字を区別します。

説明

description コマンドはロードバランスグループに対して記述を設定します。

undo description コマンドはロードバランスグループに対する記述を削除します。

例

ロードバランスグループ 10 に対する記述を marketing に追加します。

<AC> system-view

[AC] wlan load-balance group 10

[AC-wlan-lb-group10] description marketing

10.1.3 display wlan load-balance group

Syntax

display wlan load-balance group { *group-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: ロードバランスグループ ID を指定します。範囲は 1～65535 です。

all: すべてのロードバランスグループを指定します。

説明

display wlan load-balance group コマンドはロードバランスグループ情報を表示します。

例

ロードバランスグループ 1 の情報を表示します。

<AC> display wlan load-balance group 1

```
                    WLAN load balance group information
--------------------------------------------------------------------------------
Group ID            : 1
Description         :
Group members       : ap3-radio2,
                      ap2-radio1,
                      ap1-radio1,
--------------------------------------------------------------------------------
```

すべてのロードバランスグループの情報を表示します。

<AC> display wlan load-balance group all

```
                WLAN load balance group information
--------------------------------------------------------------------------------
Group ID             : 1
Description          :
Group members         : ap3-radio2,
                      ap2-radio1,
                      ap1-radio1,
--------------------------------------------------------------------------------
```

```
Group ID              : 2
Description           : marketing
Group members         : ap3-radio1,
------------------------------------------------------------------------------
```

表 10-1 コマンド出力

フィールド	説明
グループメンバ	ロードバランスグループ内の無線のリスト

10.1.4 display wlan load-balance status service-template

Syntax

display wlan load-balance status service-template *template-name* { **client** *mac-address* | **group** *group-id* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

template-name: サービステンプレート名を指定します。1～63 文字の文字列です。大文字と小文字を区別しません。

group-id: ロードバランシンググループ内の無線に関する情報を表示します。group-id 引数には、ロードバランシンググループの ID を指定します。範囲は 1～65535 です。

mac-address: クライアントを検出した無線に関する情報を表示します。mac-address 引数には、クライアントの MAC アドレスを H-H-H 形式で指定します。

説明

display wlan load-balance status service-template コマンドはサービステンプレートにバインドされている無線のロードバランシング情報を表示します。

例

サービステンプレート **st1** にバインドされ、ロードバランシンググループ 1 にある無線のロードバランシング情報を表示します。

<AC> display wlan load-balance status service-template st1 group 1

```
Current load balancing mode (threshold/gap): session (2/1)
```

```
Total radios: 4

APID/RID  Group ID  Session  Bandwidth(Mbps)  Traffic(%)  Balance(Y/N)
------------------------------------------------------------------------------
1/1       1         2        100              5           Y
1/2       1         10       50               10          N
2/1       1         2        10               1           Y
2/2       1         2        0                0           Y
```

サービステンプレート **st1** にバインドされ、MAC アドレスが **702d-2249-33bf** のクライアントを検出する無線のロードバランシング情報を表示します。

<AC> display wlan load-balance status service-template st1 client 702d-2249-33bf

```
Current load balancing mode (threshold/gap): session (2/1)
Load balancing group exist: Yes
Total radios: 4

APID/RID  Group ID  Session  Bandwidth(Mbps)  Traffic(%)  Balance(Y/N)
------------------------------------------------------------------------------
3/1       0         2        100              5           Y
1/2       1         10       50               10          N
4/1       1         2        10               1           Y
4/2       0         2        0                0           Y
```

表 10-2 コマンド出力

フィールド	説明
Load-balance group exist	負荷分散グループの有無: **Yes**または**No**
Group ID	ロードバランシンググループID。0は、無線がロードバランシンググループにないことを示します。
Session	無線に関連付けられたクライアントの数
Bandwidth(Mbps)	無線の帯域幅（Mbps）
Traffic(%)	無線でサポートされている最大帯域幅に対する、無線でのトラフィックの割合
Balance(Y/N)	ロードバランシングの状態: • **Y**—無線がロードバランシングされています。 • **N**—無線がロードバランシングされていません。

10.1.5 snmp-agent trap enable wlan load-balance

Syntax

snmp-agent trap enable wlan load-balance

undo snmp-agent trap enable wlan load-balance

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nmp-agent trap enable wlan load-balance コマンドは WLAN ロードバランスに対する SNMP 通知を有効にします。

undo snmp-agent trap enable wlan load-balance コマンドはデフォルトに戻します。

重要な WLAN ロードバランスイベントを NMS に報告するために、SNMP 通知を有効にします。WLAN ロードバランスイベント通知を正確に送信するために、オペレーションマニュアルのセクション 11 *システム管理 "SNMP"* に記載されるように SNMP も設定しなければなりません。

例

WLAN ロードバランスに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan load-balance

10.1.6 wlan load-balance access-denial

Syntax

wlan load-balance access-denial *access-denial*

undo wlan load-balance access-denial

デフォルト

10

View

System view

定義済みユーザロール

network-admin

パラメータ

access-denial: 紐付け要求の拒否の最大数を指定します。範囲は 2~10 です。

説明

wlan load-balance access-denial コマンドは紐付け要求に対する拒否の最大数を設定します。

undo wlan load-balance access-denial コマンドはデフォルトに戻します。

AP が拒絶する回数が最大数に達した場合、AP はクライアントからの紐付け要求を許可します。

例

紐付け要求の拒否の最大数を 4 に設定します。

<AC> system-view

[AC] wlan load-balance access-denial 4

10.1.7 wlan load-balance enable

Syntax

wlan load-balance enable

undo wlan load-balance enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan load-balance enable コマンドは WLAN ロードバランスを有効にします。

undo wlan load-balance enable コマンドは WLAN ロードバランスを有効にします。

例

WLAN ロードバランスを有効にします。

<AC> system-view

[AC] wlan load-balance enable

10.1.8 wlan load-balance group

Syntax

wlan load-balance group *group-id*

undo wlan load-balance group { *group-id* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id: ロードバランスグループ ID を指定します。範囲は 1～65535 です。

all: すべてのロードバランスグループを指定します。

説明

wlan load-balance group コマンドはロードバランスグループを作成し、その view に移行します。

undo wlan load-balance group コマンドは 1 つもしくはすべてのロードバランスグループを取り除きます。

特定の AP 間でロードバランスを実行するために、AP の無線をロードバランスグループに追加することができます。AC はロードバランスグループに属さない無線ではロードバランスを実行しません。

例

ロードバランスグループ 10 を作成し、その view に移行します。

<AC> system-view

[AC] wlan load-balance group 10

[AC-wlan-lb-group-10]

関連コマンド

ap radio

10.1.9 wlan load-balance mode bandwidth

Syntax

wlan load-balance mode bandwidth *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードロードバランス

View

System view

定義済みユーザロール

network-admin

パラメータ

value: 帯域幅しきい値を指定します。範囲は 1~500Mbps です。

gap-value: 帯域幅ギャップしきい値を指定します。範囲は 1~200Mbps です。

帯域幅ギャップしきい値のデフォルトは 20Mbps です。

説明

wlan load-balance mode bandwidth コマンドは帯域幅モードロードバランスを設定します。

undo wlan load-balance mode コマンドはデフォルトに戻します。

以下の条件が満たされたとき、AC は帯域幅モードロードバランスを実行します。

- AP の帯域幅が帯域幅しきい値に達する場合。
- 最小の帯域幅を有する AP 間の帯域幅ギャップが、帯域幅ギャップしきい値に達する場合。

例

帯域幅モードにロードバランスモードを設定し、帯域幅しきい値と帯域幅ギャップしきい値をそれぞれ 100Mbps と 20Mbps に設定します。

<AC> system-view

[AC] wlan load-balance mode bandwidth 100 gap 20

10.1.10 wlan load-balance mode session

Syntax

wlan load-balance mode session *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードロードバランスを使用します。セッションしきい値は 20 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

value: セッションしきい値を指定します。範囲は 1～120 の範囲です。

gap-value: セッションギャップしきい値を指定します。範囲は 1~12 です。セッションギャップしきい値のデフォルトは 4 です。

説明

wlan load-balance mode session コマンドはセッションモードロードバランスを設定します。

undo wlan load-balance mode コマンドはデフォルトに戻します。

以下の条件が満たされたとき、AC はセッションモードロードバランスを実行します。

- AP に紐付いたクライアント数がセッションしきい値に達する場合。
- 最小のクライアントを有する AP 間のセッションギャップが、セッションギャップしきい値に達する場合。

例

セッションモードにロードバランスモードを設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 7 と 5 に設定します。

<AC> system-view

[AC] wlan load-balance mode session 7 gap 5

10.1.11 wlan load-balance mode traffic

Syntax

wlan load-balance mode traffic *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードのロードバランシングが使用されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

value: トラフィックのしきい値を、トラフィックと AP の最大帯域幅の比率で指定します。範囲は 1～80%です。

gap-value: トラフィックギャップと AP の最大帯域幅の比率でトラフィックギャップのしきい値を指定します。この引数の値の範囲は 10～40%です。デフォルトのトラフィックギャップのしきい値は 20%です。

説明

wlan load-balance mode traffic コマンドはトラフィックモードロードバランスを設定します。

undo wlan load-balance mode コマンドはデフォルトに戻します。

次の条件が満たされると、AC はトラフィックモードのロードバランシングを実行します。

1) AP のトラフィックがトラフィックのしきい値に達する。
2) トラフィックが最も少ない AP と AP の間のトラフィックギャップがトラフィックギャップのしきい値に達する。

例

ロードバランシングモードをトラフィックモードに設定し、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 25%と 20%に設定します。

<AC> system-view

[AC] wlan load-balance mode traffic 25 gap 20

10.1.12 wlan load-balance rssi-threshold

Syntax

wlan load-balance rssi-threshold *rssi-threshold*

undo wlan load-balance rssi-threshold

デフォルト

25

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: RSSI しきい値を指定します。範囲は 5~100 です。

説明

wlan load-balance rssi-threshold コマンドは RSSI（Received Signal Strength Indicator）しきい値を設定します。

undo wlan load-balance rssi-threshold コマンドはデフォルトに戻します。

クライアントは複数の AP に検出される可能性があります。クライアントの RSSI がロードバランス RSSI しきい値より低い場合、AP はそのクライアントを検出しません。クライアントを検出できる AP が 1 つだけの場合、オーバーロードであっても AP はクライアントに対するアクセス確率を向上させます。

例

RSSI しきい値を 40 に設定します。

<AC> system-view

[AC] wlan load-balance rssi-threshold 40

目次

11 章 WLAN 無線リソースの計測の設定 11-1
11.1 WLAN 無線リソースの計測の設定コマンド 11-1
11.1.1 display wlan measure-report 11-1
11.1.2 measure 11-4
11.1.3 measure-duration 11-6
11.1.4 measure-interval 11-7
11.1.5 resource-measure 11-8
11.1.6 rm-capability mode 11-9

11章 WLAN 無線リソースの計測の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

11.1 WLAN無線リソースの計測の設定コマンド

11.1.1 display wlan measure-report

Syntax

display wlan measure-report ap *ap-name* **radio** *radio-id* [**client mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

radio *radio-id*: 番号を使用して無線を指定します。設定範囲はデバイスモデルにより異なります。

client mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、すべてのクライアントの計測結果を表示します。

説明

display wlan measure-report コマンドはクライアントの測定結果を表示します。

例

AP ap1 の無線 2 に接続したクライアントの計測結果を表示します。

<AC> display wlan measure-report ap ap1 radio 2

```
Total number of clients: 1

Client MAC address                          : 0aef-e760-3587
```

```
Link measurement:
  Link margin                          : 2 dBm
  RCPI                                 : -85 dBm
  RSNI                                 : 53 dBm
Noise histogram:
  Antenna ID                           : 3
  ANPI                                 : -56 dBm
  IPI0 to IPI10 density                : 5 12 16 13 8 5 5 15 17 1 3
Spectrum measurement:
  Transmit power                       : 20 dBm
  BSS                                  : Detected
  OFDM preamble                        : Detected
  Radar                                : Detected
  Unidentified signal                  : Undetected
  CCA busy fraction                    : 60
  RPI0 to RPI7 density                 : 3 7 11 19 15 23 15 7
Frame report entry:
  BSSID                                : a072-2351-e253
  PHY type                             : fhss
  Average RCPI                         : -10 dBm
  Last RSNI                            : 2 dBm
  Last RCPI                            : -20 dBm
  Frames                               : 1
Dot11BSSAverageAccessDelay group:
  Average access delay                 : 32 ms
  BestEffort average access delay      : 1 ms
  Background average access delay      : 1 ms
  Video average access delay           : 1 ms
  Voice average access delay           : 1 ms
  Clients                              : 32
  Channel utilization rate             : 11
Transmit stream:
  Traffic ID                           : 0
  Sent MSDUs                           : 60
  Discarded MSDUs                      : 5
  Failed MSDUs                         : 3
  MSDUs resent multiple times          : 3
  Lost QoS CF-Polls                    : 2
  Average queue delay                  : 2 ms
  Average transmit delay               : 1 ms
  Bin0 range                           : 0 to 10 ms
  Bin0 to Bin5                         : 5 10 10 5 10 10
```

表 11-1 コマンド出力

Field	Description
Link margin	受信したRSSIと最低の利用可能なRSSIとの間のギャップ。
RCPI	受信チャネル電力インジケータ。
RSNI	受信信号対雑音インジケータ。
ANPI	測定中の平均雑音電力インジケータ。
IPI0 to IPI10 density	測定期間全体に対する異なるIPI範囲の時間の割合。 IPInはIPI範囲を表します。nの値は1～10の範囲です。 • **0**: IPI <= –92 dBm. • **1**: –92 dBm < IPI <= –89 dBm. • **2**: –89 dBm < IPI <= –86 dBm. • **3**: –86 dBm < IPI <= –83 dBm. • **4**: –83 dBm < IPI <= –80 dBm. • **5**: –80 dBm < IPI <= –75 dBm • **6**: –75 dBm < IPI <= –70 dBm. • **7**: –70 dBm < IPI <= –65 dBm. • **8**: –65 dBm < IPI <= –60 dBm. • **9**: –60 dBm < IPI <= –55 dBm. • **10**: –55 dBm < IPI.
Transmit power	クライアントの送信電力。
BSS	クライアントが他のBSSからの無線パケットを検出したかどうか。
OFDM preamble	クライアントがOFDMプリアンブルを検出したかどうか。
Radar	クライアントがレーダー信号を検出したかどうか。
Unidentified signal	クライアントが未知の信号を検出したかどうか。
CCA busy fraction	全測定期間に対するチャネルのビジー時間の割合。
RPI0 to RPI7 density	測定期間全体に対するRPIの範囲が異なる時間の割合。 RPInはRPI範囲を表します。nの値は1～7の範囲です。 • **0**: RPI <= –87 dBm. • **1**: –87 dBm < RPI <= –82 dBm. • **2**: –82 dBm < RPI <= –77 dBm. • **3**: –77 dBm < RPI <= –72 dBm. • **4**: –72 dBm < RPI <= –67 dBm.

Field	Description
	● **5**: –67 dBm < RPI <= –62 dBm. ● **6**: –62 dBm < RPI <= –57 dBm. ● **7**: –57 dBm < RPI.
PHY type	物理メディアの種類 ● fhss. ● dsss. ● irbaseband. ● ofdm. ● hrdsss. ● erp.
Frames	測定中の同じMACアドレスとBSSIDからのフレーム数。
Bin0 range	Bin0の値の範囲。
Bin0 to Bin5	平均遅延範囲ごとに正常に送信されたMSDUの数。 Binxは平均遅延範囲を表します。xの値は0～5の範囲です。 ● **Bin0**: Delay< 10 ms. ● **Bin1**: 10 ms <= Delay < 20 ms. ● **Bin2**: 20 ms <= Delay < 40 ms. ● **Bin3**: 40 ms <= Delay < 80 ms. ● **Bin4**: 80 ms <= Delay < 160 ms. ● **Bin5**: 160 ms <= Delay.

11.1.2 measure

🕮 **メモ：**

spectrum、**tpc** パラメータはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

measure { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **disable** | **enable** }

undo measure

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: すべての測定機能を指定します。

link: リンク測定を指定します。リンク測定は、要求されたリンクの RCPI、RSNI、リンク冗長性を測定します。

neighbor: 隣接測定を指定します。近隣測定は、隣接 AP のチャネルおよび BSSID を測定します。

radio: 無線測定を指定します。無線測定は、チャネル負荷、雑音ヒストグラム、ビーコン、フレーム、station 統計、位置、送信ストリームを測定します。

spectrum: スペクトル測定を指定します。スペクトル測定は、基本測定、CCA 測定（Clear Channel Assessment）、RPI 測定（Receive Power Indication）を実施します。

tpc: TPC 測定を指定します。TPC 測定は、リンク冗長性とクライアントへの送信電力を測定します。

disable: 指定された測定機能またはすべての測定機能を無効にします。

enable: 指定された測定機能またはすべての測定機能を有効にします。

説明

measure enable コマンドは指定された測定機能またはすべての測定機能を有効にします。

measure disable コマンドは指定された測定機能またはすべての測定機能を無効にします。

undo measure コマンドはデフォルトに戻します。

link、**neighbor**、**radio** を有効にする場合は、**resource-measure** コマンドを有効にする必要があります。

spectrum、**tpc** を有効にする場合は、**spectrum-management** コマンドを有効にする必要があります。**spectrum-management** コマンドの詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC コマンドマニュアルの”*WLAN RRM*”を参照してください。

spectrum、**tpc** は 5GHz のラジオでのみ使用できます。

例

AP ap1 の spectrum 測定を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] measure spectrum enable

AP group apgroup1 の spectrum 測定を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure spectrum enable

関連コマンド

- **measure-duration**
- **measure-interval**
- **resource-measure**
- **spectrum-management**

11.1.3 measure-duration

Syntax

measure-duration *time*

undo measure-duration

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：500 TU

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

time: 測定期間を指定します。設定範囲は 1～10000TU です。1TU=1024 マイクロ秒です。

説明

measure-duration コマンドは測定期間を設定します。

undo measure-duration コマンドはデフォルトに戻します。

AP で測定が有効になると、AP からクライアントへの測定要求により測定期間を通知します。

例

AP ap1 の測定期間を 512TU に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] measure-duration 512

AP group apgroup1 の測定期間を 512TU に指定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure-duration 512

関連コマンド

- **measure**
- **measure-interval**

11.1.4 measure-interval

Syntax

measure-interval *value*

undo measure-interval

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：30 秒

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

value: 測定間隔を指定します。設定範囲は 1～60 秒です。

説明

measure-interval コマンドは AP が測定要求をクライアントに送信するための測定間隔を設定します。

undo measure-interval コマンドはデフォルトに戻します。

例

AP ap1 の測定間隔を 35 秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] measure-interval 35

AP group apgroup1 の測定間隔を 35 秒に指定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure-interval 35

関連コマンド

- **measure**
- **measure-duration**

11.1.5 resource-measure

Syntax

resource-measure { **disable** | **enable** }

undo resource-measure

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 無線リソース測定を無効にします。

enable: 無線リソース測定を有効にします。

説明

resource-measure enable コマンドは無線リソース測定を有効にします。

resource-measure disable コマンドは無線リソース測定を無効にします。

undo resource-measure コマンドはデフォルトに戻します。

AP で無線測定を有効にすると、AP はビーコン、プローブ応答、アソシエーション応答、再アソシエーション応答の Radio Measurement フィールドを 1 に設定し、計測要求を送信できることをクライアントに通知します。また、このフレームで、AP がサポートする計測タイプをクライアントに通知します。

AP は定期的に Measurement Pilot フレームを送信して、クライアントが AP を高速に検出できるようにします。Measurement Pilot フレームは、ビーコンよりも頻繁に送信され、より少ない情報しか運びません。

例

AP ap1 の無線資源計測を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] resource-measure enable

AP group apgroup1 の無線資源計測を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] resource-measure enable

11.1.6 rm-capability mode

Syntax

rm-capability mode { **all** | **none** | **partial** }

undo rm-capability mode

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントは、すべての無線資源計測機能が AP の無線資源計測機能と一致する場合にのみ、AP に接続することができます。

none: none モードを指定します。AP はクライアントの無線資源計測機能をチェックしません。

partial: 部分モードを指定します。クライアントは、少なくとも 1 つの無線資源計測機能が AP の無線資源計測機能と一致する場合、AP に接続することができます。

説明

rm-capability mode コマンドはクライアント無線資源計測機能の一致モードを設定します。

undo rm-capability mode コマンドはデフォルトに戻します。

この設定は、無線資源計測が有効な場合にのみ有効です。

例

AP ap1 のクライアント無線資源計測機能を部分モードに指定します

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] resource-measure enable

[AC-wlan-ap-ap1-radio-2] rm-capability mode partial

AP group apgroup1.のクライアント無線資源計測機能を部分モードに指定します

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] rm-capability mode partial

関連コマンド

resource-measure

目次

12 章 チャネルスキャンの設定 12-1
12.1 チャネルスキャンの設定コマンド 12-1
12.1.1 scan channel blacklist 12-1
12.1.2 scan channel whitelist 12-2
12.1.3 scan idle-time 12-3
12.1.4 scan max-service-time 12-4
12.1.5 scan scan-time 12-6
12.1.6 scan work-channel-only 12-7

12章 チャネルスキャンの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

12.1 チャネルスキャンの設定コマンド

12.1.1 scan channel blacklist

Syntax

scan channel blacklist *channel-list*

undo scan channel blacklist { *channel-list* | **all** }

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view では、チャネルスキャンブラックリストは存在しません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channel-list: チャネル番号を指定します。設定範囲は 1～165 です。

all: チャネルスキャンブラックリストのすべてのチャネルを指定します。

説明

scan channel blacklist コマンドはチャネルスキャンブラックリストを設定します。

undo scan channel blacklist コマンドは指定したチャネルをチャネルスキャンブラックリストから削除します。

AP のチャネルスキャンブラックリストを設定すると、AP はブラックリストのチャネルをスキャンしません。同じ AP のチャネルスキャンブラックリストとホワイトリストの両方を設定することはできません。チャネルスキャンブラックリストを設定する前に、チャネルスキャンホワイトリストのすべてのチャネルを削除してください。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP1 のチャネルスキャンブラックリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap 1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] scan channel blacklist 1 6

AP グループ 10 のモデル **QX-W1020** の AP のチャネルスキャンブラックリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-2] scan channel blacklist 1 6

12.1.2 scan channel whitelist

Syntax

scan channel whitelist *channel-list*

undo scan channel whitelist { *channel-list* | **all** }

デフォルト

Radio view では、無線は AP group radio view の設定を使用します

AP group radio view では、チャネルスキャンホワイトリストは存在しません。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

channel-list: チャネル番号を指定します。設定範囲は 1～165 です。

all: チャネルスキャンホワイトリストのすべてのチャネルを指定します。

説明

scan channel whitelist コマンドはチャネルスキャンホワイトリストを設定します。

undo scan channel whitelist コマンドは指定したチャネルをチャネルスキャンホワイトリストから削除します。

AP のチャネルスキャンホワイトリストを設定すると、AP はホワイトリスト内のチャネルだけをスキャンします。同じ AP のチャネルスキャンブラックリストとホワイトリストの両方を設定することはできません。チャネルスキャンホワイトリストを設定する前に、チャネルスキャンブラックリストのすべてのチャネルを削除してください。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP1 のチャネルスキャンホワイトリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap 1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] scan channel whitelist 1 6

AP グループ 10 のモデル **QX-W1020** の AP のチャネルスキャンホワイトリストにチャネル 1 と 6 を追加します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-2] scan channel whitelist 1 6

12.1.3 scan idle-time

Syntax

scan idle-time *idle-time*

undo scan idle-time

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、サービスアイドルタイムアウトは 100 ミリ秒です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

idle-time: サービスアイドルタイムアウトを指定します。設定範囲は 60～5000 ミリ秒です。最大サービス期間より長く設定することはできません。

説明

scan idle-time コマンドはサービスアイドルタイムアウトを設定します。

undo scan idle-time コマンドはデフォルトに戻します。

AP は、サービス期間中、指定したサービスアイドルタイムアウトが切れても、現在のサービス期間がスキャン期間を超えるまで、新しいスキャン期間を開始しません。

サービスアイドルタイムアウトは、ビーコン間隔の倍数でなければなりません。ビーコン間隔より小さいサービスアイドルタイムアウトを設定すると、ビーコン間隔値をサービスアイドルタイムアウトとして使用します。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP 1 のサービスアイドルタイムアウトを 500 ミリ秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] scan idle-time 500

AP グループ 10 のモデル **QX-W1020** の AP のサービスアイドルタイムアウトタイマーを 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan idle-time 500

関連コマンド

beacon interval

12.1.4 scan max-service-time

Syntax

scan max-service-time { *max-service-time* | **no-limit** }

undo scan max-service-time

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、最大サービス期間はソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.19 を含む以前のソフトウェアでは 5000 ミリ秒です。

ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでは no-limit です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

max-service-time: 最大サービス期間を指定します。設定範囲は 100～5000 ミリ秒です。AP の最大サービス期間に達すると、AP は転送するトラフィックがあるかどうかにかかわらず、スキャン期間を開始します。

no-limit: 無線がサービス期間を制限しないように設定します。 無線サービスの品質を確保するには、このキーワードを指定します。サービスアイドルタイムアウトが切れるまで、AP はスキャン期間を開始しません。

Radio view の設定は、AP group radio view の設定よりも優先されます。

説明

scan max-service-time コマンドは最大サービス期間を設定します。

undo scan max-service-time コマンドはデフォルトに戻します。

例

AP 1 の最大サービス期間を 3000 ミリ秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model WA4320i-ACN

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] scan max-service-time 3000

AP グループ 10 のモデル **QX-W1020** の AP の最大サービス期間を 3000 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan max-service-time 3000

12.1.5 scan scan-time

Syntax

scan scan-time *scan-time*

undo scan scan-time

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、スキャン時間は 100 ミリ秒です。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

scan-time: スキャン時間を指定します。設定範囲は 100～5000 ミリ秒です。スキャン期間は最大サービス期間より長くすることはできません。

説明

scan scan-time コマンドはスキャン時間を設定します。

undo scan scan-time コマンドはデフォルトに戻します。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

AP 1 のスキャン期間を 500 ミリ秒に指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] scan scan-time 500

AP グループ 10 のモデル QX-W1020 の AP のスキャン時間を 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1020

[AC-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan scan-time 500

12.1.6 scan work-channel-only

Syntax

scan work-channel-only { **disable** | **enable** }

undo scan work-channel-only

デフォルト

Radio view では、無線は AP group radio view の設定を使用します。

AP group radio view では、AP はサポートされたすべてのチャネルを順にスキャンします。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: 作動チャネルのみのスキャンを無効にします。

enable: 作動チャネルのみのスキャンを有効にします。

説明

scan work-channel-only enable コマンドは作動チャネルのみのスキャンを有効にします。

scan work-channel-only disable コマンドは作動チャネルのみのスキャンを無効にします。

undo work-channel-only コマンドはデフォルトに戻します。

Radio view の設定は、AP group radio view の設定よりも優先されます。

例

作動チャネルのみをスキャンするように AP **ap1** を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] scan work-channel-only enable

作動チャネルのみをスキャンするように AP グループ 1 のモデル **QX-W1020** を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-1-ap-model-QX-W1020 -radio-2] scan work-channel-only enable

目次

13 章 バンドナビゲーションの設定.....13-1
13.1 バンドナビゲーションの設定コマンド.....13-1
13.1.1 band-navigation.....13-1
13.1.2 wlan band-navigation aging-time.....13-2
13.1.3 wlan band-navigation balance access-denial.....13-3
13.1.4 wlan band-navigation balance session.....13-4
13.1.5 wlan band-navigation enable.....13-5
13.1.6 wlan band-navigation rssi-threshold.....13-6

13章 バンドナビゲーションの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

13.1 バンドナビゲーションの設定コマンド

13.1.1 band-navigation

Syntax

band-navigation { **disable** | **enable** }

undo band-navigation

デフォルト

AP view：AP group view の設定を使用します。

AP group view：有効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: AP または AP グループのバンドナビゲーションを無効にします。

enable: AP または AP グループのバンドナビゲーションを有効にします。

説明

band-navigation enable コマンドは AP または AP グループのバンドナビゲーションを有効にします。

band-navigation disable コマンドは AP または AP グループのバンドナビゲーションを無効にします。

undo band-navigation コマンドはデフォルトに戻します。

バンドナビゲーションは、グローバル、AP いずれの場合も、本コマンドを有効後、動作します。

例

AP ap1 のバンドナビゲーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] band-navigation enable

AP group 1 のバンドナビゲーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] band-navigation enable

[AC-wlan-ap-ap1-radio-1] scan idle-time 500

関連コマンド

wlan band-navigation enable

13.1.2 wlan band-navigation aging-time

Syntax

wlan band-navigation aging-time *aging-time*

undo wlan band-navigation aging-time

デフォルト

180 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: クライアント情報のエージングタイムを指定します。設定範囲は 10～600 秒です。

説明

wlan band-navigation aging-time コマンドはクライアント情報のエージングタイムを設定します。

undo wlan band-navigation aging-time コマンドはデフォルトに戻します。

AP がクライアントからアソシエーション要求を受信すると、AP はクライアントの情報を記録し、クライアント情報エージングタイマを開始します。エージングタイマが満了する前に AP がプローブ要求またはアソシエーション要求をクライアントから受信する場合、AP はクライアント情報を更新し、エージングタイマをリセットします。AP がエージングタイマ満了前にクライアントからプローブ要求またはアソシエーション要求を受信しない場合、AP はクライアントの情報を削除します。

適切なクライアント情報のエージングタイムを設定して、クライアントの関連付けとシステムリソースの効率性を確保します。

例

クライアント情報のエージングタイムを 50 秒に指定します。

<AC> system-view

[AC] wlan band-navigation aging-time 50

13.1.3 wlan band-navigation balance access-denial

Syntax

wlan band-navigation balance access-denial *access-denial*

undo wlan band-navigation balance access-denial

デフォルト

AP は 5GHz または 2.4GHz アソシエーション要求を拒否しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

access-denial: 5GHz または 2.4GHz アソシエーション要求の最大拒否回数を指定します。設定範囲は 1～10 回です。

説明

wlan band-navigation balance access-denial コマンドは 5GHz または 2.4GHz アソシエーション要求の最大拒否回数を設定します。

undo wlan band-navigation balance access-denial コマンドはデフォルトに戻します。

クライアントの 5GHz または 2.4GHz アソシエーション要求の拒否回数が指定した最大拒否回数になると、AP はクライアントのアソシエーション要求を受け入れます。

このコマンドは、5GHz と 2.4GHz の両方の接続で有効です。

band-navigation は、最初は 5GHz での接続を優先するので、2.4GHz アソシエーション要求を拒否する回数となります。

その後、GAP 数などの設定により、2.4GHz での接続を優先する状態になると、5GHz アソシエーション要求を拒否する回数となります。

例

5GHz または 2.4GHz アソシエーション要求の最大拒否回数を 5 回に指定します。

<AC> system-view

[AC] wlan band-navigation balance access-denial 5

13.1.4 wlan band-navigation balance session

Syntax

wlan band-navigation balance session *session* [**gap** *gap*]

undo wlan band-navigation balance session

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

session: 5GHz の無線クライアント数のしきい値を指定します。設定範囲は 2～120 です。

gap: 5GHz と最も少ない無線のクライアント数の差のしきい値を指定します。設定範囲は 1～8 で、デフォルト値は 4 です。

説明

wlan band-navigation balance session コマンドはバンドナビゲーションのロードバランスを設定します。

undo wlan band-navigation balance session コマンドはデフォルトに戻します。

AC は、バンドナビゲーションを有効にしてもロードバランスを有効にしない場合、デュアルバンドクライアントを 5GHz 無線に誘導します。

AP は、次の条件が満たされた場合にクライアントの 5GHz アソシエーション要求を拒否します。

- 5GHz 無線のクライアント数が、指定したしきい値に達した場合。

- 5GHz 無線のクライアント数と最も少ない無線クライアント数との差が、指定したしきい値に達した場合。

例

バンドナビゲーションの負荷分散を有効にし、クライアント数のしきい値である、session、gap をそれぞれ 10 と 5 に設定します。

<AC> system-view

[AC] wlan band-navigation balance session 10 gap 5

13.1.5 wlan band-navigation enable

Syntax

wlan band-navigation enable

undo wlan band-navigation enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan band-navigation enable コマンドはバンドナビゲーションをグローバルで有効にします。

undo wlan band-navigation enable コマンドはデフォルトに戻します。

バンドナビゲーションが動作するには、ワイヤレスサービステンプレートの高速アソシエーションが無効になっている必要があります。

バンドナビゲーションは、グローバル、AP 両方でこのコマンドが有効の場合のみ動作します。

例

グローバルバンドナビゲーションを有効にします。

<AC> system-view

[AC] wlan band-navigation enable

関連コマンド

- **band-navigation**

- **quick-association enable**

13.1.6 wlan band-navigation rssi-threshold

Syntax

wlan band-navigation rssi-threshold *rssi-threshold*

undo wlan band-navigation rssi-threshold

デフォルト

15

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: バンドナビゲーションの RSSI しきい値を指定します。設定範囲は 5～100 です。

説明

wlan band-navigation rssi-threshold コマンドはバンドナビゲーションの RSS（Received Signal Strength Indicator）しきい値を設定します。

undo wlan band-navigation rssi-threshold コマンドはデフォルトに戻します。

複数の無線でクライアントを検出する可能性があります。5GHz 無線は、クライアントの RSSI がバンドナビゲーション RSSI しきい値よりも低い場合、クライアントのアソシエーション要求を拒否します。

例

バンドナビゲーションの RSSI しきい値を 40 に指定します。

<AC> system-view

[AC] wlan band-navigation rssi-threshold 40

目次

14 章 WLAN 最適化 14-1
14.1 WLAN 最適化コマンド 14-1
14.1.1 option broadcast-multicast-buffer 14-1
14.1.2 option client hide-node-protection 14-2
14.1.3 option client reconnect 14-3
14.1.4 option keep-active 14-5
14.1.5 rrop anti-bmc network 14-6
14.1.6 rrop anti-bmc rate-limit 14-8
14.1.7 rrop anti-bmc rate-limit pps 14-9
14.1.8 rrop client fast-keep-alive 14-10

14章 WLAN 最適化

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

14.1 WLAN最適化コマンド

14.1.1 option broadcast-multicast-buffer

Syntax

option broadcast-multicast-buffer { **disable** | **enable** [**limit** *limit*] }

undo option broadcast-multicast-buffer

デフォルト

Radio view：AP group radio view の設定を使用します。

AP group radio view：有効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: マルチキャストとブロードキャストのバッファを無効にします。

enable: マルチキャストとブロードキャストのバッファを有効にします。

limit *limit*: マルチキャストパケットもしくはブロードキャストパケットをバッファできる最大数を指定します。値の範囲は 1～600 です。デフォルトの値は 100 です。

説明

option broadcast-multicast-buffer enable コマンドはマルチキャストとブロードキャストのバッファを有効にします。

option broadcast-multicast-buffer disable コマンドはマルチキャストとブロードキャストのバッファを無効にします。

undo option broadcast-multicast-buffer コマンドはデフォルトに戻します。

この機能を有効にすると、関連付いたクライアントがスリープモードになった場合、ACはブロードキャストパケットとマルチキャストパケットの送信を停止し、これらのパケットをバッファします。

この機能を無効にすると、関連付いたクライアントがスリープモードであるかどうかにかかわらず、AC はすべてのブロードキャストパケットとマルチキャストパケットをクライアントに直接送信します。

limit の引数の値をデフォルトで使用する場合、**limit** *limit* を指定せずに **option broadcast-multicast-buffer enable** コマンドを設定してください。

例

ap1 でマルチキャストとブロードキャストのバッファを無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option broadcast-multicast-buffer disable

AP group 1 の **QX-W1020** でマルチキャストとブロードキャストのバッファを無効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option broadcast-multicast-buffer disable

14.1.2 option client hide-node-protection

Syntax

option client hide-node-protection { **disable** | **enable** }

undo option client hide-node-protection

デフォルト

Radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

パラメータ

disable: 隠れ端末保護を無効にします。

enable: 隠れ端末保護を有効にします。

説明

option client hide-node-protection enable コマンドは隠れ端末保護を有効にします。

option client hide-node-protection disable コマンドは隠れ端末保護を無効にします。

undo option client hide-node-protection コマンドはデフォルトに戻します。

このコマンドは、802.11g、802.11n、および 802.11ac/ax クライアントにのみ適用可能です。

この機能を有効にすると、クライアントは隠れ端末からの干渉を避けるために RTS/CTS フレームを送信します。

本機能によって複数端末の通信衝突を軽減させることが可能です。

Radio view での設定は、AP group radio view での設定より優先されます。

例

AP**ap1** に対して隠れ端末保護を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option client hide-node-protection enable

AP group 1 の **QX-W1020** に対して隠れ端末保護を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option client hide-node-protection enable

14.1.3 option client reconnect

Syntax

option client reconnect { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] }

undo option client reconnect

デフォルト

Radio view：AP group radio view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

パラメータ

disable: AP トリガのクライアント再関連付けを無効にします。

enable: AP トリガのクライアント再関連付けを有効にします。

rssi *rssi-value*: RSSI しきい値を 5～100 の範囲で指定します。RSSI しきい値のデフォルト値および推奨値は、それぞれ 10 と 20 です。

interval *interval*: AP がクライアントの信号強度を検出する間隔を 3～10 秒の範囲で指定します。デフォルト設定は 3 秒です。

説明

option client reconnect enable コマンドは AP トリガのクライアント再関連付けを有効にします。

option client reconnect disable コマンドは AP トリガのクライアント再関連付けを無効にします。

undo option client reconnect コマンドはデフォルトに戻します。

この機能により、クライアントの信号強度が指定した RSSI しきい値よりも小さいと AP が検知したとき、AP は再認証フレームをクライアントに送信できます。再認証フレームを受信したクライアントは、AP に再関連付け、あるいは別の AP にローミングできます。

Radio view での設定は、AP group radio view での設定より優先されます。

例

#AP トリガのクライアント再関連付けを **ap1** で有効にします。RSSI しきい値を 30、検出間隔を 5 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option client reconnect enable rssi 30 interval 5

#AP トリガのクライアント再関連付けを AP **ap1** で有効にします。RSSI しきい値を 30、検出間隔を 5 秒に設定します。

AP トリガのクライアント再関連付けを AP group 1 の **QX-W1020** で有効にします。RSSI しきい値を 30、検出間隔を 5 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option client reconnect enable rssi 30 interval 5

14.1.4 option keep-active

Syntax

option keep-active { disable | enable }

undo option keep-active

デフォルト

Radio view : : AP グループの設定を引き継ぎます。

AP group の radio view：無効。

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

説明

option keep-active enable コマンドは無線クライアントのスリープ時間を短縮する機能を有効にします。

option keep-active disable コマンドは、無線クライアントのスリープ時間を短縮する機能を無効にします。

undo option keep-active コマンドはデフォルトに戻します。

スリープ状態の無線クライアントは、ビーコンフレーム内の TIM（トラフィック通知メッセージ）情報を定期的にリスニングすることで、接続している AP が無線クライアントのパケットをバッファしているかどうかを判断します。AP が無線クライアントのパケットをバッファしている場合、スリープ状態は終了し、AP とデータ通信を行います。本機能を有効にすると、AP はビーコンフレーム内の TIM を変更し、端末のスリープ時間を短縮して、伝送効率を向上させます。

例

ap1 で無線クライアントのスリープ時間短縮機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1120

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option keep-active enable

apgroup1 でクライアントのスリープ時間短縮機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1120

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] option keep-active enable

14.1.5 rrop anti-bmc network

🕮 **メモ：**

- **rrop anti-bmc network** コマンドはソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。
- **rrop anti-bmc network** コマンドは Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
  QX-W1030 Anchor-AC/Anchor-FIT ではサポートしていません。

Syntax

rrop anti-bmc network { disable | ipv4-simple enable }

undo rrop anti-bmc network

デフォルト

AP view：AP group view の設定を使用します。

AP group view：ソフトウェアバージョンにより異なります。

ソフトウェアバージョン V7.2.50 を含む以前のソフトウェアでは有効です。

ソフトウェアバージョン V7.2.52 を含む以降のソフトウェアでは無効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: ブロードキャストパケットおよびマルチキャストパケットの制御を無効にします

ipv4-simple enable: ブロードキャストパケットおよびマルチキャストパケットの制御を有効にします

説明

rrop anti-bmc network disable コマンドはブロードキャストパケットおよびマルチキャストパケットの制御を無効にします。

rrop anti-bmc network ipv4-simple enable コマンドはブロードキャストパケットおよびマルチキャストパケットの制御を有効にします。

undo rrop anti-bmc network コマンドはデフォルトに戻します。

IPv4 ネットワークで基本的なブロードキャストおよびマルチキャストパケットを制御します。本機能を有効にすると、AP は ARP ブロードキャストパケットに応答し、DHCP ブロードキャストパケットを廃棄し、他のパケットを正常に処理します。

例

#ブロードキャストパケットおよびマルチキャストパケットの制御を ap1 で有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc network ipv4-simple enable

#マルチキャストパケットのレート制限を AP group 1 で有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc network ipv4-simple enable

14.1.6 rrop anti-bmc rate-limit

🕮 メモ：

- **rrop anti-bmc rate-limit** コマンドはソフトウェアバージョン 7.2.50 を含む以降のソフトウェアからサポートしています。
- **rrop anti-bmc rate-limit** コマンドは Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
  QX-W1030 Anchor-AC/Anchor-FIT ではサポートしていません。

Syntax

rrop anti-bmc { broadcast | multicast } rate-limit { disable | enable }

デフォルト

AP view：AP group view の設定を使用します。

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

broadcast: ブロードキャストパケットのレート制限を設定します

multicast: マルチキャストパケットのレート制限を設定します

説明

rrop anti-bmc rate-limit enable コマンドはブロードキャストまたはマルチキャストパケットのレート制限を有効にします。

rrop anti-bmc rate-limit disable コマンドはブロードキャストまたはマルチキャストパケットのレート制限を無効にします。

undo rrop anti-bmc rate-limit コマンドはデフォルトに戻します。

例

#ブロードキャストパケットのレート制限を ap1 で有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc broadcast rate-limit enable

#マルチキャストパケットのレート制限を AP group 1 で有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc multicast rate-limit enable

14.1.7 rrop anti-bmc rate-limit pps

🕮 **メモ：**

- **rrop anti-bmc rate-limit pps** コマンドはソフトウェアバージョン 7.2.50 を含む以降のソフトウェアからサポートしています。
- **rrop anti-bmc rate-limit pps** コマンドは Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
  QX-W1030 Anchor-AC/Anchor-FIT ではサポートしていません。

Syntax

rrop anti-bmc { broadcast | multicast } rate-limit pps *max-pps*

undo rrop anti-bmc { broadcast | multicast } rate-limit pps

デフォルト

AP view：AP group view の設定を使用します。

AP group view：AP が 1 秒あたりに送信できるブロードキャストまたはマルチキャストパケットの最大数は指定されていません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

broadcast: 1 秒間に送信可能なブロードキャストパケットの最大数を設定します

multicast: 1 秒間に送信可能なブロードキャストパケットの最大数を設定します

max-pps: AP が 1 秒あたりに送信できるブロードキャストまたはマルチキャストパケットの最大数を 1～1410000 の範囲で指定します。AP は、指定された制限を超えるブロードキャストまたはマルチキャストパケットを破棄します。

説明

rrop anti-bmc rate-limit pps コマンドはブロードキャストまたはマルチキャストパケットの 1 秒間に送信できる最大数を設定します。

undo rrop anti-bmc rate-limit pps コマンドはデフォルトに戻します。

このコマンドは、rrop **anti-bmc rate-limit enable** が設定されている場合のみ有効です。

例

ap1 でブロードキャストパケットを 1 秒間に最大 200 個に制限します

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc broadcast rate-limit pps 200

#AP group 1 でマルチキャストパケットを 1 秒間に最大 200 個に制限します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc multicast rate-limit pps 200

14.1.8 rrop client fast-keep-alive

🕮 **メモ：**

- **rrop client fast-keep-alive** コマンドはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。ソフトウェアバージョン 7.2.85a 以前は本機能がデフォルトのパラメータ値で動作しており、無効にすることはできません。
- **rrop client fast-keep-alive** コマンドは Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。QX-W1030 Anchor-AC ではサポートしていません。

Syntax

rrop client fast-keep-alive { **disable** | **enable** [**count** *count-value*] [**interval** *interval-value*]}

undo rrop client fast-keep-alive

デフォルト

AP view：AP group radio view の設定を使用します。

AP group radio view：有効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

count *count-value*: AP がクライアントに送信できるキープアライブパケットの最大数を 128～2048 の範囲で指定します。デフォルト値は 1024 です。

interval *interval-value*: キープアライブ間隔を 3~60 秒の範囲で指定します。デフォルト値は 10 です。

説明

rrop client fast-keep-alive enable コマンドはクライアント高速キープアライブを有効にします。

rrop client fast-keep-alive disable コマンドはクライアント高速キープアライブを無効にします。

undo rrop client fast-keep-alive コマンドはデフォルトに戻します。

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。AP はユーザーデータを 3 つのグループに分けて個別にカウントします。キープアライブ間隔 (interval-value パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、count-value パラメータで設定します。

この機能は、クライアントの移動性が高いシナリオに適用できます。ネットワーク品質が悪い場合は、キープアライブカウントを減らすか、キープアライブ間隔を短くしてください。

Radio view での設定は、AP group radio view での設定より優先されます。

例

ap1 でクライアント高速キープアライブを有効にし、最大値を 300 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrop client fast-keep-alive enable count 300

関連コマンド

client keep-alive

目次

15 章 WLAN IP スヌーピング 15-1
15.1 WLAN IP スヌーピングコマンド 15-1
15.1.1 client ipv4-snooping arp-learning enable 15-1
15.1.2 wlan client ip-conflict-detection enable..... 15-2

15章 WLAN IP スヌーピング

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

15.1 WLAN IPスヌーピングコマンド

15.1.1 client ipv4-snooping arp-learning enable

Syntax

client ipv4-snooping arp-learning enable

undo client ipv4-snooping arp-learning enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

client ipv4-snooping arp-learning enable コマンドは ARP パケットのスヌーピングを有効にします。

undo client ipv4-snooping arp-learning enable コマンドは ARP パケットのスヌーピングを無効にします。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

ARP パケットのスヌーピングを無効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] undo client ipv4-snooping arp-learning enable

15.1.2 wlan client ip-conflict-detection enable

🕮 メモ：

undo wlan client ip-conflict-detection enable 実行時に IP アドレス競合検出された IP アドレスがある場合は、そのクライアントのキャッシュ情報がクリアされるまで、その IP アドレスの競合検出は行いません。クライアントのキャッシュ情報の保持時間は、**client cache aging-time** コマンドで設定した時間（初期値は 180 秒）です。

Syntax

wlan client ip-conflict-detection enable

undo wlan client ip-conflict-detection enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan client ip-conflict-detection enable コマンドは、IP アドレス競合検出機能を有効にします。

undo wlan client ip-conflict-detection enable コマンドは、IP アドレス競合検出機能を無効にします。

この機能により、システムはオンライン要求したクライアントと既にオンライン中のクライアントの間で IP アドレスの競合を検出することができます。システムはオンライン要求したクライアントと同じ IP アドレスを使用しているオンライン中のクライアントをログオフし、そのクライアント用に IP アドレス競合のエントリを作成します。クライアントのキャッシュが期限切れになるか、クライアントの IP アドレスが変更されると、システムはそのクライアントの IP アドレス競合エントリを削除します。

例

IP アドレス競合検出を無効にします。

<AC> system-view

[AC] undo wlan client ip-conflict enable

関連コマンド

client cache aging-time

目次

16 章 WLAN の高可用性の設定 16-1
16.1 デュアルリンクバックアップコマンド 16-1
16.1.1 backup-ac 16-1
16.1.2 priority 16-2
16.1.3 wlan tunnel-preempt 16-3

16章 WLAN の高可用性の設定

16.1 デュアルリンクバックアップコマンド

🕮 **メモ**:

本章のコマンドは V7.2.52 を含む以降のバージョンからサポートしています。
デュアルリンクバックアップの設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

16.1.1 backup-ac

Syntax

backup-ac ip *ipv4-address*

undo backup-ac ip

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、バックアップ AC は指定されていません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: IPv4 アドレスでバックアップ AC を指定します。

説明

backup ac コマンドはバックアップ AC を指定します。

undo backup ac コマンドデフォルトに戻します。

AP view または AP group view のどちらかで、1 つの IPv4 アドレスを指定することができます。

AP view の設定は、AP group view の設定に優先します。AP view で undo コマンドを実行した場合、AP group view で指定されたバックアップ AC が使用されます。

undo コマンドを実行すると、バックアップ CAPWAP トンネルも終了します。

例

AP ap1 でバックアップ AC を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] backup-ac ip 192.168.1.1

AP グループ group1 でバックアップ AC を指定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] backup-ac ip 192.168.1.1

16.1.2 priority

Syntax

priority *priority*

undo priority

デフォルト

AP view は、AP group view の設定を使用します。

AP group view は、AC の AP 接続優先度は 4 です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

priority: AC の AP 接続優先度を 0～7 の範囲で指定します。値が大きいほど接続優先度が高くなります。

説明

priority コマンドは AC の AP 接続優先度を設定します。

undo priority コマンドはデフォルトに戻します。

AP は、より高い接続優先度を有する AC と CAPWAP トンネルを優先して確立します。

AP 接続優先度は、AC ディスカバリ中にのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP **ap3** の AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1020

[AC-wlan-ap-ap3] priority 7

AP group **group1** の、AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] priority 7

16.1.3 wlan tunnel-preempt

Syntax

wlan tunnel-preempt { **disable** | **enable** }

undo wlan tunnel-preempt

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP は Global configuration view で設定を使用します。

Global configuration view では、マスタ CAPWAP トンネルプリエンプションは無効です。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: マスタ CAPWAP トンネルプリエンプションを無効にします。

enable: マスタ CAPWAP トンネルプリエンプションを有効にします。

説明

wlan tunnel-preempt enable コマンドはマスタ CAPWAP トンネルプリエンプションを有効にします。

wlan tunnel-preempt disable コマンドはマスタ CAPWAP トンネルプリエンプションを無効にします。

undo wlan tunnel-preempt コマンドはデフォルトに戻します。

wlan tunnel-preempt コマンドは、デュアルリンクバックアップを利用している環境において、優先度の高い AP との CAPWAP トンネルが切断されバックアップ AP との CAPWAP トンネルがマスタに切り替わった後、再度優先度の高い AP との CAPWAP トンネルが復旧した場合の動作を設定します。

この機能が有効な場合、高優先の AP との CAPWAP トンネルが復旧した際、10 分後にマスタに接続が切り戻ります。この機能が無効な場合、高優先の AP との CAPWAP トンネルが復旧しても、マスタに接続は切り戻りません。

例

AP **ap1** のマスタ CAPWAP トンネルプリエンプションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-ap-ap1] wlan tunnel-preempt enable

AP グループ **group1** の AP の CAPWAP トンネルプリエンプションを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] wlan tunnel-preempt enable

グローバルにマスタ CAPWAP トンネルプリエンプションを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan tunnel-preempt enable

目次

17 章 WLAN RRM 17-1
17.1 WLAN RRM コマンド 17-1
17.1.1 adjacency-factor 17-1
17.1.2 ap name 17-2
17.1.3 calibrate-bandwidth self-decisive 17-3
17.1.4 calibrate-channel mode 17-5
17.1.5 calibrate-channel monitoring time-range 17-6
17.1.6 calibrate-channel pronto 17-7
17.1.7 calibrate-channel self-decisive 17-8
17.1.8 calibrate-power 2.4g max 17-10
17.1.9 calibrate-power 2.4g coverage rssi-threshold 17-11
17.1.10 calibrate-power 2.4g coverage weak-signal-client ratio 17-12
17.1.11 calibrate-power 2.4g coverage weak-signal-client threshold 17-13
17.1.12 calibrate-power 2.4g coverage weak-signal-packet ratio 17-14
17.1.13 calibrate-power 2.4g coverage weak-signal-packet threshold 17-15
17.1.14 calibrate-power 5g max 17-17
17.1.15 calibrate-power 5g coverage rssi-threshold 17-18
17.1.16 calibrate-power 5g coverage weak-signal-client ratio 17-19
17.1.17 calibrate-power 5g coverage weak-signal-client threshold 17-20
17.1.18 calibrate-power 5g coverage weak-signal-packet ratio 17-21
17.1.19 calibrate-power 5g coverage weak-signal-packet threshold 17-22
17.1.20 calibrate-power coverage enable 17-24
17.1.21 calibrate-power min 17-26
17.1.22 calibrate-power mode 17-27
17.1.23 calibrate-power self-decisive 17-28
17.1.24 calibrate-power threshold 17-30
17.1.25 channel holddown-time 17-31
17.1.26 channel-capability mode 17-32
17.1.27 channel-switch mode 17-33
17.1.28 crc-error-threshold 17-34
17.1.29 description 17-36
17.1.30 display wlan rrm baseline 17-36
17.1.31 display wlan rrm baseline apply-result 17-39
17.1.32 display wlan rrm-calibration-group 17-40
17.1.33 display wlan rrm-history ap 17-41
17.1.34 display wlan rrm-status ap 17-43
17.1.35 interference-threshold 17-46

17.1.36 power holddown-time 17-47
17.1.37 power-capability mode 17-48
17.1.38 power-constraint mode 17-50
17.1.39 rrm 17-51
17.1.40 scan-only 17-52
17.1.41 snmp-agent trap enable wlan rrm 17-53
17.1.42 spectrum-management 17-54
17.1.43 tolerance-level 17-55
17.1.44 wlan calibrate-channel pronto ap all 17-56
17.1.45 wlan calibrate-power pronto ap all 17-57
17.1.46 wlan rrm baseline apply 17-57
17.1.47 wlan rrm baseline remove 17-58
17.1.48 wlan rrm baseline save 17-59
17.1.49 wlan rrm calibration-bandwidth interval 17-60
17.1.50 wlan rrm calibration-channel interval 17-61
17.1.51 wlan rrm-calibration-group 17-62
17.1.52 wlan rrm calibration-power interval 17-63

17章 WLAN RRM

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

17.1 WLAN RRMコマンド

17.1.1 adjacency-factor

Syntax

adjacency-factor *neighbor*

undo adjacency-factor

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：3(ソフトウェアバージョン 7.2.21 を含む以前)

1(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

neighbor: 1～16 の範囲内の隣接係数を指定します。

説明

adjacency-factor コマンドは隣接係数を設定します。

undo adjacency-factor コマンドはデフォルトに戻します。

隣接係数は、TPC をトリガする管理可能な検出された無線の量と、電力調整しきい値との比較に使用される RSSI の順位を定義します。AC はそれに関連付けられた無線だけを管理できます。

たとえば、隣接係数が 3 の場合、無線が 3 つの他の管理可能な無線を検出すると、AC は無線の TPC を実行します。他の管理可能な無線によって検出された無線の RSSI を降順

でランク付けした後、AC は電力調整しきい値と比較する 3 番目に大きい RSSI を選択します。

例

AP **ap1** の無線 1 に対して、隣接係数を 7 に設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] adjacency-factor 7

AP グループ **group1** の **QX-W1020** モデルを持つ AP の無線 1 に対して、隣接係数を 7 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] adjacency-factor 7

17.1.2 ap name

Syntax

ap name *ap-name* **radio** *radio-id*

undo ap { **name** *ap-name* [**radio** *radio-id*] | **all** }

デフォルト

設定なし

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

radio-id: ID で無線を指定します。この引数の値は 1 もしくは 2 です。1 つの RRM holddown group に属することができる無線は 1 つだけです。新たな RRM holddown group に無線を追加すると、既存の RRM holddown group からはその無線が削除されます。

all: すべての無線を指定します。

説明

ap name コマンドは RRM holddown group に無線を追加します。

undo ap name コマンドは RRM holddown group から 1 つまたはすべての無線を取り除きます。

例

ap 1 の radio 2 を RRM holddown group 10 に追加します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] ap name ap1 radio 2

17.1.3 calibrate-bandwidth self-decisive

🕮 **メモ：**

- このコマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。
- Global configuration view では、**disable** のパラメータを使用できません。

Syntax

calibrate-bandwidth self-decisive { **disable** | **enable** }

undo calibrate-bandwidth self-decisive

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：global configuration view の設定を使用します。

Global configuration view：無効

View

RRM view

AP group RRM view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: 帯域幅自動調整機能を無効にします。

enable: 帯域幅自動調整機能を有効にします。

説明

calibrate-bandwidth self-decisive enable コマンドは帯域幅自動調整を有効にします。

calibrate-bandwidth self-decisive disable コマンドは帯域幅自動調整を無効にします。

undo calibrate-bandwidth self-decisive コマンドはデフォルトに戻します。

帯域幅自動調整が有効の場合、AC は帯域幅自動調整間隔に達するとチャネル品質検出を開始し、帯域幅調整を実行するかどうかを決定します。ネイバ無線の数が多い場合は、干渉を減らすために無線の帯域幅を減らし、数が少ない場合は、伝送レートを増やすために帯域幅を増やします。

このコマンドは、5 GHz 無線でのみ有効です。

例

ap1 と名付けた AP の無線 1 に対して帯域幅自動調整を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-bandwidth self-decisive enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して帯域幅自動調整を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-bandwidth self-decisive enable

#グローバルで帯域幅自動調整を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-bandwidth self-decisive enable

17.1.4 calibrate-channel mode

Syntax

calibrate-channel mode { **periodic** | **scheduled** }

undo calibrate-channel mode

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、auto-DFS モードは定期的です。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

periodic: 定期的な auto-DFS を指定します。

scheduled: スケジュールされた auto-DFS を指定します。

説明

calibrate-channel mode コマンドは auto-DFS モードを設定します。

undo calibrate-channel mode コマンドはデフォルトに戻します。

定期的な auto-DFS モードでは、AC はチャネルキャリブレーション間隔で無線用の DFS を自動的に実行します。

スケジュールされた auto-DFS モードでは、AC は指定された時間間隔で DFS を実行します。干渉が深刻な場合、進行中の無線サービスに影響を与えないようにこのモードを使用します。

例

auto-DFS モードを AP **ap1** の無線 1 に**スケジュール**するように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel mode scheduled

auto-DFS モードを AP グループ **group1** のモデル **QX-W1020** を持つ AP の無線 1 に**スケジュール**するように設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel self-decisive enable

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel mode scheduled

関連コマンド

- **calibrate-channel monitoring time-range**
- **calibrate-channel pronto**
- **wlan rrm calibration-channel interval**

17.1.5 calibrate-channel monitoring time-range

Syntax

calibrate-channel monitoring time-range *time-range-name*

undo calibrate-channel monitoring time-range

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、チャネル監視の時間範囲が指定されていません。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

time-range-name: 時間範囲の名前を指定します。大文字と小文字を区別しない 1～32 文字です。文字列は文字で始める必要がありますが、all には設定できません。

説明

calibrate-channel monitoring time-range コマンドはチャネル監視の時間範囲を指定します。

undo calibrate-channel monitoring time-range コマンドはチャネル監視の時間範囲を削除します。

スケジュールされた auto-DFS では、AC は指定された時間範囲の統計情報を収集し、チャネルレポートとネイバーレポートを生成します。

例

AP **ap1** の無線 1 に対するチャネル監視の時間範囲を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel monitoring time-range time1

AP グループ **group1** のモデル **QX-W1020** の無線 1 に対するチャネル監視の時間範囲を指定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel monitoring time-range time1

関連コマンド

time-range

17.1.6 calibrate-channel pronto

Syntax

calibrate-channel pronto

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

説明

calibrate-channel pronto コマンドはスケジュールされた auto-DFS を実行します。

例

ジョブを作成し、AP **ap1** の無線 1 に対するジョブにコマンドを割り当てます。

<AC> system-view

[AC] scheduler job calibration1

[AC-job-calibration1] command 1 system-view

[AC-job-calibration1] command 2 wlan ap ap1

[AC-job-calibration1] command 3 radio 1

[AC-job-calibration1] command 4 rrm

[AC-job-calibration1] command 5 calibrate-channel pronto

ジョブを作成し、AP グループ **g1** のモデル **QX-W1020** を持つ AP の無線 1 に対するジョブにコマンドを割り当てます。

<AC> system-view

[AC] scheduler job calibration2

[AC-job-calibration2] command 1 system-view

[AC-job-calibration2] command 2 wlan ap-group g1

[AC-job-calibration2] command 3 ap-model QX-W1020

[AC-job-calibration2] command 4 radio 1

[AC-job-calibration2] command 5 rrm

[AC-job-calibration2] command 6 calibrate-channel pronto

17.1.7 calibrate-channel self-decisive

Syntax

calibrate-channel self-decisive { **disable** | **enable** }

undo calibrate-channel self-decisive

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：無効

View

RRM view

AP group RRM view

Global configuration view(ソフトウェアバージョン 7.2.24 以降のバージョンでサポート)

定義済みユーザロール

network-admin

パラメータ

disable: auto-DFS を無効にします。

enable: auto-DFS を有効にします。

説明

calibrate-channel self-decisive enable コマンドは auto-DFS を有効にします。

calibrate-channel self-decisive disable コマンドは auto-DFS を無効にします。

undo calibrate-channel self-decisive コマンドはデフォルトに戻します。

例

ap1 と名付けた AP の無線 1 に対して auto-DFS を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して auto-DFS を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel self-decisive enable

関連コマンド

calibrate-channel mode

17.1.8 calibrate-power 2.4g max

🕮 メモ：

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g max *tx-power*

undo calibrate-power 2.4g max

デフォルト

2.4GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 2.4g max コマンドは TPC 実行後の無線に対して最大送信電力を設定します。

undo calibrate-power 2.4g max コマンドはデフォルトに戻します。

このコマンドは、auto-TPC で設定できる無線の最大送信電力を設定します。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

2.4GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g max 15

17.1.9 calibrate-power 2.4g coverage rssi-threshold

> 🕮 メモ：
>
> このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage rssi-threshold *rssi*

undo calibrate-power 2.4g coverage rssi-threshold

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 2.4g coverage rssi-threshold コマンドは 2.4 GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

undo calibrate-power 2.4g coverage rssi-threshold コマンドはデフォルトに戻します。

例

2.4GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] calibrate-power 2.4g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**

- **calibrate-power coverage enable**

17.1.10 calibrate-power 2.4g coverage weak-signal-client ratio

> 🕮 **メモ**:
> このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-client ratio *percent*

undo calibrate-power 2.4g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 2.4g coverage weak-signal-client ratio コマンドは 2.4 GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、calibrate-power 2.4 g coverage weak-signal-client threshold コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

17.1.11 calibrate-power 2.4g coverage weak-signal-client threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-client threshold *counts*

undo calibrate-power 2.4g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 2.4g coverage weak-signal-client threshold コマンドは 2.4 GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 2.4g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

17.1.12 calibrate-power 2.4g coverage weak-signal-packet ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-packet ratio *percent*

undo calibrate-power 2.4g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 2.4g coverage weak-signal-packet ratio コマンドは 2.4 GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、calibrate-power 2.4 g coverage weak-signal-packet threshold コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

17.1.13 calibrate-power 2.4g coverage weak-signal-packet threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-packet threshold *counts*

undo calibrate-power 2.4g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 2.4g coverage weak-signal-packet threshold コマンドは 2.4 GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 2.4g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

17.1.14 calibrate-power 5g max

🕮 メモ：

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g max *tx-power*

undo calibrate-power 5g max

デフォルト

5GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 5g max コマンドは TPC 実行後の無線に対して最大送信電力を設定します。

undo calibrate-power 5g max コマンドはデフォルトに戻します。

このコマンドは、auto-TPC で設定できる無線の最大送信電力を設定します。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

5GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g max 15

17.1.15 calibrate-power 5g coverage rssi-threshold

> 🕮 メモ：
>
> このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage rssi-threshold *rssi*

undo calibrate-power 5g coverage rssi-threshold

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 5g coverage rssi-threshold コマンドは 5GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

undo calibrate-power 5g coverage rssi-threshold コマンドはデフォルトに戻します。

例

5GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] calibrate-power 5g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**

- **calibrate-power coverage enable**

17.1.16 calibrate-power 5g coverage weak-signal-client ratio

> 🕮 **メモ**:
> このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-client ratio *percent*

undo calibrate-power 5g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 5g coverage weak-signal-client ratio コマンドは 5GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、**calibrate-power 5g coverage weak-signal-client threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

17.1.17 calibrate-power 5g coverage weak-signal-client threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-client threshold *counts*

undo calibrate-power 5g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 5g coverage weak-signal-client threshold コマンドは 5GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 5g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

17.1.18 calibrate-power 5g coverage weak-signal-packet ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-packet ratio *percent*

undo calibrate-power 5g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 5g coverage weak-signal-packet ratio コマンドは 5GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、**calibrate-power 5g coverage weak-signal-packet threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

17.1.19 calibrate-power 5g coverage weak-signal-packet threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-packet threshold *counts*

undo calibrate-power 5g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 5g coverage weak-signal-packet threshold コマンドは 5GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 5g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

17.1.20 calibrate-power coverage enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

Syntax

Radio view または AP グループの Radio view:

calibrate-power coverage { disable | enable }

undo calibrate-power coverage

Global configuration View:

calibrate-power coverage enable { 2.4g | 5g | all }

undo calibrate-power coverage enable { 2.4g | 5g | all }

デフォルト

Radio view：AP group RRM view の設定を使用します。

AP group Radio view：global configuration view の設定を使用します。

Global configuration view：無効

View

Radio view

AP group Radio view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

all: 2.4GHz 無線と 5GHz 無線両方を指定します。

説明

calibrate-power coverage enable コマンドは死角検出を有効にします。

calibrate-power coverage disable コマンドは死角検出を無効にします。

undo calibrate-power coverage コマンドはデフォルトに戻します。

この機能により、AC は無線信号カバレッジに死角 (または弱い信号領域) が存在するかどうかを判断できます。死角が検出された場合、AC は auto-TPC を実行するときに対応する AP の送信電力を増加させます。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱い信号クライアントの数が、しきい値に達するか、または超えている場合。
- 無線に関連付けられた弱い信号クライアントの割合がしきい値に達するか、それを超えている場合。

AC は、次の条件が満たされた場合に、クライアントが弱信号クライアントであると判断します。

- クライアントの弱信号パケット数がしきい値に達するか、またはしきい値を超えた場合。
- クライアントの弱信号パケットの割合がしきい値に達するか、それを超えた場合。

パケットの RSSI が RSSI しきい値より低い場合、そのパケットは弱い信号パケットと見なされます。

例

ap1 と名付けた AP の Radio3 で死角検出を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 3

[AC-wlan-ap-ap1-radio-3] calibrate-power coverage enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 3 で、死角検出を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 3

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-3] calibrate-power coverage enable

#グローバルで 2.4GHz 無線の死角検出を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power coverage enable 2.4g

関連コマンド

- calibrate-power 2.4g coverage rssi-threshold
- calibrate-power 2.4g coverage weak-signal-client ratio

- calibrate-power 2.4g coverage weak-signal-client threshold
- calibrate-power 2.4g coverage weak-signal-packet ratio
- calibrate-power 2.4g coverage weak-signal-packet threshold
- calibrate-power 5g coverage rssi-threshold
- calibrate-power 5g coverage weak-signal-client ratio
- calibrate-power 5g coverage weak-signal-client threshold
- calibrate-power 5g coverage weak-signal-packet ratio
- calibrate-power 5g coverage weak-signal-packet threshold

17.1.21 calibrate-power min

Syntax

calibrate-power min *tx-power*

undo calibrate-power min

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：11dBm (ソフトウェアバージョン 7.2.16)

1dBm (ソフトウェアバージョン 7.2.19 と 7.2.21)

6dBm (ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

tx-power: 無線に対する最小伝送電力を指定します。

ソフトウェアバージョン 7.2.16 での設定範囲は 11~20dBm です。

ソフトウェアバージョン 7.2.19 を含む以降のソフトウェアでの設定範囲は 1~20dBm です。

説明

alibrate-power min コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power min コマンドはデフォルトに戻します。

このコマンドは、TPC が実行された後も無線の伝送電力がネットワーク要求を満足できることを保証します。

例

ap1 と名付けた AP の無線 1 に対して最小伝送電力を 10dBm で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power min 10

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して最小伝送電力を 10dBm で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power min 10

17.1.22 calibrate-power mode

Syntax

calibrate-power mode { **coverage** | **custom** | **density** }

undo calibrate-power mode

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、TPC モードはカスタムです。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

coverage: カバレッジモードを指定します。

custom: カスタムモードを指定します。

density: デンシティモードを指定します。

説明

calibrate-power mode コマンドは TPC モードを設定します。

undo calibrate-power mode コマンドはデフォルトに戻します。

AP 間の干渉を避けるには、デンシティモードを使用します。信号カバレッジのパフォーマンスを向上させるには、カバレッジモードを使用します。これらの 2 つのモードがネットワーク要件を満たせない場合、カスタムモードを使用して電力調整設定をカスタマイズします。

デンシティモードまたはカバレッジモードでは、電力調整の設定はシステムによって定義され、変更することはできません。

例

AP **ap1** の無線 1 に対して TPC モードをカバレッジに設定します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power mode coverage

AP グループ **group1** のモデル **QX-W1020** の無線 1 に対して TPC モードをデンシティに設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power mode density

17.1.23 calibrate-power self-decisive

Syntax

calibrate-power self-decisive { **disable** | **enable** }

undo calibrate-power self-decisive

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：無効

View

RRM view

AP group RRM view

Global configuration view(ソフトウェアバージョン 7.2.24 以降のバージョンでサポート)

定義済みユーザロール

network-admin

パラメータ

disable: AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を無効にします。

enable: AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を有効にします。

説明

calibrate-power self-decisive enable コマンドは AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を有効にします。

calibrate-power self-decisive disable コマンドは AC がパワーキャリブレーション間隔で TPC を実行するための定期的な auto-TPC を無効にします。

undo calibrate-power self-decisive コマンドはデフォルトに戻します。

例

ap1 と名付けた AP の無線 1 に対して auto-TPC を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power self-decisive enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して auto-TPC を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power self-decisive enable

関連コマンド

wlan rrm calibration-power interval

17.1.24 calibrate-power threshold

Syntax

calibrate-power threshold *value*

undo calibrate-power threshold

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：65(ソフトウェアバージョン 7.2.21 を含む以前)

75(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

value: 電力しきい値を範囲で指定します。

ソフトウェアバージョン 7.2.19 を含む以前のソフトウェアでの設定範囲は 50～90 です。

この範囲は、無線の電力が-90dBm~-50dBm の範囲にあることを示します。

ソフトウェアバージョン 7.2.21 を含む以降のソフトウェアでの設定範囲は 1~196 です。
この範囲は、無線の電力が-196dBm~-1dBm の範囲にあることを示します。

説明

calibrate-power threshold コマンドは電力しきい値を設定します。

undo calibrate-power threshold コマンドはデフォルトに戻します。

無線同士の干渉を防ぐため､高密度な WLAN では-80dBm に設定することを推奨します。

例

ap1 と名付けた AP の無線 1 に対して電力しきい値を 70 で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power threshold 70

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して電力しきい値を 70 で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power threshold 70

17.1.25 channel holddown-time

Syntax

channel holddown-time *minutes*

undo channel holddown-time

デフォルト

720 分

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

minutes: channel holddown time を 10~1440 分の範囲で指定します。

説明

channel holddown-time コマンドは channel holddown time を設定します。

undo channel holddown-time コマンドはデフォルトに戻します。

RRM holddown group 内の無線のチャネルが変更されるたび、システムは無線に対する channel holddown タイマを開始します。RRM holddown group 内のすべての無線に対するチャネルは、指定された channel holddown time 中は保持されます。

例

RRM holddown group 10 に対して channel holddown time を 600 分に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] channel holddown-time 600

17.1.26 channel-capability mode

Syntax

channel-capability mode { **all** | **none** | **partial** }

undo channel-capability mode

デフォルト

radio view：AP group RRM view の設定を使用します。

AP group radio view：チェックなし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントは、クライアントのサポートされたチャネルがすべて、無線のサポートされたチャネルと一致するときのみ紐付けを許可されます。

none: none モードを指定します。クライアントチャネル能力はチェックされません。

partial: partial モードを指定します。クライアントは、クライアントのサポートされたチャネルのうち 1 つでも、無線のサポートされたチャネルのうちの 1 つと一致すれば紐付けを許可されます。

説明

channel-capability mode コマンドはクライアントチャネル能力マッチモードを設定します。

undo channel-capability mode コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線でのみ使用できます。

このコマンドは、無線が 5GHz モードで動作し、スペクトル管理が有効なときのみ無線に対して効力をもちます。

例

ap1 と名付けた AP の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] channel-capability mode all

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel-capability mode all

関連コマンド

spectrum-management

17.1.27 channel-switch mode

Syntax

channel-switch mode { **continuous** | **suspend** }

undo channel-switch mode

デフォルト

radio view：AP group RRM view の設定を使用します。

AP group radio view：チャネルスイッチの間、オンライン中のすべてのクライアントはフレームの送信を停止します。

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

continuous: チャネルスイッチの間、オンライン中のクライアントがフレームの送信を継続するように設定します。

suspend: チャネルスイッチが完了するまで、オンライン中のクライアントがフレームの送信を停止するように設定します。

説明

channel-switch mode コマンドはチャネルスイッチモードを設定します。

undo channel-switch mode コマンドはデフォルトに戻します。

例

ap1 と名付けた AP の無線 1 に対して **continuous** モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] channel-switch mode continuous

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **continuous** モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel-switch mode continuous

関連コマンド

spectrum-management

17.1.28 crc-error-threshold

Syntax

crc-error-threshold *percent*

undo crc-error-threshold

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：20%(ソフトウェアバージョン 7.2.21 を含む以前)

0%(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: CRC エラーしきい値を 0~100%の範囲で指定します。

説明

crc-error-threshold コマンドは CRC エラーしきい値を設定します。

undo crc-error-threshold コマンドはデフォルトに戻します。

すべての 802.11 パケットの CRC エラーパケットの割合が無線の CRC エラーしきい値に達したことを AC が検出すると、無線は DFS を実行します。

例

ap1 と名付けた AP の無線 1 に対して CRC エラーしきい値を 50%で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] crc-error-threshold 50

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して CRC エラーしきい値を 50%で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] crc-error-threshold 50

17.1.29 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

text: RRM holddown group 記述を 1~64 字のケースセンシティブな文字列で指定します。

説明

description コマンドは RRM holddown group に記述を設定します。

undo description コマンドはデフォルトに戻します。

例

RRM holddown group 10 に対する記述を office に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] description office

17.1.30 display wlan rrm baseline

Syntax

display wlan rrm baseline { **all** | **name** *baseline-name* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての無線ベースラインを指定します。

name *baseline-name*: 無線ベースラインを名前で指定します。大文字と小文字を区別しない 1～32 文字の文字列を指定します。

verbose: 詳細情報を表示します。このキーワードを指定しない場合、コマンドは簡易情報を表示します。

説明

display wlan rrm baseline コマンドは無線ベースライン情報を表示します。

無線ベースラインのロケーション識別子を使用して無線を管理する権利がない場合、無線ベースラインに関する情報を表示することはできません。

例

無線ベースラインの簡易情報を表示します。

<AC> display wlan rrm baseline all

```
Baseline name  : apbaseline
Radio range    : AP
Created at     : 2015-06-22 19:56:31

Baseline name  : groupbaseline
Radio range    : AP group
Created at     : 2015-06-22 19:56:12

Baseline name  : globalbaseline
Radio range    : Global
Created at     : 2015-06-22 19:55:12
```

表 17-1 コマンド出力

フィールド	説明
Radio range	ベースラインに保存された無線の範囲: • **AP**—AP上の無線 • **AP group**—APグループ内のAP上の無線 • **Global**—ACに関連付けられたすべてのAPの無線
Created at	ベースラインが作成された日時

無線ベースラインの詳細情報を表示します。

<AC> display wlan rrm baseline all verbose

```
--------------------------------------------------------------------------------
Baseline name : apbaseline
```

```
Radio range   : AP
Created at    : 2015-06-22 19:56:31
--------------------------------------------------------------------------------
APName           RadioID RadioType Bandwidth Channel Power RegionCode
--------------------------------------------------------------------------------
ap1              2       dot11gn   20        13      20    CN
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Baseline name : groupbaseline
Radio range   : AP group
Created at    : 2015-06-22 19:56:12
--------------------------------------------------------------------------------
APName           RadioID RadioType Bandwidth Channel Power RegionCode
--------------------------------------------------------------------------------
ap1              1       dot11an   40        157     20    CN
ap2              1       dot11an   40        149     20    CN
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Baseline name : globalbaseline
Radio range   : Global
Created at    : 2015-06-22 19:55:12
--------------------------------------------------------------------------------
APName           RadioID RadioType Bandwidth Channel Power RegionCode
--------------------------------------------------------------------------------
ap1              1       dot11an   40        149     20    CN
ap1              2       dot11gn   20        13      20    CN
ap2              1       dot11an   40        149     20    CN
ap2              2       dot11gn   20        1       20    CN
--------------------------------------------------------------------------------
```

表 17-2 コマンド出力

フィールド	説明
Radio range	ベースラインに保存された無線の範囲: • **AP**—AP上の無線 • **AP group**—APグループ内のAP上の無線 • **Global**—ACに関連付けられたすべてのAPの無線
Created at	ベースラインが作成された日時
Power	無線の送信電力（dBm）

フィールド	説明
RegionCode	APの地域コード

17.1.31 display wlan rrm baseline apply-result

Syntax

display wlan rrm baseline apply-result

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan rrm baseline apply-result コマンドは無線ベースラインの最新のアプリケーション結果を表示します。

例

無線ベースラインの最新のアプリケーション結果を表示します。

<AC> display wlan rrm baseline apply-result

```
Radio count : 6
Success     : 4
Failure     : 2
Failure reason
  Radio doesn't exist          : 0
  Radio is down               : 0
  Mismatching radio type       : 0
  Mismatching region code      : 1
  No service template          : 0
  Illegal channel             : 0
  Mismatching bandwidth        : 1
  Channel locked              : 0
  Channel fixed               : 0
  Within channel holddown time  : 0
  Mismatching channel gap policy: 0
  Power locked                : 0
  Within power holddown time    : 0
  Power lower than min. power   : 0
```

```
Power greater than max. power : 0
```

表 17-3 コマンド出力

フィールド	説明
Radio count	無線ベースライン内の無線の数です。
Success	成功したアプリケーションの数です。
Failure	失敗したアプリケーションの数です。
Mismatching radio type	ベースラインに保存された無線モードが実際の無線モードと一致しません。
Mismatching region code	ベースラインに保存されたリージョンコードは、APの実際のリージョンコードと一致しません。
Wireless service not effective	サービステンプレートは、ベースラインの無線にバインドされていないか、バインドされたサービステンプレートが無効になっています。
Mismatching channel gap policy	ベースラインのチャネルが、指定されたチャネルギャップと一致しません。
Power lower than min. power	ベースラインの送信電力は、指定された最小送信電力よりも低いです。
Power greater than max. power	ベースラインの送信電力は、指定された最大送信電力よりも高いです。

17.1.32 display wlan rrm-calibration-group

Syntax

display wlan rrm-calibration-group { **all** | *group-id* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: RRM holddown group を指定します。

group-id: ID で RRM holddown group を指定します。この引数の値の範囲は 1～128 です。

説明

display wlan rrm-calibration-group コマンドは RRM holddown group 情報を表示します。

例

RRM holddown group 10 の情報を表示します。

<AC> display wlan rrm-calibration-group 10

```
        RRM Calibration Group Information
-------------------------------------------------------------------------------
Group ID             : 10
Description          : office
Channel holddown time   : 720 minutes
Power holddown time    : 60 minutes
Group members         : ap4-radio2, ap3-radio2
-------------------------------------------------------------------------------
```

表 17-4 コマンド出力

Field	Description
Group ID	RRM holddown groupのID
Description	RRM holddown groupに対する記述
Channel holddown time	Channel holddown time
Power holddown time	Power holddown time
Group members	RRM holddown group内のRadios

17.1.33 display wlan rrm-history ap

Syntax

display wlan rrm-history ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan rrm-history ap コマンドは、チャネルと電力と帯域幅モードに関する最新 10 件までの変動履歴を表示します。変動履歴には、時間、原因、電力、干渉が含まれます。

例

過去のチャネルと電力の情報を表示します。

<AC> display wlan rrm-history ap name ap1

```
                    AP RRM History
------------------------------------------------------------------------------
 Flags : I - Interference,   P - Packets discarded,    F - Retransmission,
        R - Radar select,   C - Coverage,           B - Channelbusy,
        M - Manual,        D - Bandwidth,          O - Others
------------------------------------------------------------------------------

                     AP RRM History : ap1
------------------------------------------------------------------------------
 Radio : 2                          Basic BSSID : 000f-e2ff-7700
------------------------------------------------------------------------------
       Ch  Power BW    Load Util Intf Reason    Date        Time
           (dBm) (MHz) (%)  (%)  (%)          (yyyy-mm-dd) (hh:mm:ss)
------------------------------------------------------------------------------
 Before 132 20    20    5    0    8    ----C---- 2022-11-04   12:57:27
 After  132 17    20    5    0    8    -         -           -
------------------------------------------------------------------------------
 Before 132 17    20    5    0    8    ----C---- 2022-11-04   13:08:27
 After  132 14    20    5    0    8    -         -           -
------------------------------------------------------------------------------
 Before 132 14    20    5    0    8    ----C---- 2022-11-04   13:19:27
 After  132 11    20    5    0    8    -         -           -
------------------------------------------------------------------------------
 Before 124 11    20    22   5    9    ---R----- 2022-11-07   05:58:57
 After  100 11    20    25   2    11   -         -           -
------------------------------------------------------------------------------
```

表 17-5 コマンド出力

Field	Description
Radio	Radio ID
Basic BSSID	Basic service set identifier
Ch	無線の動作チャネル
Power	無線の伝送電力
BW	無線の帯域幅モード
Load	チャネルロードの割合
Util	チャネル使用の割合
Intf	チャネルで検出された干渉の割合
Reason	チャネルもしくは電力もしくは帯域幅モードの変動理由
Date	チャネルもしくは電力もしくは帯域幅モードの変動した日付
Time	チャネルもしくは電力もしくは帯域幅モードの変動した時間

17.1.34 display wlan rrm-status ap

Syntax

display wlan rrm-status ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan rrm-status ap コマンドは詳細な RRM の情報を表示します。

チャネルと電力の両方とも無効な場合、このコマンドは RRM の情報を表示しません。

例

チャネルと電力に関する詳細な情報を表示します。

<AC> display wlan rrm-status ap name ap1

```
                    AP RRM Profile : ap1
--------------------------------------------------------------------------------
 Radio   : 1                          Basic BSSID    : 70f9-6d31-2fe0
 Channel : 157                         Tx Power (dBm) : 18
--------------------------------------------------------------------------------
   Ch    Nbrs    Load    Util    Intf    PER    Retry    Radar
                 (%)     (%)     (%)     (%)     (%)
--------------------------------------------------------------------------------
   36    0       0       -       0       0      -        -
   40    0       0       -       0       0      -        -
   44    0       0       -       0       0      -        -
   48    0       0       -       0       0      -        -
   52    0       0       -       0       0      -        -
   56    0       0       -       0       0      -        -
   60    0       0       -       0       0      -        -
   64    0       0       -       0       0      -        -
   100   0       0       -       0       0      -        -
   104   0       0       -       0       0      -        -
   108   0       0       -       0       0      -        -
   112   0       0       -       0       0      -        -
   116   0       0       -       0       0      -        -
   132   0       0       -       0       0      -        -
   136   0       0       -       0       0      -        -
   140   0       0       -       0       0      -        -
   149   1       0       -       0       0      -        -
   153   4       0       -       0       0      -        -
   157   0       0       0       0       0      0        -
   161   2       0       -       0       0      -        -
   165   0       0       -       0       0      -        -
--------------------------------------------------------------------------------
  Nbr-MACAddress   Ch    Intf   SignalStrength   Type
                         (%)    (dBm)
--------------------------------------------------------------------------------
  000f-e212-ff01   161   0      -60              Unmanaged
  5866-ba74-e461   153   0      -72              Unmanaged
```

```
  70f9-6d30-9020   153   0      -40            Managed
  70f9-6d31-3080   149   0      -54            Managed
  70f9-6d31-34e0   161   0      -59            Managed
  7425-8a86-bbe0   153   0      -48            Unmanaged
  7425-8a86-c720   153   0      -63            Unmanaged
--------------------------------------------------------------------------------
 Radio   : 2                          Basic BSSID    : 70f9-6d31-2ff0
 Channel : 1                          Tx Power (dBm) : 19
--------------------------------------------------------------------------------
    Ch    Nbrs    Load    Util    Intf    PER    Retry    Radar
                 (%)     (%)     (%)     (%)     (%)
--------------------------------------------------------------------------------
    1     6       4       0       4       0      0        -
    6     4       2       -       2       0      -        -
    11    6       2       -       2       0      -        -
--------------------------------------------------------------------------------
  Nbr-MACAddress   Ch    Intf   SignalStrength   Type
                         (%)    (dBm)
--------------------------------------------------------------------------------
  000f-e212-ff11   1     49     -77              Unmanaged
  0023-89e1-ed00   11    0      -87              Unmanaged
  006a-55f6-ae10   1     57     -88              Unmanaged
  5866-ba64-aa31   1     10     -60              Unmanaged
  5866-ba74-e471   6     0      -76              Unmanaged
  5866-baa9-a610   11    0      -62              Unmanaged
  70f9-6d30-9030   6     0      -63              Managed
  70f9-6d31-3090   1     51     -86              Managed
  70f9-6d31-34f0   6     0      -85              Managed
  7425-8a86-bbf0   6     0      -73              Unmanaged
  7425-8a86-c731   11    0      -93              Unmanaged
  80f6-2ec0-3330   11    0      -76              Unmanaged
  80f6-2ec0-3331   11    0      -73              Unmanaged
  80f6-2edd-d2d0   1     40     -60              Unmanaged
  80f6-2edd-d2d1   1     44     -68              Unmanaged
  80f6-2ede-0b30   11    0      -74              Unmanaged
```

表 17-6 コマンド出力

Field	Description
Radio	Radio ID
Basic BSSID	Basic service set identifier
Channel	無線の動作チャネル

Field	Description
Tx Power	無線の伝送電力
Ch	無線にサポートされたチャネル
Nbrs	検出された無線の数
Load	チャネルで検出されたロードの割合(%)。チャネルロードは、干渉と同様に、アウトバウンドパケットとインバウンドパケット間の割合を参照します。干渉は無線によって受信されるエラーパケットを参照します。
Util	チャネル使用の割合。チャネル使用はアウトバウンドパケットとインバウンドパケット間の割合を参照します。
Intf	チャネルで検出された干渉の割合(%)。
PER	チャネルで検出されたビットエラーレート(%)。
Retry	チャネルで検出された再伝送レート(%)。
Radar	レーダー検出状況 ● –：チャネルでレーダー信号は検出されませんでした。 ● **Detected**：チャネルでレーダー信号が検出されました。
Nbr-MACAddress	検出された無線のMACアドレス
SignalStrength	無線の信号強度（dBm）
Type	無線のタイプ ● **Managed**—同じACによって管理されている無線です。 ● **Unmanaged**—検出されましたが、同じACによって管理されていない無線です。 ● 。

17.1.35 interference-threshold

Syntax

interference-threshold *percent*

undo interference-threshold

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：50%(ソフトウェアバージョン 7.2.21 を含む以前)

70%(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: チャネル干渉しきい値を 0~100%の範囲で指定します。

説明

interference-threshold コマンドはチャネル干渉しきい値を設定します。

undo interference-threshold コマンドはデフォルトに戻します。

すべてのデータパケットの干渉パケットの割合が無線の干渉しきい値に達したことを AC が検出すると、無線は DFS を実行します。干渉パケットは、他の無線に送信されるパケットです。

例

ap1 と名付けた AP の無線 1 に対してチャネル干渉しきい値を 60%で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] interference-threshold 60

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対してチャネル干渉しきい値を 60%で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] interference-threshold 60

17.1.36 power holddown-time

Syntax

power holddown-time *minutes*

undo power holddown-time

デフォルト

60 分

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

minutes: power holddown time を 10~1440 分の範囲で指定します。

説明

power holddown-time コマンドは power holddown time を設定します。

undo power holddown-time コマンドはデフォルトに戻します。

RRM holddown group 内の無線の電力が変更されるたび、システムは無線に対する power holddown タイマを開始します。RRM holddown group 内のすべての無線に対する電力は、指定された power holddown time 中は保持されます。

例

RRM holddown group 10 に対して power holddown time を 600 分に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] power holddown-time 600

17.1.37 power-capability mode

Syntax

power-capability mode { **all** | **none** | **partial** }

undo power-capability mode

デフォルト

radio view：AP group RRM view の設定を使用します。

AP group radio view：チェックなし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントは、クライアントの伝送電力能力がすべて、無線の伝送電力能力と一致するときのみ無線への紐付けを許可されます。

none: none モードを指定します。クライアント伝送電力能力はチェックされません。

partial: partial モードを指定します。クライアントは、クライアントの伝送電力能力のうち 1 つでも、無線の伝送電力能力のうちの 1 つと一致すれば無線への紐付けを許可されます。

説明

power-capability mode コマンドは送信電力機能一致モードを設定します。

undo power-capability mode コマンドはデフォルトに戻します。

このコマンドはスペクトル管理もしくは無線資源計測が有効な場合にのみ反映されます。無線資源計測に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN* を参照してください。

例

ap1 と名付けた AP の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] power-capability mode all

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **all** モードを設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-capability mode all

関連コマンド

- **resource-measure**
- **spectrum-management**

17.1.38 power-constraint mode

Syntax

power-constraint mode { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }

undo power-constraint mode

デフォルト

radio view：AP group RRM view の設定を使用します。

AP group radio view：auto

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

auto: auto モードを指定します。

anpi-interval *anpi-interval-value*: 電力制約の値を計算するため、ANPI（Average Noise Power Indicator）に 0~30dBM の範囲で値を追加します。デフォルト値は 10dBm です。

manual *power-constraint*: 電力制約の値を 0~30dBm の範囲で指定します。

説明

power-constraint mode コマンドは電力制約モードを設定します。

undo power-constraint mode コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線でのみ使用できます。

auto モードを指定する場合、装置は以下の数式を用いて電力制約の値を計算します。

power-constraint = RCPI(Received Channel Power Indicator)-(ANPI + *anpi-interval-value*)

このコマンドはスペクトル管理と無線資源計測を有効にした場合のみ効力を持ちます。無線資源計測に関する詳細は、オペレーションマニュアルのセクション 2 *WLAN* を参照してください。

例

ap1 と名付けた AP の無線 1 に対して **manual** モードを設定し、電力制約の値を 5dBm に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

[AC-wlan-ap-ap1-radio-1] power-constraint mode manual 5

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して **manual** モードを設定し、電力制約の値を 5dBm に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-constraint mode manual 5

関連コマンド

- **resource-measure**
- **spectrum-management**

17.1.39 rrm

Syntax

rrm

View

Radio view

定義済みユーザロール

network-admin

説明

rrm コマンドは RRM（Radio Resource Management）view に移行します。

例

RRM view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

17.1.40 scan-only

Syntax

scan-only { **disable** | **enable** }

undo scan-only

デフォルト

RRM view では、AP group RRM view の構成が使用されます。

AP group RRM view では、無線スキャンが無効になっています。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

disable: 無線スキャンを無効にします。

enable: 無線スキャンを有効にします。

説明

scan-only enable コマンドは無線スキャンを有効にします。

scan-only disable コマンドは無線スキャンを無効にします。

undo scan-only コマンドはデフォルトに戻します。

この機能により、AP は WLAN 環境をスキャンし、収集された統計情報を指定された間隔で AC に報告します。AC は統計を使用してチャネルレポートとネイバーレポートを生成します。

チャネルレポートおよびネイバーレポートを表示するには、**display wlan rrm-status ap** コマンドを使用します。

定期的な auto-DFS、スケジュールされた auto-DFS、または定期的な auto-TPC を設定した場合、この機能をイネーブルにする必要はありません。

例

AP **ap1** の無線 1 に対して無線スキャンを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] scan-only enable

AP グループ **group1** のモデル **QX-W1020** の無線 1 に対して無線スキャンを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] scan-only enable

関連コマンド

display wlan rrm-status ap

17.1.41 snmp-agent trap enable wlan rrm

Syntax

snmp-agent trap enable wlan rrm

undo snmp-agent trap enable wlan rrm

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan rrm コマンドは WLAN RRM に SNMP 通知を有効にします。

undo snmp-agent trap enable wlan rrm コマンドはデフォルトに戻します。

NMS に WLAN RRM の重要なイベントを通知するために、SNMP 通知を有効にしてください。WLAN RRM 通知を正しく送信するために、オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* に記述されるように SNMP の設定も行わなければなりません。

例

WLAN RRM に SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan rrm

17.1.42 spectrum-management

Syntax

spectrum-management { **enable** | **disable** }

undo spectrum-management

デフォルト

radio view：AP group RRM view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

disable: A スペクトル管理を無効にします。

enable: スペクトル管理を有効にします。

説明

spectrum-management enable コマンドはスペクトル管理を有効にします。

spectrum-management disable コマンドはスペクトル管理を無効にします。

undo spectrum-management コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線でのみ使用できます。

例

ap1 と名付けた AP の無線 1 に対してスペクトル管理を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] spectrum-management enable

apgroup1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対してスペクトル管理を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

17.1.43 tolerance-level

Syntax

tolerance-level *percent*

undo tolerance-level

デフォルト

RRM view：AP group RRM view の設定を使用します。

AP group RRM view：20%(ソフトウェアバージョン 7.2.21 を含む以前)

1%(ソフトウェアバージョン 7.2.27 を含む以降)

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: 許容レベルを範囲で指定します。

ソフトウェアバージョン7.2.19 を含む以前のソフトウェアでの設定範囲は 1～45%です。

ソフトウェアバージョン 7.2.21 のソフトウェアでの設定範囲は 0~45%です。

ソフトウェアバージョン7.2.27 を含む以降のソフトウェアでの設定範囲は 0~100%です。

説明

tolerance-level コマンドは許容レベルを設定します。

undo tolerance-level コマンドはデフォルトに戻します。

現在のチャネルが CRC エラーしきい値、干渉しきい値、または再伝送しきい値に達する場合、AC は最適なチャネルを選択します。最適なチャネルと現在のチャネル間の品質ギャップが許容レベルを超えるまで、AC は無線に最適なチャネルを適用しません。

例

ap1 と名付けた AP の無線 1 に対して許容レベルを 25%で設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] tolerance-level 25

group1 と名付けた AP group のモデル **QX-W1020** の無線 1 に対して許容レベルを 25%で設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] tolerance-level 25

17.1.44 wlan calibrate-channel pronto ap all

Syntax

wlan calibrate-channel pronto ap all

View

System view

定義済みユーザロール

network-admin

説明

⚠ **注意：**

このコマンドはシステム資源を消費します。注意して使用してください。

wlan calibrate-channel pronto ap all コマンドはすべての AP の無線に対して on-demand DFS を実行します。

例

すべての AP の無線に対して on-demand DFS を実行します。

<AC> system-view

[AC] wlan calibrate-channel pronto ap all

17.1.45 wlan calibrate-power pronto ap all

Syntax

wlan calibrate-power pronto ap all

View

System view

定義済みユーザロール

network-admin

説明

⚠ **注意：**

このコマンドはシステム資源を消費します。注意して使用してください。

wlan calibrate-power pronto ap all コマンドはすべての AP の無線に対して on-demand TPC を実行します。

例

すべての AP の無線に対して on-demand TPC を実行します。

<AC> system-view

[AC] wlan calibrate-power pronto ap all

17.1.46 wlan rrm baseline apply

Syntax

wlan rrm baseline apply name *baseline-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*: ベースライン名を大文字と小文字を区別しない 1～32 文字の文字列で指定します。

説明

wlan rrm baseline apply コマンドは無線ベースラインを適用します。

次のいずれかの条件を満たす場合、無線ベースラインを適用することはできません。

1) 無線ベースラインのロケーション識別子を使用して無線を管理する権利が無い。
2) 無線ベースラインの名前が start_config_baseline.csv。

例

無線ベースラインを適用する。

<AC> system-view

[AC] wlan rrm baseline apply name bl

関連コマンド

- **display wlan rrm baseline apply-result**
- **wlan rrm baseline save**

17.1.47 wlan rrm baseline remove

Syntax

wlan rrm baseline remove name *baseline-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*: ベースライン名を大文字と小文字を区別しない 1～32 文字の文字列で指定します。

説明

wlan rrm baseline remove コマンドは無線ベースラインを削除します。

無線ベースラインのロケーション識別子を使用して無線を管理する権利がない場合、無線ベースラインを適用することはできません。

例

無線ベースラインを削除する。

<AC> system-view

[AC] wlan rrm baseline remove name bl

関連コマンド

wlan rrm baseline save

17.1.48 wlan rrm baseline save

Syntax

wlan rrm baseline save name *baseline-name* { **ap** *ap-name* **radio** *radio-id* | **ap-group** *group-name* **ap-model** *ap-model* **radio** *radio-id* | **global** }

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*: ベースライン名を大文字と小文字を区別しない 1～32 文字の文字列で指定します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

radio *radio-id*: 無線 ID を指定します。

ap-group *group-name*: AP グループ名を 1～31 文字の大文字と小文字を区別しない文字で指定します。AP グループが既に存在することを確認してください。

ap-model *ap-model*: AP モデルを指定します。

global: すべての無線を指定します。

説明

wlan rrm baseline save コマンドは現在の無線設定を保存して無線ベースラインを作成します。

無線ベースラインは、無線または複数の無線の現用チャネル、送信レート、および他の無線属性を保存します。現在の無線設定を保存して無線ベースラインを作成し、ベースラインを適用してこれらの設定を使用することができます。

無線ベースラインは、AC 上のファイルシステム内の.csv ファイルに保存されます。

例

AP **ap1** の無線 1 に対して設定を保存し、無線ベースライン **ap1-1** を作成します。

<AC> system-view

[AC] wlan rrm baseline save name ap1-1 ap ap1 radio 1

AP グループ **group1** のモデル **QX-W1020** の AP の無線 1 に対して設定を保存し、無線ベースライン **ap1g1-1** を作成します。

<AC> system-view

[AC] wlan rrm baseline save name ap1g1-1 ap-group group1 ap-model QX-W1020 radio 1

すべての無線の設定を保存し、**グローバル**な無線ベースラインを作成します。

<AC> system-view

[AC] wlan rrm baseline save name global global

17.1.49 wlan rrm calibration-bandwidth interval

🕮 **メモ**：

このコマンドはソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

Syntax

wlan rrm calibration-bandwidth interval *minutes*

undo wlan rrm calibration-bandwidth interval

デフォルト

13 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: 帯域幅自動調整間隔を 3～1440 分の範囲で指定します。

説明

wlan rrm calibration-bandwidth interval コマンドは帯域幅自動調整間隔を設定します。

undo wlan rrm calibration-bandwidth interval コマンドはデフォルトに戻します。

例

帯域幅自動調整間隔を 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-bandwidth interval 10

関連コマンド

calibrate-bandwidth self-decisive

17.1.50 wlan rrm calibration-channel interval

Syntax

wlan rrm calibration-channel interval *minutes*

undo wlan rrm calibration-channel interval

デフォルト

ソフトウェアバージョンにより異なります。

ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは 8 分です。

ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでは 23 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: チャネルキャリブレーション間隔を 3～1440 分の範囲で指定します。

説明

wlan rrm calibration-channel interval コマンドはチャネルキャリブレーション間隔を設定します。

undo wlan rrm calibration-channel interval コマンドはデフォルトに戻します。

例

チャネルキャリブレーション間隔を 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-channel interval 10

関連コマンド

calibrate-channel self-decisive

17.1.51 wlan rrm-calibration-group

Syntax

wlan rrm-calibration-group *group-id*

undo wlan rrm-calibration-group { **all** | *group-id* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべての RRM holddown group を指定します。

group-id: RRM holddown group ID を 1～128 の範囲で指定します。

説明

wlan rrm-calibration-group コマンドは新規に RRM holddown group を作成、または既存の RRM holddown group の view を入力して、その view に移行します。

undo wlan rrm-calibration-group コマンドは RRM holddown group を取り除きます。

例

RRM holddown group 10 を作成します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10]

17.1.52 wlan rrm calibration-power interval

Syntax

wlan rrm calibration-power interval *minutes*

undo wlan rrm calibration-power interval

デフォルト

8 分

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes: パワーキャリブレーション間隔を 3～180 分の間隔で指定します。

説明

wlan rrm calibration-power interval コマンドはパワーキャリブレーション間隔を設定します。

undo wlan rrm calibration-power interval コマンドはデフォルトに戻します。

例

パワーキャリブレーション間隔を 10 分で設定します。

<AC> system-view

[AC] wlan rrm calibration-power interval 10

関連コマンド

calibrate-power self-decisive

目次

18 章 WLAN 無線ロードバランス 18-1
18.1.1 wlan radio-load-balance overload-5g ssid-hide 18-1

18章 WLAN 無線ロードバランス

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

18.1.1 wlan radio-load-balance overload-5g ssid-hide

🕮 メモ：

- このコマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- このコマンドは QX-W1110 および QX-W1010 では利用できません。

Syntax

wlan radio-load-balance overload-5g ssid-hide { **disable** | **enable** [**session** *value* [**gap** *gap-value*]] } [**force-logoff**]

undo wlan radio-load-balance overload-5g ssid-hide

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、5GHz 無線ロードバランス機能は v7.2.21 を含む以降のソフトウェアでは有効です。v7.2.19 は無効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: 5GHz 無線ロードバランスを無効にします。

enable: 5GHz 無線ロードバランスを有効にします。

session *value*: セッションしきい値を指定します。範囲は 1～120 で、デフォルトは v7.2.21 を含む以降のソフトウェアでは 5 です。V7.2.19 は 40 です。

gap *gap-value*: セッションギャップしきい値を指定します。範囲は 1～24 で、デフォルトは v7.2.21 を含む以降のソフトウェアでは 4 です。V7.2.19 は 10 です。

force-logoff: レーダー回避が発生して 1 つの 5GHz 無線が使用不可状態になることでクライアントの接続が残った 5GHz 無線に片寄ることを想定し、使用不可状態になったラ

ジオが復旧した際に、クライアントを均等に接続しなおすために強制的に半数のクライアントを切断します。デフォルトは無効です。

説明

wlan radio-load-balance overload-5g ssid-hide enable コマンドは 5GHz 無線ロードバランスを有効にします。

wlan radio-load-balance overload-5g ssid-hide disable コマンドは 5GHz 無線ロードバランスを無効にします。

undo wlan radio-load-balance overload-5g ssid-hide コマンドはデフォルトに戻します。

このコマンドは、2 つの 5GHz 無線で同一の SSID を使用している時、それぞれの 5GHz 無線にクライアントがバランスよく接続するように設定することができます。

このコマンドを設定した後、次の２つの条件が満たされると、5GHz 無線はビーコンフレームの SSID を非表示にします。

- 5GHz 無線に関連付けられているクライアントの数がしきい値に達した場合
- 同じ AP 内の２つの 5GHz 無線の間のセッションギャップが、しきい値に達した場合

5GHz 無線に関連付けられているクライアントの数がセッションしきい値を下回ると、5GHz 無線はビーコンフレームの SSID の非表示を停止します。

なお､5GHz 無線でレーダー検知をするとその 5GHz 無線が一定時間利用できなくなるため、その 5GHz 無線に接続されていたすべてのクライアントが、同じ SSID の残された 5GHz 無線に接続され、5GHz 無線が過負荷になる可能性があります。レーダー検知をした 5GHz 無線が復旧した際、クライアントの接続状態を均等に戻す場合、**force-logoff** を設定しておくことでクライアントの半分を強制的にログオフし、再接続させます。再接続は端末に依存するため、必要な場合にのみこのキーワードを指定してください。

例

AP **ap1** で､クライアント数 1 ギャップ 1 の 5GHz 無線ロードバランスを有効にします。にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1010

[AC-wlan-ap-ap1] wlan radio-load-balance overload-5g ssid-hide enable session 1 gap 1

AP グループ **group1** で、クライアント数 20 ギャップ 5 の 5GHz 無線ロードバランスを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] wlan radio-load-balance overload-5g ssid-hide enable session 20 gap 5

目次

19 章 WLAN アップリンク検出の設定 19-1
19.1 WLAN アップリンク検出コマンド 19-1
19.1.1 wlan uplink track 19-1

19章 WLAN アップリンク検出の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

19.1 WLANアップリンク検出コマンド

19.1.1 wlan uplink track

Syntax

wlan uplink track *track-entry-number*

undo wlan uplink track

デフォルト

WLAN アップリンク検出はトラックエントリと関連付けられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: トラックエントリ ID を指定します。範囲は 1～1024 です。

説明

wlan uplink track コマンドはWLANアップリンク検出をトラックエントリと関連付けます。

undo wlan uplink track コマンドはデフォルトに戻します。

本コマンドにより、トラックエントリに関連付けられたアップリンク状態に基づいて無線状態を AC が調節できるようになります。トラックエントリがネガティブ状態の場合、AC は接続しているすべての AP の無線を無効にします。トラックエントリがポジティブ状態の場合、AC は接続しているすべての AP の無線を有効にします。

本コマンドを複数回実行した場合、最新の設定が有効になります。

例

トラックエントリ 1 を WLAN アップリンク検出に関連付けます。

<AC> system-view

[AC] wlan uplink track 1

目次

20 章 WLAN メッシュの設定 20-1
20.1 WLAN メッシュコマンド 20-1
20.1.1 akm mode sae 20-1
20.1.2 display wlan mesh-link ap 20-2
20.1.3 display wlan mesh-policy 20-4
20.1.4 display wlan mesh-profile 20-5
20.1.5 interface wlan-mesh 20-7
20.1.6 link-hold-rssi 20-8
20.1.7 link-initiation enable 20-8
20.1.8 link-keepalive 20-9
20.1.9 link-maximum-number 20-10
20.1.10 link-rate-mode 20-11
20.1.11 link-saturation-rssi 20-12
20.1.12 mesh-id 20-13
20.1.13 mesh-interface 20-14
20.1.14 mesh peer-mac-address 20-15
20.1.15 mesh-peer intra-ac-mpp enable 20-17
20.1.16 mesh-policy 20-17
20.1.17 mesh-port access vlan 20-19
20.1.18 mesh-port hybrid pvid 20-20
20.1.19 mesh-port hybrid vlan 20-21
20.1.20 mesh-port link-type 20-23
20.1.21 mesh-port trunk permit vlan 20-24
20.1.22 mesh-port trunk pvid 20-25
20.1.23 mesh-profile 20-27
20.1.24 mesh-profile enable 20-28
20.1.25 preshared-key 20-29
20.1.26 probe-request-interval 20-30
20.1.27 portal-service enable 20-30
20.1.28 temporary-link enable 20-32
20.1.29 wlan mesh-policy 20-33
20.1.30 wlan mesh-profile 20-33

20章 WLAN メッシュの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

🕮 **メモ：**

- WLAN メッシュの設定は、ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
- QX-W1100 シリーズの AP は、ソフトウェアバージョン 7.2.50 を含む以降のソフトウェアから WLAN メッシュ機能をサポートしています。
- Anchor-AC 自身で WLAN メッシュ機能を使用することはできません。

20.1 WLAN メッシュコマンド

20.1.1 akm mode sae

Syntax

akm mode sae

undo akm mode

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

説明

akm mode sae コマンドは akm（authentication and key management）モードを SAE（simultaneous authentication of equals）に設定します。

undo akm mode コマンドはデフォルトに戻します。

akm モードを設定する、あるいは削除する前に、メッシュプロファイルが無効であることを確認してください。

例

メッシュプロファイル 1 の akm モードを SAE に設定します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] akm mode sae

関連コマンド

display wlan mesh-profile

20.1.2 display wlan mesh-link ap

Syntax

display wlan mesh-link ap [**name** *ap-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。AP を指定しない場合は、すべての AP のメッシュリンク情報を表示します。

verbose: メッシュリンクの詳細情報を表示します。このパラメータを指定しない場合、簡易情報を表示します。

説明

display wlan mesh-link コマンドはメッシュリンク情報を表示します。

パラメータを指定しない場合、すべてのメッシュリンクの情報を表示します。

例

AP **ap1** のメッシュリンクの簡易情報を表示します。

<AC> display wlan mesh-link ap name ap1

```
AP name: ap1
 Peer          Local         Status     RSSI  Packets(Rx/Tx)
 4ab7-c78a-22ff  75bb-c36d-4ef8  Forwarding  22    0/0
```

表 20-1 コマンド出力

フィールド	説明
Peer	ピアMPのMACアドレス
Local	ローカルAPのMACアドレス
Status	リンクのステータス。メッシュリンクがトラフィックを転送している場合、**Forwarding**と表示されます。
RSSI	メッシュリンクのRSSI
Packets(Rx/Tx)	メッシュリンクのパケット統計情報： • **Rx**－受信パケット数 • **Tx**－送信パケット数

すべての AP のメッシュリンクの詳細情報を表示します。

<AC> display wlan mesh-link ap verbose

```
AP name: ap1
 Peer MAC               : 84d9-317d-9710
 Local MAC              : 70f9-6dd7-cf00
 Status                 : Forwarding
 Link mode              : dot11an
 RSSI                   : 67
 SNR                    : 67
 Noise                  : 0 dBm
 Cost                   : 0
 Incorrect packet         : 0.00 %
 Packets
   Received             : 1508
   Sent                 : 14617
   Resent               : 162
   Lost                 : 0

AP name: ap2
 Peer MAC               : 84d9-317d-9710
 Local MAC              : 0606-e203-1111
 Status                 : Forwarding
 Link mode              : dot11an
 RSSI                   : 62
 SNR                    : 62
 Noise                  : 0 dBm
 Cost                   : 0
 Incorrect packet         : 0.03 %
 Packets
```

```
Received              : 2921
Sent                  : 2877
Resent                : 178
Lost                  : 1
```

表 20-2 コマンド出力

フィールド	説明
Peer MAC	ピアMPのMACアドレス
Local MAC	ローカルAPのMACアドレス
Status	リンクのステータス。メッシュリンクがトラフィックを転送している場合、**Forwarding**と表示されます。
Link mode	無線モード
RSSI	メッシュリンクのRSSI
SNR	信号対雑音比
Cost	リンクコスト
Incorrect packets	送信エラーが発生した送信パケットの割合
Received	受信パケットの総数
Sent	送信されたパケットの総数
Resent	再送信されたパケット数
Lost	ロスしたパケット数

20.1.3 display wlan mesh-policy

Syntax

display wlan mesh-policy [*mesh-policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-policy-name: 大文字と小文字を区別しない 1～31 文字でメッシュポリシ名を指定します。ポリシ名を指定しない場合、すべてのメッシュポリシの情報を表示します。

説明

display wlan mesh-policy コマンドはメッシュポリシ情報を表示します。

例

全てのメッシュポリシの情報を表示します。

<AC> display wlan mesh-policy

```
Mesh policy name                 : default_mesh_policy
Mesh link initiation              : Enabled
Max links                        : 2
Probe request interval            : 1000 ms
Link hold RSSI                   : 15 dBm
Link saturation RSSI              : 150 dBm
Link establish threshold          : 5
Link rate mode                   : fixed
Temporary link establish          : Enabled
Transmission method              : Air
Active link keepalive transmit level : 0
```

表 20-3 コマンド出力

フィールド	説明
Mesh link initiation	メッシュリンク開始機能の状況： ● 有効 ● 無効
Max links	リンクの最大数
Link hold RSSI	メッシュリンクホールドRSSI
Link rate mode	リンクレートモード： ● Fixedーリンクは固定レートで動作しています。 ● Real-timeーリンクレートはリアルタイムでRSSIに適応しています。

20.1.4 display wlan mesh-profile

Syntax

display wlan mesh-profile [*mesh-profile-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。メッシュプロファイルを指定しない場合、すべてのメッシュプロファイルの情報を表示します。

説明

display wlan mesh-profile コマンドはメッシュプロファイル情報を表示します。

例

全てのメッシュプロファイルの情報を表示します。

<AC> display wlan mesh-profile

```
Mesh profile number         : 1
Mesh ID                   : 11
Link keepalive interval     : 2 s
Link backhaul rate          : 18 Mbps
Mesh profile status         : Enabled
Link metric type           : Not Configured
AKM mode                  : None
PSK status                : Disabled

Mesh profile number         : 2
Mesh ID                   : 22
Link keepalive interval     : 2 s
Link backhaul rate          : 18 Mbps
Mesh profile status         : Enabled
Link metric type           : Not Configured
AKM mode                  : None
PSK status                : Disabled
```

表 20-4 コマンド出力

フィールド	説明
Mesh profile status	メッシュプロファイルの状況： ● 有効 ● 無効
AKM mode	akmモード ● None－akmモードは指定されていません。 ● SAE－SAEモードが指定されています。
PSK status	事前共有鍵設定状況： ● Enabled－事前共有鍵が設定されています。 ● Disabled－事前共有鍵は設定されていません。

20.1.5 interface wlan-mesh

Syntax

interface wlan-mesh *interface-number*

undo interface wlan-mesh *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0〜1023 です。

説明

interface wlan-mesh コマンドはメッシュインタフェースを作成し、その view に移行します。あるいは既存のメッシュインタフェースの view に移行します。

undo interface wlan-mesh コマンドはメッシュインタフェースを削除します。

例

AP **ap1** にメッシュインタフェース 1 を作成し、WLAN メッシュインタフェース view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1030

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-mesh1]

AP グループ **g1** のすべての AP にメッシュインタフェース 2 を作成し、AP グループ view の WLAN メッシュインタフェース view に移行します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2]

関連コマンド

mesh-interface

20.1.6 link-hold-rssi

Syntax

link-hold-rssi *value*

undo link-hold-rssi

デフォルト

15 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: メッシュリンクホールド RSSI を指定します。値の範囲は 5～100dBm です。

説明

link-hold-rssi コマンドはメッシュリンクホールド RSSI（メッシュリンクを保持するための最小信号強度）を設定します。

undo link-hold-rssi コマンドはデフォルトに戻します。

例

メッシュリンク **abc** に対してメッシュリンクホールド RSSI を 24dBm に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-hold-rssi 24

関連コマンド

display wlan mesh-policy

20.1.7 link-initiation enable

Syntax

link-initiation enable

undo link-initiation enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

説明

link-initiation enable コマンドはメッシュリンク開始を有効にします。

undo link-initiation enable コマンドはメッシュリンク開始を無効にします。

メッシュリンク開始を有効にすることで、MP はリンクオープン要求を送信していないピアに対してリンクオープン要求を送信します。この機能が無効の場合、MP はピアがリンクオープン要求を送信するまで、ピアに対してリンクオープン要求を送信しません。

例

メッシュリンク開始を無効にします。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] undo link-initiation enable

関連コマンド

display wlan mesh-policy

20.1.8 link-keepalive

Syntax

link-keepalive *keepalive-interval*

undo link-keepalive

デフォルト

2 秒

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

keepalive-interval: keepalive 間隔を指定します。値の範囲は 1～1800 秒です。

説明

link-keepalive コマンドはメッシュリンク keepalive 間隔を設定します。

undo link-keepalive コマンドはデフォルトに戻します。

メッシュリンクの MP はメッシュリンク状態を検出するために keepalive パケットを使用します。大きい MAC アドレスをもつ MP は、keepalive 間隔で keepalive パケットをピアの端に送信します。keepalive パケットを送信した MP は、連続して 3 回の keepalive 間隔終了前に応答を受信しない場合、メッシュリンクを切断します。また、keepalive パケットを受信した MP は、連続して 3 回の keepalive 間隔終了前に keepalive パケットを受信しない場合、メッシュリンクを切断します。リンク状態を正しく検出するため、送信側の keepalive 間隔は、受信側の keepalive 間隔の 3 倍以下に設定してください。

例

メッシュプロファイル 1 でメッシュリンク keepalive 間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] link-keepalive 6

関連コマンド

display wlan mesh-profile

20.1.9 link-maximum-number

🕮 **メモ**:

ホップ数（ネットワーク内のメッシュリンクの最長経路）が増加するにつれてスループットは低下します。

Syntax

link-maximum-number *max-link-number*

undo link-maximum-number

デフォルト

2

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

max-link-number: メッシュリンクの最大数を指定します。値の範囲は 1～8 です。

説明

link-maximum-number コマンドは無線のメッシュリンクの最大数を設定します。

undo link-maximum-number コマンドはデフォルトに戻します。

MP はメッシュリンクが最大数に達すると、無線での新規メッシュリンクの確立を停止します。

例

メッシュポリシ **abc** に対してメッシュリンクの最大数を 5 に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-maximum-number 5

関連コマンド

display wlan mesh-policy

20.1.10 link-rate-mode

Syntax

link-rate-mode { **fixed** | **real-time** }

undo link-rate-mode

デフォルト

fixed モード

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

fixed: fixed モードを指定します。fixed モードでは、メッシュリンクのインタフェースレートは、無線インタフェースレートの現在の設定の最大値に固定します。

real-time: real-time モードを指定します。real-time モードでは、メッシュリンクのインタフェースレートは自動的に RSSI に適応します。

説明

link-rate-mode コマンドはメッシュリンクに対してリンクレートモードを設定します。

undo link-rate-mode コマンドはデフォルトに戻します。

例

メッシュポリシ **abc** に対して、メッシュリンクレートモードを real-time に指定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-rate-mode real-time

関連コマンド

display wlan mesh-policy

20.1.11 link-saturation-rssi

Syntax

link-saturation-rssi *value*

undo link-saturation-rssi

デフォルト

150 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: リンク飽和 RSSI 値を 30～150 dBm の範囲で指定します。

説明

link-saturation-rssi コマンドはリンク飽和 RSSI を設定します。

undo link-saturation-rssi コマンドはデフォルトに戻します。

強力な信号強度がチップのパフォーマンスに影響を与えないように、リンクの RSSI がリンク飽和 RSSI を超えた場合に MP はアクティブ リンクを終了します。

例

メッシュポリシ **abc** に対して、リンク飽和 RSSI を 50 dBm に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-saturation-rssi 50

関連コマンド

display wlan mesh-policy

20.1.12 mesh-id

Syntax

mesh-id *mesh-id*

undo mesh-id

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

mesh-id: メッシュ ID を指定します。大文字と小文字を区別する 1～32 文字で指定できます。

説明

mesh-id コマンドはメッシュプロファイルにメッシュ ID に割り当てます。

undo interface wlan-mesh コマンドはデフォルトに戻します。

例

メッシュプロファイル 1 にメッシュ ID を割り当てます。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] mesh-id mesh

関連コマンド

display wlan mesh-profile

20.1.13 mesh-interface

Syntax

Radio view:

mesh-interface { *interface-number* | **disable** }

undo mesh-interface

AP グループの Radio view:

mesh-interface *interface-number*

undo mesh-interface

デフォルト

Radio view: AP グループの Radio view の設定を使用します。

AP グループの Radio view: 設定なし

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

mesh-interface コマンドは無線にメッシュインタフェースをバインドします。

mesh-interface disable コマンドは無線からメッシュインタフェースのバインドを解除し、AP が AP グループの Radio view の設定を引き継がないようにします。

undo mesh-interface コマンドはデフォルトに戻します。

1 つの無線に対して 1 つのメッシュインタフェースをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

AP view で作成されたメッシュインタフェースは、AP view の無線にのみバインドできます。AP グループ view で作成されたメッシュインタフェースは、AP view の無線と AP グループ View の無線の両方にバインドできます。

例

AP **ap1** の radio 1 にメッシュインタフェース 1 をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-interface 1

AP グループ **g1** の AP の radio 1 にメッシュインタフェース 2 をバインドする。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh-interface 2

関連コマンド

interface wlan-mesh

20.1.14 mesh peer-mac-address

Syntax

Radio view:

mesh peer-mac-address [**blacklist**] { *mac-address* | **disable** }

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

AP グループの Radio view:

mesh peer-mac-address [**blacklist**] *mac-address*

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

デフォルト

Radio view: AP グループの Radio view の設定を使用します。

AP グループの Radio view: 設定なし

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

blacklist: MP の MAC アドレスをメッシュピアブラックリストに追加します。このパラメータを指定しない場合、MAC アドレスはメッシュピアホワイトリストに追加されます。

mac-address: MP の MAC アドレスを H-H-H 形式で指定します。

説明

mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストに MP を追加します。

mesh peer-mac-address disable コマンドはすべての MP からメッシュピアブラックリストもしくはホワイトリストを削除し、AP が AP グループ view の設定を引き継がないようにします。

undo mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストから MP を削除します。

ブラックリストとホワイトリストの両方を設定した場合、ホワイトリストのみ適用されます。

同じ MAC アドレスをホワイトリストもしくはブラックリストに追加するために、このコマンドを複数回実行した場合、最後の設定が適用されます。

Radio view の設定は AP グループの Radio view の設定より優先されます。

例

AP **ap1** のメッシュピアホワイトリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh peer-mac-address 4ab7-c78a-22ff

AP **ap1** のメッシュピアブラックリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh peer-mac-address blacklist 4ab7-c78a-22ff

AP グループ **g1** の AP のメッシュピアホワイトリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh peer-mac-address 4ab7-c78a-22ff

20.1.15 mesh-peer intra-ac-mpp enable

Syntax

mesh-peer intra-ac-mpp enable

undo mesh-peer intra-ac-mpp enable

デフォルト

ループを防ぐため、同一の AC に関連付いている MPP はメッシュピアになることはできません。

View

Global configuration view

定義済みユーザロール

network-admin

説明

mesh-peer intra-ac-mpp enable コマンドは同一の AC に関連付いた MPP がメッシュピアになることを有効にします。

undo mesh-policy コマンドはデフォルトに戻します。

同一の AC に関連付いた MPP が VLAN1 でメッシュリンクを確立しないようにしてください。

例

同一の AC に関連付いた MPP がメッシュピアになるように設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] mesh-peer intra-ac-mpp enable

20.1.16 mesh-policy

Syntax

Radio view:

mesh-policy name { **default** | **name** *policy-name* }

undo mesh-policy

AP グループの Radio view:

mesh-policy name *policy-name*

undo mesh-policy

デフォルト

Radio view: AP グループの Radio view の設定を使用します。

AP グループの Radio view: デフォルトメッシュポリシの **default_mesh_policy** が無線にバインドされています。

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシ名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

default: デフォルトメッシュポリシの **default_mesh_policy** を指定します。

説明

mesh-policy コマンドはメッシュポリシを無線にバインドします。

undo mesh-policy コマンドはデフォルトに戻します。

1 つの無線に 1 つのメッシュポリシをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

Radio view の設定は AP グループの Radio view の設定より優先されます。

例

AP **ap1** の radio 1 にメッシュポリシ **policy1** をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-policy name policy1

AP グループ **g1** の AP の radio1 にメッシュポリシ **policy2** をバインドします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh-policy name policy2

AP **ap1** の radio 1 にデフォルトメッシュポリシをバインドします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-policy default

関連コマンド

wlan mesh-policy

20.1.17 mesh-port access vlan

Syntax

mesh-port access vlan *vlan-id*

undo mesh-port access vlan

デフォルト

VLAN 1

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port access vlan コマンドはアクセスタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port access vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN が存在することを確認してください。

例

AP **ap1** の WLAN メッシュ 1 に VLAN 2 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port access vlan 2

AP グループ **g1** の AP の WLAN メッシュ 2 に VLAN 2 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port access vlan 2

関連コマンド

- **interface wlan-mesh**
- **remote-configuration enable**

20.1.18 mesh-port hybrid pvid

Syntax

mesh-port hybrid pvid vlan *vlan-id*

undo mesh-port hybrid pvid

デフォルト

ハイブリッドポートの PVID は、ポートのリンクタイプがアクセスだったときに属していた VLAN の値です。

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port hybrid pvid vlan コマンドはハイブリッドタイプのメッシュインタフェースの PVID を設定します。

undo mesh-port hybrid pvid コマンドはハイブリッドタイプのメッシュインタフェースの PVID を VLAN 1 に設定します

2 つの MP が互いにメッシュリンクを確立するために使用するメッシュインタフェースが同じ PVID を持っていることを確認してください。

ハイブリッドポートがポート VLAN からパケットを転送できるように、ハイブリッドポートにポート VLAN を割り当ててください。

例

#AP **ap1** の WLAN メッシュ 1 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type hybrid

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid pvid vlan 100

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid vlan 100 untagged

#AP グループ **g1** の AP の WLAN メッシュ 2 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type hybrid

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid pvid vlan 100

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid vlan 100 untagged

関連コマンド

- **mesh-port hybrid vlan**
- **mesh-port link-type**

20.1.19 mesh-port hybrid vlan

Syntax

mesh-port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo mesh-port hybrid vlan *vlan-id-list*

デフォルト

ハイブリッドポートは、ポートのリンクタイプがアクセスのときに属していた VLAN のタグなしメンバです。

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: スペースで区切られた VLAN の値を最大 10 個まで指定します。各項目は VLAN ID、もしくは VLAN ID の範囲を vlan-id 1～vlan-id 2 の形式で指定します。VLAN ID の値の範囲は 1～4094 です。vlan-id 2 パラメータの値は、vlan-id 1 パラメータの値以上である必要があります。指定した VLAN は、デバイスに既に存在している必要があります。

tagged: 指定した VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: 指定した VLAN のタグなしメンバとしてポートを設定します。VLAN タグを削除した後、VLAN のタグなしメンバが VLAN からパケットを送信します。

説明

mesh-port hybrid vlan コマンドはハイブリッドタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port hybrid vlan コマンドは指定された VLAN からハイブリッドタイプのメッシュインタフェースを除外します。

ハイブリッドポートでは、複数の VLAN を許可できます。ハイブリッドポートでこのコマンドを複数回実行すると、ハイブリッドポートは指定された VLAN をすべて許可します。

例

AP **ap1** で WLAN メッシュ 1 をハイブリッドポートとして作成し、タグ付きメンバとして VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type hybrid

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid vlan 2 4 50 to 100 tagged

AP グループ **g1** の AP で WLAN メッシュ 2 をハイブリッドポートとして作成し、タグ付きメンバとして VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type hybrid

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- **mesh-port hybrid pvid**
- **mesh-port link-type**

20.1.20 mesh-port link-type

Syntax

mesh-port link-type { **access** | **hybrid** | **trunk** }

undo mesh-port link-type

デフォルト

アクセスポート

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートリンクタイプをアクセスに設定します。

hybrid: ポートリンクタイプをハイブリッドに設定します。

trunk: ポートリンクタイプをトランクに設定します。

説明

mesh-port link-type コマンドはメッシュインタフェースのリンクタイプを設定します。

undo mesh-port link-type コマンドはデフォルトに戻します。

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、まずアクセスポートに設定する必要があります。

例

AP **ap1** で WLAN メッシュ 1 をトランクポートに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type trunk

AP グループ **g1** の AP で WLAN メッシュ 2 をトランクポートに設定します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type trunk

20.1.21 mesh-port trunk permit vlan

Syntax

mesh-port trunk permit vlan { *vlan-id-list* | **all** }

undo mesh-port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

VLAN 1

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: スペースで区切られた VLAN の値を最大 10 個まで指定します。各項目は VLAN ID、もしくは VLAN ID の範囲を vlan-id 1 から vlan-id 2 の形式で指定します。VLAN ID の値の範囲は 1 から 4094 です。vlan-id 2 パラメータの値は、vlan-id 1 パラメータの値以上である必要があります。指定した VLAN は、デバイスに既に存在している必要があります。

tagged: 指定した VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: 指定した VLAN のタグなしメンバとしてポートを設定します。VLAN タグを削除した後、VLAN のタグなしメンバが VLAN からパケットを送信します。

説明

mesh-port trunk permit vlan コマンドはトランクタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port trunk permit vlan コマンドは指定された VLAN からトランクタイプのメッシュインタフェースを除外します。

トランクポートでは、複数の VLAN を許可できます。トランクポートでこのコマンドを複数回実行すると、トランクポートは指定された VLAN をすべて許可します。

トランクポートでは、PVID からのパケットのみがタグなしで通過できます。

例

AP **ap1** で WLAN メッシュ 1 をトランクポートとして作成し、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type trunk

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk permit vlan 2 4 50 to 100

AP グループ **g1** の AP で WLAN メッシュ 2 をトランクポートとして作成し、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type trunk

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk permit vlan 2 4 50 to 100

関連コマンド

- **mesh-port link-type**
- **mesh-port trunk pvid**

20.1.22 mesh-port trunk pvid

Syntax

mesh-port trunk pvid *vlan-id*

undo mesh-port trunk pvid

デフォルト

トランクポートの PVID は VLAN 1 です。

View

WLAN-mesh interface view

AP グループの WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port trunk pvid コマンドはトランクタイプのメッシュインタフェースの PVID を設定します。

undo mesh-port trunk pvid コマンドはデフォルトに戻します。

存在しない VLAN をトランクポートのポート VLAN として指定できます。

2 つの MP が互いにメッシュリンクを確立するために、使用するメッシュインタフェースが同じ PVID を持っていることを確認してください。

トランクポートがポート VLAN からパケットを送信できるようにするには、トランクポートをポート VLAN に割り当てる必要があります。

例

#AP **ap1** の WLAN メッシュ 1 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk pvid vlan 100

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk permit vlan 100

#AP グループ **g1** の AP の WLAN メッシュ 2 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk pvid vlan 100

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk permit vlan 100

関連コマンド

- **mesh-port link-type**
- **mesh-port trunk permit vlan**

20.1.23 mesh-profile

Syntax

Radio view:

mesh-profile { *mesh-profile-number* | **disable** }

undo mesh-profile

AP グループの Radio view:

mesh-profile *mesh-profile-number*

undo mesh-profile

デフォルト

Radio view: AP グループの Radio view の設定を使用します。

AP グループの Radio view: 設定なし

View

Radio view

AP グループの Radio view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number:メッシュインタフェースの番号を指定します。値の範囲は 1～32 です。

説明

mesh-profile コマンドはメッシュイプロファイルを作成し、無線にバインドします。

mesh-profile disable コマンドは無線からメッシュプロファイルのバインドを解除し、AP が AP グループの設定を引き継がないようにします。

undo interface wlan-mesh コマンドを使用して、デフォルト設定に戻します。

Radio view の設定は AP グループの Radio view の設定より優先されます。

例

AP **ap1** の radio 1 にメッシュプロファイル 1 をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-profile 1

AP グループ **g1** の AP の radio 1 にメッシュプロファイル 2 をバインドします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-1020

[AC-wlan-ap-group-g1-ap-model-QX-1020] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-1020-radio-1] mesh-profile 2

関連コマンド

- **mesh-profile enable**
- **wlan mesh-profile**

20.1.24 mesh-profile enable

Syntax

mesh-profile enable

undo mesh-profile enable

デフォルト

無効

View

Mesh profile view

定義済みユーザロール

network-admin

説明

mesh-profile enable コマンドはメッシュプロファイルを有効にします。

undo mesh-profile enable コマンドはメッシュプロファイルを無効にします。

メッシュプロファイルを有効にする前に、メッシュ ID を割り当てる必要があります。

例

メッシュプロファイル 1 を有効にします。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] mesh-profile enable

関連コマンド

mesh-id

20.1.25 preshared-key

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 文字列形式で鍵を設定します。

raw-key: 16 進数形式で鍵を設定します。

cipher: 暗号化形式で鍵を指定します。

simple: 平文形式で鍵を指定します。安全のため、平文形式で指定された鍵は暗号化形式で格納されます。

string: 大文字と小文字を区別する鍵列を指定します。鍵の長さの範囲は以下の通りです。

- **pass-phrase plaintext**－8～63 文字
- **pass-phrase ciphertext**－41～117 文字
- **raw-key plaintext**－64 桁の 16 進数字
- **raw-key ciphertext**－117 文字

説明

preshared-key コマンドはメッシュプロファイルに事前共有鍵を追加します。

undo preshared-key コマンドはデフォルトに戻します。

このコマンドを使用する前に、メッシュプロファイルが無効であることを確認してください。

メッシュプロファイルに設定できる事前共有鍵は 1 つです。このコマンドを複数回実行した場合、最後の設定が適用されます。

例

メッシュプロファイル 1 に平文の事前共有鍵 **abcdefghij** を追加します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] preshared-key pass-phrase simple abcdefghij

関連コマンド

display wlan mesh-profile

20.1.26 probe-request-interval

Syntax

probe-request-interval *interval-value*

undo probe-request-interval

デフォルト

1000 ミリ秒

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

probe-request-interval コマンドはプローブ要求間隔を設定します。

undo probe-request-interval コマンドはデフォルトに戻します。

例

メッシュポリシ a**bc** に対してプローブ要求間隔を 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] probe-request-interval 500

関連コマンド

display wlan mesh-policy

20.1.27 portal-service enable

Syntax

AP view もしくは AP グループ view:

portal-service { **disable** | **enable** }

undo portal-service

Global configuration view:

portal-service enable

undo portal-service

デフォルト

AP view では、AP グループ view の設定を使用します。AP グループ view に設定が存在しない場合、global configuration view の設定を使用します。

AP グループ view では、global configuration view の設定を使用します。

Global configuration view では、MPP はプローブ要求を送信します。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: MPP がプローブ要求を無効にします。

enable: MPP がプローブ要求を有効にします。

説明

portal-service enable コマンドは MPP がプローブ要求を送信するのを無効にします。

portal-service disable コマンドは MPP がプローブ要求を送信し、AP group view もしくは global configuration view の設定を引き継がないようにします。

undo probe-service コマンドを使用して、デフォルト設定に戻します。

WLAN メッシュネットワークを有線ネットワークに接続するメッシュポイントとして、MPP は多数のメッシュリンクを確立する必要があります。パフォーマンスを維持するために、MPP がネイバ検出のプローブ要求を送信しないように無効にできます。MPP は、他の MP からのプローブ要求にのみ応答します。

例

AP **ap1** でプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] portal-service enable

AP グループ **group1** の AP でプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] portal-service enable

グローバルでプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] portal-service enable

20.1.28 temporary-link enable

Syntax

temporary-link enable

undo temporary-link enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

temporary-link enable コマンドはテンポラリメッシュリンクの確立を有効にします。

undo temporary-link enable コマンドはデフォルトに戻します。

例

テンポラリメッシュリンクの確立を有効にします。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] temporary-link enable

20.1.29 wlan mesh-policy

Syntax

wlan mesh-policy *policy-name*

undo wlan mesh-policy *policy-name*

デフォルト

システム定義のポリシ「**default_mesh_policy**」が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシ名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

説明

wlan mesh-policy コマンドはメッシュポリシを作成し、その view に移行します。あるいは既存のメッシュポリシの view に移行します。

undo wlan mesh-policy コマンドはメッシュポリシを削除します。

無線で使用中のメッシュポリシ内の属性設定を削除、修正する前に、無線にバインドされたメッシュプロファイルを無効にしてください。

システム定義のメッシュポリシを修正もしくは削除することはできません。

例

メッシュポリシ **abc** を作成し、その view に移行します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc]

20.1.30 wlan mesh-profile

Syntax

wlan mesh-profile *mesh-profile-number*

undo wlan mesh-profile *mesh-profile-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。

説明

wlan mesh-profile コマンドはメッシュプロファイルを作成し、その view に移行します。あるいは既存のメッシュプロファイルの view に移行します。

undo wlan mesh-profile コマンドはメッシュプロファイルを削除します。

メッシュプロファイル内の属性設定を修正するには、メッシュプロファイルを無効にする必要があります。

例

メッシュプロファイル 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1]

関連コマンド

mesh-profile enable

目次

21 章 コンフィグレーションプロファイルの設定 21-1
21.1 コンフィグレーションプロファイルの設定コマンド 21-1
21.1.1 acl 21-1
21.1.2 address 21-3
21.1.3 address range 21-4
21.1.4 authentication-mode 21-5
21.1.5 authorization-attribute 21-7
21.1.6 configuration profile 21-9
21.1.7 configuration-profile 21-10
21.1.8 dhcp enable 21-11
21.1.9 dhcp relay server-address 21-12
21.1.10 dhcp select 21-13
21.1.11 dhcp server ip-pool 21-14
21.1.12 dns-list 21-15
21.1.13 expired 21-16
21.1.14 forbidden-ip-range 21-17
21.1.15 gateway-list 21-18
21.1.16 interface 21-19
21.1.17 interface bridge-aggregation 21-19
21.1.18 interface vlan-interface 21-20
21.1.19 ip address 21-21
21.1.20 ip address dhcp-alloc 21-22
21.1.21 ip route-static 21-23
21.1.22 line 21-24
21.1.23 line class 21-25
21.1.24 local-user 21-26
21.1.25 nat address-group 21-28
21.1.26 nat inbound 21-29
21.1.27 nat outbound 21-32
21.1.28 network 21-35
21.1.29 packet-filter 21-36
21.1.30 password 21-37
21.1.31 port access vlan 21-39
21.1.32 port hybrid pvid 21-39
21.1.33 port hybrid vlan 21-41
21.1.34 port link-aggregation group 21-42
21.1.35 port link-type 21-43

21.1.36 port trunk permit vlan 21-44
21.1.37 port trunk pvid 21-45
21.1.38 port-isolate enable 21-46
21.1.39 qos priority 21-47
21.1.40 qos trust 21-48
21.1.41 rule (IPv4 advanced ACL view) 21-49
21.1.42 rule (IPv4 basic ACL view) 21-55
21.1.43 rule (Layer 2 ACL view) 21-57
21.1.44 rule comment 21-59
21.1.45 service-type 21-60
21.1.46 set authentication password 21-60
21.1.47 shutdown 21-62
21.1.48 step 21-63
21.1.49 telnet server enable 21-64
21.1.50 vlan 21-65

21章 コンフィグレーションプロファイルの設定

21.1 コンフィグレーションプロファイルの設定コマンド

> 🕮 **メモ**：
> この章のコマンドは、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

21.1.1 acl

Syntax

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

acl { name *acl-name* | **number** *acl-number* [**name** *acl-name*] }

acl { **advanced** | **basic** } { *acl-number* | **name** *acl-name* }

acl mac { *acl-number* | **name** *acl-name* }

undo acl { all | **name** *acl-name* | **number** *acl-number* }

undo acl { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

all: すべての ACL を指定します。

説明

acl コマンドは ACL を作成し、ACL の view に移行します。すでに ACL が作成されている場合、その view に移行します。

undo acl コマンドは指定された、あるいはすべての ACL を削除します。

ACL のルールが一致順序を含む、あるいは以下の一致基準が有効である場合、一致するパケットはソフトウェアベースのパケット転送を行います。

- 送信元および宛先 IP アドレス
- 送信元ポート、宛先ポート
- トランスポートレイヤプロトコル
- ICMP メッセージタイプ、メッセージコード、およびメッセージ名
- VPN インスタンス
- ロギング
- タイムレンジ

ソフトウェアベースのパケット転送は、転送エントリのため、コントロールプレーンにパケットを送信します。これは装置のパケット転送に影響します。

例

コンフィグレーションプロファイル **ap1** に標準 IPv4 ACL 2000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000]

コンフィグレーションプロファイル **ap1** に ACL 名が flow の標準 IPv4 ACL を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic name flow

[AC-config-profile-ap1-acl-ipv4-basic-flow]

コンフィグレーションプロファイル **ap1** に 拡張 IPv4 ACL 3000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3000

[AC-config-profile-ap1-acl-ipv4-adv-3000]

コンフィグレーションプロファイル **ap1** に L2 ACL 4000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl mac 4000

[AC-config-profile-ap1-acl-mac-4000]

コンフィグレーションプロファイル **ap1** に ACL 名が flow の L2 ACL を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl mac name flow

[AC-config-profile-ap1-acl-mac-flow]

21.1.2 address

Syntax

address *start-address end-address*

undo address *start-address end-address*

デフォルト

設定なし

View

Configuration profile-NAT address group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address: アドレス範囲の開始 IP アドレスと終了 IP アドレスを指定します。終了アドレスは開始アドレスより小さくできません。同じ場合、アドレス範囲には IP アドレスが 1 つしかありません。IP アドレスの範囲は 65535 個まで指定できます。

説明

address コマンドは NAT アドレスグループにアドレス範囲を追加します。

undo address コマンドは NAT アドレスグループからアドレス範囲を削除します。

NAT アドレスグループは、アドレス範囲のセットです。外部ネットワーク宛てのパケットの送信元アドレスは、アドレス範囲の 1 つのアドレスに変換されます。

単一の NAT アドレスグループまたは複数の NAT アドレスグループのアドレス範囲が重複していないことを確認します。

例

コンフィグレーションプロファイル **ap1** に作成した NAT アドレスグループ 2 にアドレス範囲を追加します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] nat address-group 2

[AC-config-profile-address-group-2] address 10.1.1.1 10.1.1.15

[AC-config-profile-address-group-2] address 10.1.1.20 10.1.1.30

関連コマンド

nat address-group

21.1.3 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。

説明

address range コマンドはダイナミックの割り当てを行うため DHCP アドレスプールの IP アドレス範囲を設定します。

undo address range コマンドは DHCP アドレスプールの IP アドレス範囲を削除します。

IP アドレス範囲が指定されていない場合、address pool view で **network** コマンドを使用してサブネットのすべての IP アドレスを割り当てることができます。IP アドレス範囲が指定されている場合、IP アドレス範囲の IP アドレスのみを割り当てることができます。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

address range で指定されたアドレス範囲は **network** コマンドで指定されたサブネット内にある必要があります。範囲外のアドレスを割り当てることはできません。

例

コンフィグレーションプロファイル **ap1** の DHCP アドレスプール 1 に 192.168.8.1～192.168.8.150 のアドレス範囲を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 1

[AC-config-profile-ap1-dhcp-pool-1] address range 192.168.8.1 192.168.8.150

関連コマンド

network

21.1.4 authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

デフォルト

VTY line の認証モードは password です。

コンソールユーザの認証モードは製品モデルにより異なります。

QX-W1000 シリーズは none です。

QX-W1100 シリーズは password です。

View

Configuration profile-user line view

Configuration profile-user line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細はオペレーションマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

説明

authentication-mode コマンドは user line の認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

network-admin またはレベル 15 ユーザの役割を割り当てられたユーザだけがこのコマンドを実行することができます。他のユーザがこのコマンドを実行する権利を与えられても、このコマンドを実行することができません。

認証モードが **none** である場合、すべてのユーザは認証なしでログインすることができます。装置のセキュリティを改善するため、認証モードを **password** あるいは **scheme** にしてください。

VTY line view で、**authentication-mode** コマンドは **protocol inbound** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

認証モードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを none にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode none

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを password に設定し、パスワードを 321 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode password

[AC-config-profile-ap1-line-vty0] set authentication password simple 321

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを scheme に設定します。ローカルユーザ 123 を設定し、パスワードを 321 に設定します。Telnet サービスを割り当て、ユーザのユーザロールを network-admin に割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode scheme

[AC-config-profile-ap1-line-vty0] quit

[AC-config-profile-ap1] local-user 123

[AC-config-profile-ap1-luser-manage-123] password simple 321

[AC-config-profile-ap1-luser-manage-123] service-type telnet

[AC-config-profile-ap1-luser-manage-123] authorization-attribute user-role network-admin

関連コマンド

set authentication password

21.1.5 authorization-attribute

Syntax

authorization-attribute { **idle-cut** *minutes* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **idle-cut** | **session-timeout** | **user-role** *role-name* | **vlan** | **work-directory** } *

デフォルト

FTP、SFTPユーザは作業ディレクトリとしてNASのルートディレクトリを設定します。しかし、ユーザはルートディレクトリへのアクセス許可がありません。

network-admin あるいは level-15 のユーザによって作成されたローカルユーザは network-operator のユーザロールが割り当てられています。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

idle-cut *minute*: アイドルタイムアウト時間を設定します。設定範囲は 1～120 分です。指定されるアイドル時間を超過したアイドル中のオンラインユーザはログアウトされます。

user-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザに 64 のユーザロールを指定することができます。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1～4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

work-directory *directory-name*: FTP、SFTP ユーザの作業ディレクトリを指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。このディレクトリは既に存在している必要があります。デフォルトで FTP、SFTP ユーザは装置のルートディレクトリにアクセスすることができます。

説明

authorization-attribute コマンドはローカルユーザまたはユーザグループの許可属性を設定します。ローカルユーザ、またはローカルユーザのユーザグループが認証を通過すると、装置はユーザにそれらの属性を割り当てます。

undo authorization-attribute コマンドはデフォルトに戻します。

アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。

SSH、Telnet、端末ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

HTTP、HTTPS ユーザの場合、許可属性はユーザロールが適用できます。

FTP ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

ローカルユーザのほかのタイプは適用されません。

ユーザが許可されたユーザロールのみ適用させるため、あらかじめ定義されたユーザロールを削除するために **undo authorization-attribute user-role** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** に作成した装置管理ユーザ abc の許可される VLAN を VLAN 2 として設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user abc class network

[AC-config-profile-ap1-luser-network-abc] authorization-attribute vlan 2

21.1.6 configuration profile

Syntax

configuration profile *profile-name* **[model** *model-name* **]**

undo configuration profile *profile-name*

デフォルト

設定無し

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: コンフィグレーションプロファイルの名前を 1～64 文字の文字列で指定します。文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (]) 、スラッシュ (/) 、ハイフン (-) が使用可能です。大文字と小文字は区別されます。

model *model-name*: AP モデル名を指定します。このパラメータは、コンフィグレーションプロファイルを作成するときに必要です。

説明

configuration profile コマンドはコンフィグレーションプロファイルを作成し、その View に移行するか、既存のコンフィグレーションプロファイルの View に移行します。

undo configuration profile コマンドは、既存のコンフィグレーションプロファイルを削除します。

AC でコンフィグレーションプロファイルを作成し、プロファイルを 1 つまたは複数の AP に関連付けることができます。その後、AC はプロファイルで指定された設定を、関連付けられた AP がオンラインになったときに自動的に展開します。

コンフィグレーションプロファイルを作成するときは、AP モデル名を指定する必要があります。AC は、AP モデルに基づいてプロファイルにデフォルト設定を生成します。

AC には最大 2048 のコンフィグレーションプロファイルを作成することができます。

例

AP **ap1 model QX-W1130** のコンフィグレーションプロファイルを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1]

21.1.7 configuration-profile

メモ：

- **configuration-profile** と **remote-configuration** を同じ AP に対して設定しないでください。
- コンフィグレーションプロファイルで設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**configuration-profile** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

configuration-profile *profile-name*

undo configuration-profile

デフォルト

設定無し

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

profile-name: コンフィグレーションプロファイルの名前を 1～64 文字の文字列で指定します。文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (]) 、スラッシュ (/) 、ハイフン (-) が使用可能です。大文字と小文字は区別されます。

説明

configuration-profile コマンドは、既存のコンフィグレーションプロファイルを AP または AP グループと関連付けます。

undo configuration-profile コマンドは、デフォルトに戻します。

既存のコンフィグレーションプロファイルを AP または AP グループに関連付けます。AP または AP グループ内の AP がオンラインになると、AC はプロファイル内の設定を AP に自動的に展開します。

コンフィグレーションプロファイルと AP または AP グループの関連付けを解除するには、undo configuration-profile コマンドを実行します。また、undo configuration-profile コ

マンドを実行すると、AP または AP グループ内の AP の設定が工場出荷時のデフォルトに復元されます。

例

AP **ap1 model QX-W1130** とコンフィグレーションプロファイル **profile1** を関連付けます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] configuration-profile profile1

AP グループ **apgroup1** の 型番 **QX-W1130** とコンフィグレーションプロファイル **profile1** を関連付けます。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] configuration-profile profile1

21.1.8 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

Configuration profile view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP に関する設定は DHCP を有効にしたのち適用されます。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

コンフィグレーションプロファイル **ap1** の DHCP を有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp enable

21.1.9 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上に置くことはできません。その場合、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 10 で DHCP リレーエージェントの DHCP サーバアドレス 1.1.1.1 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] dhcp relay server-address 1.1.1.1

21.1.10 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。無効にした場合、インタフェースは受信した DHCP パケットを廃棄します。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 2 で DHCP リレーエージェントを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2] dhcp select relay

21.1.11 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

pool-name: アドレスプールを固有に識別するため DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

dhcp server ip-pool コマンドは DHCP アドレスプールを作成し、その view に移行します。

undo dhcp server ip-pool コマンドは指定した DHCP アドレスプールを削除します。

またコマンドを使用して既存の DHCP アドレスプールに移行することができます。

DHCP アドレスプールは DHCP クライアントに割り当てられる設定パラメータを記録するために使用されます。

例

コンフィグレーションプロファイル **ap1** に DHCP アドレスプール pool1 を作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool pool1

[AC-config-profile-ap1-dhcp-pool-pool1]

関連コマンド

- **dhcp server apply ip-pool**
- **display dhcp server pool**

21.1.12 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: DNS サーバを指定します。&<1-8>は DNS サーバのアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを指定します。

undo dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo dns-list** コマンドは DHCP アドレスプールのすべての DNS サーバのアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** の DHCP アドレスプール 0 の DNS サーバアドレス 10.1.1.254 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

display dhcp server pool

21.1.13 expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

デフォルト

1 日

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

day *day*: 日数を指定します。設定範囲は 0～365 日です。

hour *hour*: 時間を指定します。設定範囲は 0～23 時間です。デフォルトは 0 時間です。

minute *minute*: 分を指定します。設定範囲は 0～59 分です。デフォルトは 0 分です。

second *second*: 秒を指定します。設定範囲は 0～59 秒です。デフォルトは 0 秒です。

unlimited: リース期間を指定しません。正確には 136 年のリース期間です。

説明

expired コマンドは DHCP アドレスプールのリース期間を指定します。

undo expired コマンドは DHCP アドレスプールのリース期間をデフォルトに戻します。

DHCP サーバは DHCP クライアントにリース期間と共に IP アドレスを割り当てます。リース期間が終了する前に、DHCP クライアントはリース期間を延長する必要があります。

- リース期間の延長が成功した場合、DHCP クライアントは IP アドレスを使用し続けることができます。
- リース期間の延長が失敗したとき、以下のイベントの両方が発生します。
  - リース期間が終了した後 DHCP クライアントは IP アドレスを使用することができません。
  - DHCP サーバは終了したアドレスとして IP アドレスにラベルをつけます。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のリース期間を 1 日、2 時間、3 分、4 秒に指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

21.1.14 forbidden-ip-range

Syntax

forbidden-ip-range *start-ip-address* [*end-ip-address*]

undo forbidden-ip-range [*start-ip-address* [*end-ip-address*]]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 除外する IP アドレス範囲の開始アドレスを指定します

end-ip-address: 除外する IP アドレス範囲の終了アドレスを指定します

説明

forbidden-ip-range コマンドはアドレスプールのダイナミック割り当てから IP アドレス範囲を除外します。

undo forbidden-ip-range コマンドは設定を削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のダイナミック割り当てから 192.168.10.1 から 192.168.10.10 のアドレス範囲を除外します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 1

[AC-config-profile-ap1-dhcp-pool-1] forbidden-ip-range 192.168.10.1 192.168.10.10

21.1.15 gateway-list

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-64>: ゲートウェイを指定します。&<1-64>はゲートウェイアドレスを半角スペースで区切り最大 64 つまで指定できることを示します。ゲートウェイアドレスは割り当て可能な IP アドレスと同一のサブネットに存在する必要があります。

説明

gateway-list コマンドは DHCP アドレスプールのゲートウェイアドレスを指定します。

undo gateway-list コマンドは DHCP アドレスプールからゲートウェイアドレスを削除します。

パラメータを指定しない場合、**undo gateway-list** コマンドはすべてのゲートウェイアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のゲートウェイアドレスに 10.1.1.1 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] gateway-list 10.1.1.1

21.1.16 interface

Syntax

interface *interface-type interface-number*

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

interface コマンドは interface view に移行します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 の interface view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1]

21.1.17 interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。（1 で固定です。）

説明

interface bridge-aggregation コマンドはアグリゲートインタフェースを作成し、aggregate interface view に移行します。すでにアグリゲートインタフェースが存在する場合、aggregate interface view に移行します。

undo interface bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

例

コンフィグレーションプロファイル **ap1** にアグリゲートインタフェース Bridge-Aggregation 1 を作成し、aggregate interface view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface bridge-aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation1]

21.1.18 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-number: VLAN インタフェース番号を指定します。設定範囲は 1～4094 です。

説明

interface vlan-interface コマンドは VLAN インタフェースを作成し、作成された VLAN インタフェースの view に移行あるいは既存の VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、VLAN を作成してください。

例

コンフィグレーションプロファイル **ap1** に VLAN インタフェース 2 を作成し、作成された VLAN インタフェースの view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 2

[AC-config-profile-ap1-vlan2] quit

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2]

21.1.19 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリ IP アドレスあるいはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP、DHCP、PPP を通して IP アドレスを取得するインタフェースはセカンダリ IP アドレスを設定することができません。

undo ip address コマンドはインタフェースからすべての IP アドレスを削除します。

undo ip address *ip-address* { *mask* | *mask-length* }コマンドはプライマリ IP アドレスを削除します。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** コマンドはセカンダリ IP アドレスを削除します。

インタフェースに割り当てたプライマリ IP アドレスとセカンダリ IP アドレスは同一ネットワークセグメント上に設定することができますが、装置の異なるインタフェースは異なるネットワークセグメント上に存在する必要があります。

例

コンフィグレーションプロファイル **ap1** に 作成した VLAN インタフェース 10 にプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] ip address 129.12.0.1 255.255.255.0

[AC-config-profile-ap1-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub

21.1.20 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは DHCP を使用して IP アドレスを取得するインタフェースを設定します。

undo ip address dhcp-alloc コマンドはインタフェースで DHCP の使用を停止します。

undo ip address dhcp-alloc コマンドを実行すると、インタフェースは DHCP を通して取得した IP アドレスをリリースするため、DHCP-RELEASE メッセージを送信します。インタフェースがダウンしている場合、メッセージを送信することができません。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 10 に、 DHCP を使用して IP アドレスを取得する設定をします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] ip address dhcp-alloc

21.1.21 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } *next-hop-address*

undo ip route-static *dest-address* { *mask-length* | *mask* } [*next-hop-address*]

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: IP アドレスのマスク長を指定します。設定範囲は 0～32 です。

mask: IP アドレスのマスクを指定します。ドットで区切り、10 進数で指定します。

next-hop-address: ネクストホップの IP アドレスを指定します。ドットで区切り、10 進数で指定します。詳細はオペレーションマニュアルのセクション 6 *ルーティングプロトコル “スタティックルーティング”* を参照してください。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドはスタティックルートを削除します。

宛先アドレスとマスクの両方が 0.0.0.0（あるいは 0）である場合、設定されたルートはデフォルトルートです。デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

例

コンフィグレーションプロファイル **ap1** に宛先アドレスが 1.1.1.1/24、ネクストホップが 2.2.2.2、のスタティックルートを設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] ip route-static 1.1.1.1 24 2.2.2.2

21.1.22 line

Syntax

line { **console** | **vty** } *first-number* [*last-number*] }

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

console *first-number*: first console line の相対番号を指定します。

vty *first-number*: first VTY line の相対番号を指定します（0～63）。

vty *last-number*: last VTY user line の相対番号を指定します（1～63）。*first-number* よりも小さくすることはできません。

説明

line コマンドは 1 つ以上の user line view に移行します。

シングル user line に設定を行うために、このコマンドを使用して user line view に移行します。

同じ設定を複数の user line に行うために、このコマンドを使用して複数の user line view に移行します。

例

コンフィグレーションプロファイル **ap1** の user line Console 0 の view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] line console 0

[AC-config-profile-ap1-line-console0]

コンフィグレーションプロファイル **ap1** の user lines VTY 0～VTY 4 の view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] line vty 0 4

[AC-config-profile-ap1-line-vty0-4]

関連コマンド

line class

21.1.23 line class

Syntax

line class { **console** | **vty** }

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

line class コマンドは user line class view に移行します。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **authentication-mode**
- **set authentication password**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

コンフィグレーションプロファイル **ap1** の VTY line class view で認証モードを none にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line class vty

[AC-config-profile-ap1-line-class-vty] authentication-mode none

関連コマンド

line

21.1.24 local-user

Syntax

local-user *user-name* [**class manage**]

undo local-user { *user-name* **class manage** | **all** [**service-type** { **ftp** | **http** | **https | ssh** | **telnet** | **terminal** } | **class manage**] }

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: ローカルユーザ名を指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/），バックスラッシュ、垂直バー（|）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

class: ローカルユーザタイプを指定します。指定しない場合、装置管理ユーザを指定します。

- **manage**: 装置管理ユーザを指定します。装置管理ユーザは FTP、HTTP、HTTPS、SSH、Telnet、端末サービスを使用することができます。

all: すべてのユーザを指定します。

service-type: ローカルユーザの使用するサービスタイプを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **https**: HTTPS ユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

説明

local-user コマンドはローカルユーザを追加し、local user view に移行します。

undo local-user コマンドはローカルユーザを削除します。

Configuration profile view では装置管理ユーザのみ作成することができ、最大 16 の装置管理ユーザが作成することができます。

例

コンフィグレーションプロファイル **ap1** に装置管理ユーザ user1 を追加し、local user view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1]

関連コマンド

service-type

21.1.25 nat address-group

Syntax

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

group-id : NAT アドレスグループの ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: NAT アドレスグループに名前を割り当てます。*group-name* 引数は、1~63 文字のストリングで、大文字と小文字が区別されます。

説明

nat address-group コマンドは NAT アドレスグループを作成し、そのビューを移行するか、または既存の NAT アドレスグループのビューを移行します。

undo nat address-group コマンドは NAT アドレスグループを削除します。

NAT アドレスグループは、アドレス範囲のセットです。address コマンドを使用して、NAT アドレスグループにアドレス範囲を追加します。ダイナミック NAT は、パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

例

コンフィグレーションプロファイル **ap1** に番号が 1 で名前が abc の NAT アドレスグループを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] nat address-group 1 name abc

関連コマンド

- **address**
- **nat inbound**
- **nat outbound**

21.1.26 nat inbound

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、すべてを指定することはできません。

address-group: アドレス変換のアドレスグループを指定します。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換をイネーブルにします。逆アドレス変換は、既存の NO-PAT エントリを使用して、内部ネットワークからアクティブに開始された接続の宛先アドレスを外部ネットワークに変換します。

add-route: 変換後に自動的に送信元アドレスにルートを追加します。出力インタフェースは NAT インタフェースで、ネクストホップは変換前の送信元アドレスです。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 受信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 受信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat inbound コマンドは受信ダイナミック NAT ルールを設定します。

undo nat inbound コマンドは受信ダイナミック NAT ルールを削除します。

受信ダイナミック NAT は、ACL によって許可された受信パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

受信ダイナミック NAT は、次のモードをサポートします。

- [PAT] :IP アドレス変換とポート変換の両方を実行します。
- [NO-PAT] :IP アドレス変換だけを実行します。

NO-PAT モードでは、逆アドレス変換がサポートされます。逆アドレス変換では、ACL 逆マッチングを使用して、変換するパケットを識別します。ACL リバースマッチングは次のように機能します。

- パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
- 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

受信ダイナミック NAT は通常、次のいずれかと連携して双方向 NAT を実装します。

- 送信ダイナミック NAT (nat outbound コマンド) 。
- NAT Server (nat server コマンド) 。
- 送信スタティック NAT (nat static コマンド) 。

アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。nat inbound コマンドでは、PAT モードと NO-PAT モードの両方で使用できません。

内部ネットワークと外部ネットワークが存在するサブネットが重複している場合は、add-route キーワードを指定しないでください。その他のネットワークシナリオの場合:

- add-route キーワードを指定すると、デバイスはパケットの変換後に自動的に送信元アドレスにルートを追加します。宛先アドレスは NAT アドレスグループ内の NAT アドレス、出力インタフェースはコマンドが実行されるインタフェース、ネクストホップは変換前の送信元アドレスです。
- add-route キーワードを指定しない場合は、ルートを手動で追加する必要があります。自動ルート追加は低速であるため、手動でルートを追加することをお勧めします。

ACL は、インタフェース上の 1 つの受信ダイナミック NAT ルールだけで使用できます。

1 つのインタフェースに複数の受信ダイナミック NAT ルールを設定できます。

同じプライオリティ値で設定された受信ダイナミック NAT ルールは、その ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

コンフィグレーションプロファイル **ap1** にサブネット 10.110.10.0/24 からのパケットだけを通過させる、ACL 2001 を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2001

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule deny

[AC-acl-ipv4-basic-2001] quit

コンフィグレーションプロファイル **ap1** にアドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AC-config-profile-ap1] nat address-group 1

[AC-config-profile-ap1-address-group-1] address 202.110.10.10 202.110.10.12

[AC-config-profile-ap1-address-group-1] quit

#インバウンド NO-PAT ルールを# コンフィグレーションプロファイル **ap1** のインタフェース VLAN インタフェース 10 に設定します。NAT は、受信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換し、変換されたパケットのルートを自動的に追加します。ルール名を abc に、優先順位を 0 に設定します。

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat inbound 2001 address-group 1 no-pat add-route rule abc priority 0

21.1.27 nat outbound

Syntax

NO-PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** text] [**counting**]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: ipv 4-acl-number:2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

address-group: NAT のアドレスグループを指定します。アドレスグループを指定しない場合、インタフェースの IP アドレスが NAT アドレスとして使用されます。Easy IP が使用されている。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換を有効にします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。

port-preserved: PAT のポート番号を保持しようとします。このキーワードは、ダイナミック NAT ポートブロックマッピングでは有効になりません。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、引用符 (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 送信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 送信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat outbound コマンドは送信ダイナミック NAT 規則を設定します。

undo nat outbound コマンドは送信ダイナミック NAT 規則を削除します。

送信ダイナミック NAT は通常、外部ネットワークに接続されたインタフェースで設定されます。1 つのインタフェースに複数の送信ダイナミック NAT ルールを設定できます。

送信ダイナミック NAT は、次のモードをサポートします。

- PAT :IP アドレス変換とポート変換の両方を実行します。PAT モードでは、エンドポイントに依存しないマッピング動作が使用されている場合、外部ホストは内部ホストにアクティブにアクセスできます。
- NO-PAT :IP アドレス変換だけを実行します。reversible キーワードを指定した場合、NO-PAT モードでは、外部ホストが内部ホストにアクティブにアクセスできます。ACL が指定されている場合、リバースアドレス変換は ACL リバースマッチングで許可されたパケットだけに適用されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

ダイナミック NAT 444 は、NO-PAT モードをサポートしません。

NAT アドレスグループを指定する場合は、次の制約事項および注意事項に従ってください。

- アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。
- nat outbound コマンドでは、PAT モードと NO-PAT モードの両方でアドレスグループを使用できません。
- NAT アドレスグループでポートブロックパラメータが指定されている場合、このコマンドはダイナミック NAT ポートブロックマッピングを設定します。ACL 許可ルールに一致するパケットは、ダイナミック NAT 444 によって処理されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL は、インタフェース上の 1 つの送信ダイナミック NAT ルールだけで使用できます。
- ACL を指定すると、NAT は ACL によって許可された送信パケットの送信元 IP アドレスをアドレスグループの IP アドレスに変換します。ACL を指定しない場合、NAT はすべてのパケットを変換します。
- インタフェースに ACL が設定されている送信ダイナミック NAT ルールは、ACL が設定されていないルールよりも優先されます。ACL ベースのダイナミック NAT ルールが 2 つ設定されている場合、ACL 番号が大きい方のルールのプライオリティが高くなります。

同じプライオリティ値で設定された送信ダイナミック NAT ルールと ACL は、ルール内の ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

コンフィグレーションプロファイル **ap1** にサブネット 10.110.10.0/24 からのパケットだけを通過させる、ACL 2001 を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2001

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2001] rule deny

[AC-config-profile-ap1-acl-ipv4-basic-2001] quit

コンフィグレーションプロファイル **ap1** にアドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AC-config-profile-ap1] nat address-group 1

[AC-config-profile-ap1-address-group-1] address 202.110.10.10 202.110.10.12

[AC-config-profile-ap1-address-group-1] quit

コンフィグレーションプロファイル **ap1** のインタフェース VLAN インタフェース 10 に送信ダイナミック PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001 address-group 1

[AC-config-profile-ap1-Vlan-interface10] quit

コンフィグレーションプロファイル **ap1** のインタフェース VLAN インタフェース 10 に送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001 address-group 1 no-pat

[AC-config-profile-ap1-Vlan-interface10] quit

#VLAN インタフェース 10 の IP アドレスを変換後のアドレスとして使用するには、Easy IP を有効にします。

[AC-config-profile-ap1] interface Vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001

[AC-config-profile-ap1-Vlan-interface10] quit

#VLAN インタフェース 10 で送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。逆アドレス変換を有効にします。

[AC-config-profile-ap1] interface Vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] nat outbound 2001 address-group 1 no-pat reversible

21.1.28 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*]

undo network *network-address* [*mask-length* | **mask** *mask*]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address: ダイナミック割り当てのサブネットを指定します。マスク長やマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

説明

network コマンドは DHCP アドレスプールのダイナミック割り当てのサブネットを指定します。

undo network コマンドは指定されたサブネットを削除します。

DHCP アドレスプールで 1 つのプライマリサブネットのみを指定することができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ネットワークの設定の変更あるいは削除を行うと現在のアドレスプールから割り当てられたアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のサブネットとして 192.168.8.0/24 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0

関連コマンド

gateway-list

21.1.29 packet-filter

Syntax

packet-filter [mac] { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

undo packet-filter [mac] { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

デフォルト

設定なし

View

Configuration profile- interface view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

inbound: インタフェースで受信されるパケットをフィルタリングします。

outbound: インタフェースで送信されるパケットをフィルタリングします。

説明

packet-filter コマンドはパケットをフィルタするため、インタフェースに ACL を適用します。

undo packet-filter コマンドはインタフェースから ACL を削除します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 に受信トラフィックをフィルタするため、標準 IPv4 ACL 2001 を適用します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] packet-filter 2001 inbound

21.1.30 password

Syntax

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストのパスワードを設定します。

hash: ハッシュパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

🕮 **メモ：**

string は以下の要件を満たす文字列にしてください。

- 10 文字以上。
- アルファベット、数字、記号のうち 2 種類以上を含む。
- ユーザ名またはユーザ名の逆の文字を含まない。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

プレーンテキストパスワードとハッシュパスワードをサポートします。

例

コンフィグレーションプロファイル **ap1** に 装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1] password simple 123456TESTplat&!

21.1.31 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべてのアクセスポートは VLAN1 に所属しています。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 3

[AC-config-profile-ap1-vlan3] quit

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port access vlan 3

21.1.32 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port hybrid pvid コマンドはハイブリッドポートの PVID を設定します。

undo port hybrid pvid コマンドはハイブリッドポートの PVID を 1 に設定します。

ハイブリッドポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドでハイブリッドポートの PVID を削除する場合、ポートの PVID の設定は適用されません。

ローカルとリモートのハイブリッドポートに同じ PVID を設定することを推奨します。

PVID からのパケットの転送を許可するためにハイブリッドポートの設定に **port hybrid pvid** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をハイブリッドポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 をタグ無しメンバとして割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 100

[AC-config-profile-ap1-vlan100] quit

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type hybrid

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid pvid vlan 100

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged

関連コマンド

- **port hybrid vlan**
- **port link-type**

21.1.33 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属している VLAN のタグなしメンバです。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

tagged: ポートは VLAN タグを削除しないで指定した VLAN のパケットを送信するように設定します。

untagged: ポートは VLAN タグを削除したのち、指定した VLAN のパケットを送信するように設定します。

説明

port hybrid vlan コマンドは指定した VLAN にハイブリッドポートを割り当てます。

undo port hybrid vlan コマンドは指定した VLAN からハイブリッドポートを削除します。

ハイブリッドポートは、複数の VLAN が通過できます。**port hybrid vlan** コマンドを繰り返し実行すると、ハイブリッドポートを通過する VLAN は、各実行の *vlan-id-list* により指定された VLAN に設定されます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をハイブリッドポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当て、これらの VLAN のパケットにタグを付けて送信するよう GigabitEthernet 1/0/1 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type hybrid

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

port link-type

21.1.34 port link-aggregation group

Syntax

port link-aggregation group *number*

undo port link-aggregation group

デフォルト

設定なし

View

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

number: アグリゲーショングループに対応するアグリゲートインタフェースの数を指定します。（1 で固定です。）

説明

port link-aggregation group コマンドは指定したアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドは所属しているアグリゲーショングループからインタフェースを削除します。

インタフェースは 1 つのアグリゲーショングループのみ所属することができます。

例

コンフィグレーションプロファイル **ap1** の アグリゲーショングループ 1 に GigabitEthernet 1/0/1 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-aggregation group 1

21.1.35 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

access

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートのリンクタイプをアクセスとして指定します。

hybrid: ポートのリンクタイプをハイブリッドとして指定します。

trunk: ポートのリンクタイプをトランクとして指定します。

説明

port link-type コマンドはポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

トランクポートからハイブリッドポート（またはその逆）のリンクタイプを変更するには、まずリンクタイプをアクセスに設定する必要があります。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のリンクタイプをトランクポートに設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

21.1.36 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

トランクポートは VLAN 1 からのパケットのみ通過できるように許可します。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を通過できるように許可します。許可されていない VLAN ユーザがポートを通して制限されたリソースにアクセスすることを防ぐため､注意して **port trunk permit vlan all** コマンドを使用してください。

説明

port trunk permit vlan コマンドはトランクポートを指定した VLAN に割り当てます。

undo port trunk permit vlan コマンドはトランクポートを指定した VLAN から削除します。

トランクポートは複数の VLAN を通過できます。**port trunk permit vlan** コマンドを繰り返し実行すると、トランクポートを通過する VLAN は、各 *vlan-id-list* により指定された VLAN に設定されます。

トランクポート上では、PVID のトラフィックのみタグなしで通過することができます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をトランクポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100

関連コマンド

port link-type

21.1.37 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

VLAN 1

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port trunk pvid コマンドはトランクポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

トランクポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドを使用してトランクポートの PVID を削除しても、ポートの PVID の設定には影響しません。

ローカルおよびリモートのトランクポートは、PVID のトラフィックが正常に送信されるために同じ PVID を使用する必要があります。

PVID からのパケットの転送を許可するためにトランクポートの設定に **port trunk permit vlan** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をトランクポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**

21.1.38 port-isolate enable

Syntax

port-isolate enable

undo port-isolate enable

デフォルト

Layer2 Ethernet interface view では、ポートアイソレーションは有効です。

Layer2 Aggregate interface view では、ポートアイソレーションは無効です。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port-isolate enable コマンドはポートアイソレーションを有効にします。

undo port-isolate コマンドはポートアイソレーションを無効にします。

Ethernet interface view での設定は、そのインタフェースにのみ適用されます。

aggregate interface view での設定は、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定の適用に失敗した場合、装置はどのアグリゲーションメンバポートもアイソレーショングループに割り当てません。設定の適用失敗がアグリゲーションメンバポートで起きた場合、装置は失敗が起きたポートをスキップし、別のアグリゲーションメンバポートをアイソレーショングループに割り当てます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port-isolation enable

コンフィグレーションプロファイル **ap1** のアグリゲートインタフェース Bridge-Aggregation 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface Bridge-Aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation-1] port-isolate enable

21.1.39 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0～7 です。

説明

qos priority コマンドはインタフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface gigabitethernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] qos priority 2

21.1.40 qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

インタフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

説明

qos trust コマンドはインタフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface gigabitethernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] qos trust dot1p

21.1.41 rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **source** | **source-port** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-IPv4 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当て

ます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6)、**udp** (17)を指定できます。**ip** はすべてのプロトコルを指定します。表 21-1 にプロトコルの値に関わらず指定できるパラメータを示します。

表 21-1 拡張 IPv4 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-wildcard* | **any** }	送信元アドレスを定義します。	*source-address*と*source-wildcard*はドットで区切られた10進数表記の送信元IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の送信元IPアドレスを示します。
destination { *dest-address dest-wildcard* | **any** }	宛先アドレスを定義します。	*dest-address*と*dest-wildcard*はドットで区切られた10進数表記の宛先IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の宛先IPアドレスを示します。
precedence *precedence*	IPプレシーデンスの値を指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～7です。名前は**routine** (0)、**priority** (1)、**immediate** (2)、**flash** (3)、**flash-override** (4)、**critical** (5)、**internet** (6)、**network** (7)が指定できます。
tos *tos*	ToSプレシーデンスを指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～15です。名前は**max-reliability** (2)、**max-throughput** (4)、**min-delay** (8)、**min-monetary-cost** (1)、**normal** (0)が指定できます。

パラメータ	機能	説明
dscp *dscp*	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**af11** (10)、**af12** (12)、**af13** (14)、**af21** (18)、**af22** (20)、**af23** (22)、**af31** (26)、**af32** (28)、**af33** (30)、**af41** (34)、**af42** (36)、**af43** (38)、**cs1** (8)、**cs2** (16)、**cs3** (24)、**cs4** (32)、**cs5** (40)、**cs6** (48)、**cs7** (56)、**default** (0)、**ef** (46)が指定できます。
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション8 *ACL and QoS* *“タイムレンジ”*を参照してください。

protocol が **tcp** (6)あるいは **udp** (17)である場合、設定するパラメータを表 21-2 に示します。

表 21-2 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*は*operator*が範囲であるときのみ必要です。 TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**domain** (53)、**echo** (7)、**exec** (512)、**finger** (79)、**ftp** (21)、**ftp-data** (20)、**gopher** (70)、**hostname** (101)、**irc** (194)、**klogin** (543)、**kshell** (544)、**login** (513)、**lpd** (515)、**nntp** (119)、**pop2** (109)、**pop3** (110)、**smtp** (25)、**sunrpc** (111)、**tacacs** (49)、**talk** (517)、
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	

パラメータ	機能	説明
		telnet (23)、**time** (37)、**uucp** (540)、**whois** (43)、**www** (80) UDPポート番号は以下の名前で指定できます **biff** (512)、**bootpc** (68)、**bootps** (67)、**discard** (9)、**dns** (53)、**dnsix** (90)、**echo** (7)、**mobilip-ag** (434)、**mobilip-mn** (435)、**nameserver** (42)、**netbios-dgm** (138)、**netbios-ns** (137)、**netbios-ssn** (139)、**ntp** (123)、**rip** (520)、**snmp** (161)、**snmptrap** (162)、**sunrpc** (111)、**syslog** (514)、**tacacs-ds** (65)、**talk** (517)、**tftp** (69)、**time** (37)、**who** (513)、**xdmcp** (177)
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	ACK、FIN、PSH、RST、SYN、URGを含む1つまたは複数のTCPフラグを指定します。	TCP用のパラメータです。各値は0(フラグビットがセットされていません)または1(フラグビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、ack 0 psh 1が設定されたルールは、ACKフラグが設定されていないパケット、およびPSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmp** (1)である場合、設定するパラメータを表 21-3 に示します。

表 21-3 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 21-4に示します。

表 21-4 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

コンフィグレーションプロファイル **ap1** にアドレス 129.9.0.0/16 から 202.38.160.0/24 の宛先ポート 80 の TCP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3000

[AC-config-profile-ap1-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

コンフィグレーションプロファイル **ap1** に 192.168.1.0/24 宛の ICMP パケットを除くすべての IP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3001

[AC-config-profile-ap1-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-adv-3001] rule permit ip

コンフィグレーションプロファイル **ap1** に FTP の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3002

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data

コンフィグレーションプロファイル **ap1** に SNMP と SNMP trap の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3003

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp source-port eq snmp

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

関連コマンド

- **acl**
- **step**
- **time-range**

21.1.42 rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **source** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-IPv4 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *"タイムレンジ"* を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

コンフィグレーションプロファイル **ap1** に アドレス 10.0.0.0/8、172.17.0.0/16、192.168.1.0/24 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule deny source any

関連コマンド

- **acl**
- **step**
- **time-range**

21.1.43 rule (Layer 2 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**time-range**]

undo rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

cos *vlan-pri*: 802.1p プライオリティを定義します。

- プライオリティの設定範囲は 0～7 です。
- **best-effort** (0)、**background** (1)、**spare** (2)、**excellent-effort** (3)、**controlled-load** (4)、**video** (5)、**voice** (6)、**network-management** (7)の用語で定義することができます。

dest-mac *dest-address dest-mask*: 宛先 MAC アドレス範囲を定義します。*dest-address* と *dest-mask* は宛先 MAC アドレスとマスクを示します。マスクの形式は H-H-H です。

lsap *lsap-type lsap-type-mask*: LLC カプセル化の DSAP と SSAP フィールドを定義します。*lsap-type* は 16 進数表記でカプセル化フォーマットを示します。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。

type *protocol-type protocol-type-mask*: L2 の 1 つ以上のプロトコルを定義します。*protocol-type* は 16 進数表記で Ethernet_II と Ethernet_SNAP のプロトコルタイプを示します。*protocol-type-mask* は 16 進数表記でプロトコルタイプのマスクを示します。

source-mac *source-address source-mask*: 送信元 MAC アドレス範囲を定義します。*source-address* は送信元 MAC アドレスを示します。*sour-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *"タイムレンジ"* を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

L2 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

L2 ACL 4000 のルールを作成します。ARP パケットを許可し、RARP パケットを拒否します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] rule permit type 0806 ffff

[AC-config-profile-ap1-acl-mac-4000] rule deny type 8035 ffff

関連コマンド

- **acl**
- **step**

21.1.44 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

設定なし

View

Configuration profile-IPv4 basic/advanced ACL view

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ACL のルール ID を指定します。設定範囲は 0～65534 です。ACL のルールはすでに作成されている必要があります。

text: ACL のルールの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rule comment コマンドは ACL のルールの説明を設定します。

undo rule comment コマンドは ACL のルールの説明を削除します。

例

標準 IPv4 ACL 2000 を作成し、ルールの説明を追加します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule 0 comment This rule is used on Gigabitethernet 1/0/1.

21.1.45 service-type

Syntax

service-type { **ftp** | { **telnet** | **terminal** } * }

undo service-type { **ftp** | { **telnet** | **terminal** } * }

デフォルト

ローカルユーザは許可されておらず、サービスを使用することができません。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

ftp: ユーザが FTP サービスを使用することを許可します。許可されたディレクトリは **authorization-attribute work-directory** コマンドで変更することができます。

telnet: ユーザが Telnet サービスを使用することを許可します。

terminal: ユーザが端末サービスを使用し、コンソールポートからログインすることを許可します。

説明

service-type コマンドはローカルユーザが使用するサービスタイプを指定します。

undo service-type コマンドはローカルユーザが使用するサービスタイプを削除します。

複数のサービスタイプをユーザに割り当てることができます。

例

コンフィグレーションプロファイル **ap1** に作成した 装置管理ユーザ user1 が Telnet、FTP サービスを使用することを許可します。

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1] service-type telnet

[AC-config-profile-ap1-luser-manage-user1] service-type ftp

21.1.46 set authentication password

Syntax

set authentication password { **hash** | **simple** } *password*

undo set authentication password

デフォルト

コンソールユーザのパスワード設定は AP モデルにより異なります。

QX-W1000 シリーズは設定なしです。

QX-W1100 シリーズは qx_admin です。

line class vty のパスワード設定は AP モデルにより異なります。

QX-W1000 シリーズは設定なしです。

QX-W1100 シリーズは qx_admin です。

View

Configuration profile-user line view

Configuration profile-user line class view

定義済みユーザロール

network-admin

パラメータ

hash: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。

password: 大文字、小文字が区別されたパスワードを指定します。**simple** が指定された場合、設定範囲は 1～16 文字です。**hash** が指定された場合、設定範囲は 1～110 文字です。

説明

set authentication password コマンドはパスワード認証のパスワードを設定します。

undo set authentication password コマンドはパスワードを削除します。

セキュリティのため、保存されたパスワードは設定に関わらず常に暗号テキストで表示されます。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

例

コンフィグレーションプロファイル **ap1** の user line Console 0 でパスワード認証のパスワード hello を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line console 0

[AC-line-console0] authentication-mode password

[AC-line-console0] set authentication password simple hello

関連コマンド

authentication-mode

21.1.47 shutdown

Syntax

shutdown

undo shutdown

デフォルト

インタフェースはアップ状態です。

View

Configuration profile-interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはインタフェースをシャットダウンします。

undo shutdown コマンドはインタフェースをアップします。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をシャットダウンし、それからアップします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] shutdown

[AC-config-profile-ap1-GigabitEthernet1/0/1] undo shutdown

コンフィグレーションプロファイル **ap1** の アグリゲートインタフェース Bridge-Aggregation 1 を up にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface bridge-aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation1] undo shutdown

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 2 をシャットダウンし、up にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2] shutdown

[AC-config-profile-ap1-Vlan-interface2] undo shutdown

21.1.48 step

Syntax

step *step-value*

undo step

デフォルト

ACL のルール番号付けステップは 5 で、開始ルール ID は 0 です。

View

Configuration profile-IPv4 basic/advanced ACL view

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

step-value: ACL ルールのステップ数を指定します。設定範囲は 1～20 です。

説明

step コマンドは ACL ルールに自動的に番号を割り振るためのステップ数を設定します。

undo step コマンドはデフォルトに戻します。

ルールの番号づけステップはシステムが自動的にルール番号の増分を設定します。たとえば、デフォルトの ACL の番号づけステップは 5 です。ルールを作成するとき、ID を割り当てない場合、ルールの番号は 0、5、10、15、...と番号づけられます。番号づけのステップを広くする場合、2 つのルールの間に多くのルールを挿入することができます。ス

テップを変更したときはいつでも、ルールは 0 から再ナンバリングが行われます。たとえば、5 つのルールの番号 5、10、13、15、20 がつけられている場合、ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6、8 に再ナンバリングされます。

例

コンフィグレーションプロファイル **ap1** に作成した 標準 IPv4 ACL 2000 のステップ数を 2 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] step 2

21.1.49 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

デフォルトは AP モデルにより異なります。

QX-W1000 シリーズでは無効です。

QX-W1100 シリーズでは有効です。

View

Configuration profile view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは Telnet サーバ機能を有効にします。

undo telnet server enable コマンドは Telnet サーバ機能を無効にします。

管理者は Telnet サーバ機能が有効であるときのみ装置に Telnet を行うことができます。

例

Telnet サーバ機能を有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] telnet server enable

21.1.50 vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

VLAN 1（システムデフォルト VLAN）

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

vlan-id1, vlan-id2: VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN の範囲を指定します。*vlan-id1* と *vlan-id2* は VLAN ID を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: VLAN 1～4094 を指定します。

説明

vlan *vlan-id* コマンドは VLAN を作成し、その view あるいは既存の VLAN の view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは *vlan-id1* から *vlan-id2* の VLAN を作成します。

vlan all コマンドは VLAN 1～VLAN 4094 を作成します。

undo vlan コマンドは指定された VLAN を削除します。

システムデフォルト VLAN（VLAN 1）を作成あるいは削除することはできません。

例

コンフィグレーションプロファイル **ap1** に VLAN 2 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 2

[AC-config-profile-ap1-vlan2]

コンフィグレーションプロファイル **ap1** に VLAN 4～VLAN 100 を作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 4 to 100

目次

22 章 Web リダイレクトの設定 22-1
22.1 Web リダイレクトの設定コマンド 22-1
22.1.1 web-redirect url 22-1

22章 Web リダイレクトの設定

22.1 Webリダイレクトの設定コマンド

22.1.1 web-redirect url

🕮 メモ：

このコマンドは、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

Syntax

web-redirect url *url-string* [**interval** *interval*]

undo web-redirect

デフォルト

無効

Viwe

service-template view

定義済みのユーザーロール

network-admin

パラメータ

url *url-string* :ユーザのリダイレクト先の URL を 1 文字から 256 文字の文字列で指定します。URL は存在する URL を指定してください。形式は、http://または https://で始まる完全な URL であることを確認してください。

interval *interval* :指定した URL にユーザがリダイレクトされる時間間隔を指定します。60 秒から 86400 秒の範囲で指定します。デフォルトの間隔は 86400 秒です。

説明

web-redirect url コマンドは Web リダイレクト機能を有効にします。

undo web-redirect url コマンドは Web リダイレクト機能を無効にします。

この機能は、Web ブラウザを介して外部ネットワークにアクセスする前に、ユーザを指定された URL にリダイレクトします。指定された間隔が経過すると、ユーザは再び指定された URL にリダイレクトされます。

Web リダイレクト機能は、デフォルトのポート番号 80 を使用する HTTP パケットに対してのみ有効です。

url *url-string* オプションを使用することで、 異なるユーザに異なる広告ページを発信することができます。

設定パラメータは以下の通りです。

・userip=%c:ユーザの IP アドレスです。

・usermac=%m:ユーザの MAC アドレスです。

・nasid=%n:デバイスの NAS 識別子です。

・ssid=%E:ユーザが関連付ける SSID です。

・originalurl=%o:ユーザがブラウザに入力する元の URL です

パラメータ形式は以下の形式に準拠していることを確認してください。

http://XXXX/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o

例

#サービステンプレート service 1 で Web リダイレクトを設定します。リダイレクト URL を http://192.0.0.1/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o に設定します。間隔は 3600 秒に設定します。

<AC> system-view

[AC] wlan service-template service-template1

[AC-wlan-st-service-template1] web-redirect url http://192.0.0.1/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o interval 3600

目次

23 章 IoT 機能の設定 23-1
23.1 BLE 機能の設定コマンド 23-1
23.1.1 description 23-1
23.1.2 display wlan module-information 23-2
23.1.3 display iot ble neighbor-information 23-3
23.1.4 iot auto-module 23-5
23.1.5 iot auto-module persistent 23-6
23.1.6 iot auto-module persistent all 23-7
23.1.7 module 23-8
23.1.8 module enable 23-9
23.1.9 module firmware-upgrade 23-10
23.1.10 rfid-tracking ble advertisement 23-11
23.1.11 rfid-tracking ble advertisement { disable | enable } 23-13
23.1.12 rfid-tracking ble advertisement interval 23-15
23.1.13 rfid-tracking ble advertisement mode 23-16
23.1.14 rfid-tracking ble aging-time 23-18
23.1.15 tx-power 23-20
23.1.16 type ble 23-21
23.1.17 wlan execute module reset 23-22
23.2 サーバへの IoT データのレポート設定コマンド 23-23
23.2.1 azure-dps group-symmetric-key 23-23
23.2.2 azure-dps id-scope 23-24
23.2.3 display iot transport-profile 23-25
23.2.4 display iot transport-profile in-use 23-26
23.2.5 filter rssi threshold 23-28
23.2.6 filter rssi-fluctuation threshold 23-29
23.2.7 filter recent-packet duration 23-30
23.2.8 filter highest-rssi 23-31
23.2.9 iot transport-profile 23-32
23.2.10 iot-transport-profile 23-33
23.2.11 keepalive interval 23-34
23.2.12 report interval 23-35
23.2.13 server-url 23-36
23.2.14 transport-profile enable 23-37
23.3 ワイヤレスロケーション共通パラメータの設定コマンド 23-38
23.3.1 display wlan rfid-tracking radio 23-38
23.3.2 rfid-tracking client rate-limit 23-39

23.3.3 rfid-tracking client rate-limit cir 23-40
23.3.4 rfid-tracking dilution 23-41
23.3.5 rfid-tracking dilution factor 23-43
23.3.6 rfid-tracking ignore ap-frame 23-44
23.3.7 rfid-tracking ignore beacon 23-45
23.3.8 rfid-tracking keepalive 23-46
23.3.9 rfid-tracking rate-limit 23-48
23.3.10 rfid-tracking rate-limit cir 23-49
23.3.11 rfid-tracking rssi 23-50
23.3.12 rfid-tracking rssi threshold 23-51

23章 IoT 機能の設定

23.1 BLE機能の設定コマンド

🕮 **メモ**:

この章のコマンドは、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

23.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Module view

定義済みユーザロール

network-admin

パラメータ

text: モジュールの説明を指定します。text 引数は大文字と小文字を区別する 1～64 文字の文字列です。

説明

description コマンドはモジュールの説明を指定します。

undo description コマンドはモジュールの説明を削除します。

description コマンドでモジュールの説明を設定することが出来ます。

IoT AP にインストールまたは接続されているモジュールを効率的に管理するには、型番、場所、および機能に基づいたモジュールの説明を設定します。

例

モジュール 1 の説明を L3-office に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] description L3-office

23.1.2 display wlan module-information

Syntax

display wlan module-information { all | ap *ap-name* **{ module all | module** *module-id* **} } [online]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module all: すべてのモジュールを指定します。

module *module-id*: モジュール ID を指定します。*module-id* 引数の値の範囲は、AP モデルによって異なります。

online: オンライン状態のモジュールを指定します。

説明

display wlan module-information コマンドは AP のモジュール情報を表示します。

例

AP ap1 のモジュール 1 に関する情報を表示します。

<AC> display wlan module-information ap ap1 module 1

```
AP name             :1110
Maximum modules      :1
  Module 1:
  Module administrative type    : BLE
  Module physical type         : NEC
  Model                      : T103-MP
  HW version                  : Ver.A
  SW version                  : A1253 V200R001B01D029SP53
```

```
Serial ID                 : 219801A1LHA10A100626
Module MAC                : 0023-89e2-ed76
Module physical status      : Normal
Module administrative status  : Disabled
Description               : Not configured
```

表 23-1

フィールド	説明
Module administrative type	設定されているモジュールタイプ
Module physical type	モジュールの物理タイプ
Model	モジュールの型番。使用可能なモジュールがない場合、このフィールドにはN/Aと表示されます。
HW version	モジュールのハードウェアバージョン
SW version	モジュールのソフトウェアバージョン
Serial ID	モジュールのシリアルID
Module MAC	モジュールのMACアドレス。（H-H-H形式）
Module physical status	物理モジュールの状態： ● Unavailable ● Normal ● Absent
Module administrative status	モジュールの設定状態： ● Enable ● Disable
Description	モジュールの説明

23.1.3 display iot ble neighbor-information

Syntax

display iot ble neighbor-information ap *ap-name* **{ module all | module** *module-id* **| mac** *mac-addr* **}**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module all: すべてのモジュールを指定します。

module *module-id*: モジュール ID を指定します。*module-id* 引数の値の範囲は、AP モデルによって異なります。

mac *mac-addr*: MAC アドレスを指定します。MAC アドレスは、大文字と小文字を区別しない XXXX-XXXX-XXXX 形式の 14 文字の文字列です。各 X は、0~9 の数字または a~f の小文字を表します。

説明

display iot ble neighbor-information コマンドは、AP 周辺の BLE デバイス情報を表示します。

例

AP ap1 周辺の BLE デバイス情報を表示します。

```
<AC> display iot ble neighbor-information ap ap1 module 1
--------------------------------------------------------------------------------
--------
Module ID  MAC address     Address type        RSSI      Last update time
--------------------------------------------------------------------------------
--------
1          1111-2222-AAAA   Public              -5        Mon Nov  2 13:54:23
2021
1          ABAB-CCCC-FFFF   PrivateResolvable    6        Mon Nov  2 13:54:23
2021
```

表 23-2

フィールド	説明
MAC address	BLEデバイスのMACアドレス

フィールド	説明
Address type	アドレスの種類： • Public • Static • PrivateResolvable • PrivateNonResolvable

23.1.4 iot auto-module

Syntax

iot auto-module { disable | enable }

undo iot auto-module

デフォルト

AP view: AP group view の設定を使用します。

AP group view: 無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

enable: 自動モジュール機能を有効にします。

disable: 自動モジュール機能を無効にします。

説明

iot auto-module enable コマンドは自動モジュール機能を有効にします。

iot auto-module disable コマンドは自動モジュール機能を無効にします。

undo iot auto-module コマンドはデフォルトに戻します。

自動モジュール機能を有効にすると、手動モジュールを設定しなくてもモジュールを AP に関連付けることができます。

AP view の設定は、AP group view の設定より優先されます。

例

AP ap1 の自動モジュール機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] iot auto-module enable

#AP group 10 の自動モジュール機能を有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module enable

23.1.5 iot auto-module persistent

Syntax

iot auto-module persistent { disable | enable }

undo iot auto-module persistent

デフォルト

AP view: AP group view の設定を使用します。

AP group view: 無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

enable: 自動モジュール変換機能を有効にします。

disable: 自動モジュール変換機能を無効にします。

説明

iot auto-module persistent enable コマンドは自動モジュール変換機能を有効にします。

iot auto-module persistent disable コマンドは自動モジュール変換機能を無効にします。

undo iot auto-module persistent コマンドはデフォルトに戻します。

自動モジュール変換機能を有効にすると、モジュールがオンラインになった後、自動的に自動モジュールを手動モジュールに変換します。手動モジュールに自動的に変換されるのは、自動モジュール変換機能を有効にした後でオンラインになったモジュールのみで

す。オンライン状態の自動モジュールを手動モジュールに変換する場合は、**iot auto-module persistent all** コマンドを使用します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 の自動モジュール変換機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] iot auto-module persistent enable

#AP group 10 の自動モジュール変換機能を有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module persistent enable

23.1.6 iot auto-module persistent all

Syntax

iot auto-module persistent all

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

iot auto-module persistent all コマンドは、すべてのオンライン状態の自動モジュールを手動モジュールに変換し、変換された各モジュールにシリアル番号を自動的に割り当てます。

例

#AP ap1 のすべてのオンライン状態の自動モジュールを、手動モジュールに変換します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] iot auto-module persistent all

#AP group 10 のすべてのオンライン状態の自動モジュールを、手動モジュールに変換します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module persistent all

23.1.7 module

Syntax

module *module-id*

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

module-id: モジュール ID を指定します。値の範囲は AP モデルによって異なります。

説明

module コマンドは module view に入ります。

例

AP ap1 の module view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1]

#AP group apgroup10 の AP モデル QX-W1110 で、module view に移行します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-apgroup1] ap-model QX-W1110

[AC-wlan-ap-apgroup1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1]

23.1.8 module enable

Syntax

module { disable | enable }

undo module

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 無効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: モジュールを有効にします。

disable: モジュールを無効にします。

説明

module enable コマンドはモジュールを有効にします。

module disable コマンドはモジュールを無効にします。

undo module コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 のモジュールを有効にします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] module enable

#AP group 1 の AP モデル QX-W1110 のモジュールを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] module enable

23.1.9 module firmware-upgrade

Syntax

module firmware-upgrade { disable | enable }

undo module firmware-upgrade

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 有効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: モジュールの自動ファームウェアアップグレードを有効にします。

disable: モジュールの自動ファームウェアアップグレードを無効にします。

説明

module firmware-upgrade enable コマンドはモジュールの自動ファームウェアアップグレードを有効にします。

module firmware-upgrade disable コマンドはモジュールの自動ファームウェアアップグレードを無効にします。

undo module firmware-upgrade コマンドはデフォルトに戻します。

この機能により、ファームウェアバージョンが AP のイメージファイルに保存されているバージョンと異なる場合に、モジュールのファームウェアを自動でアップグレードできます。

モジュールに対してこの機能を有効にすると、モジュールがインストールされている IoT AP が再起動されるたびにこの機能が有効になります。

モジュールファームウェアのアップグレードプロセス中に、shutdown コマンドを使用して、ファームウェアアップグレード中の IoT AP と接続するインターフェイスをシャットダウンしないでください。Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で module1 の、自動ファームウェアアップグレードを有効にします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] module firmware-upgrade enable

#AP group 10 の AP モデル QX-W1110 で、module1 の自動ファームウェアアップグレードを有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1110

[AClan-ap-group-10-ap-model-QX-W1110] module 1

[AClan-ap-group-10-ap-model-QX-W1110-module-1] module firmware-upgrade enable

23.1.10 rfid-tracking ble advertisement

Syntax

rfid-tracking ble advertisement [*ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**

undo rfid-tracking ble advertisement [*ad-number* **] { major-id | measured-power | minor-id | uuid }**

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの ad1 および ad2 のアドバタイズメント情報は、mjor-id は 1、minor-id は 1、measured-power は-58、uuid は E1CC5B618C06428E8720FE619DB80193 です。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

ad-number: アドバタイズメントタイプを指定します。この引数を指定しない場合、ad 1 アドバタイズメントが設定されます。

major-id *major-id*: BLE モジュールのアドバタイズメント情報の Major-ID を指定します。major-id 引数の値の範囲は 0 から 65535 です。

measured-power *measured-power*: BLE モジュールのアドバタイズメント情報の measured-power を指定します。*measured-power* 引数の値の範囲は 0~127 で、0〜-127 dBm の信号強度を表します。measured-power 引数の値が大きいほど信号強度が弱くなります。measured-power は、iBeacon を送信したデバイスから 1 m (3.28 フィート) 離して配置した、受信デバイスで検出される信号強度です。measured-power は、アドバタイズを受信したデバイスと iBeacon 送信デバイス間の距離の計算に使用できます。

minor-id *minor-id*: BLE モジュールのアドバタイズメント情報の Minor-ID を指定します。*minor-id* 引数の値の範囲は 0 から 65535 です。

uuid *uuid*: BLE モジュールのアドバタイズメント情報の uuid を指定します。*uuid* 引数の値の範囲は、大文字と小文字を区別しない 0~f の 32 桁の 16 進数文字列です。

説明

rfid-tracking ble advertisement コマンドは BLE モジュールのアドバタイズメント情報を設定します。

undo rfid-tracking ble advertisement コマンドはデフォルトに戻します。

BLE モジュールは、Major-ID、Minor-ID、Measured-power、UUID を含む iBeacon アドバタイズメントを近くのアプリケーションソフトウェアにブロードキャストします。アドバタイズメントを受信したアプリケーションソフトウェアは、アドバタイズメント情報に応じて特定の動作を行い、ソフトウェア機能を実現します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement major-id 4

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement minor-id 4

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement uuid 34ae56115098ca67321a11256bca3007

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement measured-power 30

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement major-id 4

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement minor-id 4

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement uuid 34ae56115098ca67321a11256bca3007

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement measured-power 30

AP ap 1 上で、BLE モジュール 1 の ad 2 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 major-id 5

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 minor-id 5

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 uuid 44ae56115098ca67321a11256bca3008

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 measured-power 30

AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad 2 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 major-id 5

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 minor-id 5

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 uuid 44ae56115098ca67321a11256bca3008

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 measured-power 30

23.1.11 rfid-tracking ble advertisement { disable | enable }

Syntax

rfid-tracking ble advertisement { disable | enable }

undo rfid-tracking ble advertisement

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 無効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: BLE モジュールの iBeacon 送信機能を有効にします。

disable: BLE モジュールの iBeacon 送信機能を無効にします。

説明

rfid-tracking ble advertisement enable コマンドは BLE モジュールの iBeacon 送信機能を有効にします。

rfid-tracking ble advertisement disable コマンドは BLE モジュールの iBeacon 送信機能を無効にします。

undo rfid-tracking ble advertisement コマンドはデフォルトに戻します。

BLE モジュールが iBeacon ad1 および ad2 アドバタイズメントを定期的にブロードキャストできるようにします。iBeacon アドバタイズメントには、UUID、Major-ID、Minor-ID が含まれます。ad1 または ad2 アドバタイズメントのパラメータを設定するには、rfid-tracking ble advertisement コマンドを使用します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap 1 上の BLE モジュール 1 の iBeacon 送信機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement enable

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の iBeacon 送信機能を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement enable

23.1.12 rfid-tracking ble advertisement interval

Syntax

rfid-tracking ble advertisement [*ad-number* **] interval** *interval*

undo rfid-tracking ble advertisement [*ad-number* **] interval**

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの iBeacon ad1 および ad2 アドバタイズメントをブロードキャストする間隔は 100 センチ秒です。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

ad-number: アドバタイズメントタイプを指定します。この引数を指定しない場合、コマンドは ad1 アドバタイズメントをブロードキャストする間隔を設定します。

interval: BLE モジュールが iBeacon アドバタイズメントをブロードキャストする間隔を 10 の倍数値で指定します。値の範囲は 50~1000 で、単位はセンチ秒です。

説明

rfid-tracking ble advertisement interval コマンドは BLE モジュールが iBeacon をブロードキャストする間隔を設定します。

undo rfid-tracking ble advertisement interval コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメントを 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement interval 200

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement interval 200

AP ap 1 上で、BLE モジュール 1 の ad 2 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 interval 200

AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad 2 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 interval 200

23.1.13 rfid-tracking ble advertisement mode

Syntax

rfid-tracking ble advertisement mode { continuous *ad-number* **| periodic {** *ad-number period* **}&<2> }**

undo rfid-tracking ble advertisement mode

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの iBeacon ad1 のアドバタイズメントを連続モードで送信します。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

continuous: 連続モードを指定します。

ad-number: アドバタイズメントタイプを指定します。

periodic: *periodic モードを指定します。*

{ ad-number period }&<2>: アドバタイズメントタイプとアドバタイズメント期間を 10 の倍数値で指定します。アドバタイズメント期間の範囲は 50～6000 で、単位はセンチ秒です。&<2>は、2 つのアドバタイズメントタイプと 2 つのアドバタイズメント期間を指定する必要があることを示します。

説明

rfid-tracking ble advertisement mode コマンドは BLE アドバタイズメントモードを設定します。

undo rfid-tracking ble advertisement mode コマンドはデフォルトに戻します。

BLE モジュールは、次のモードでアドバタイズメントを送信できます。

- 連続モード: 指定された間隔で 1 種類のアドバタイズメント (ad 1 または ad 2) だけを送信します。
- Periodic モード: 指定した間隔で ad 1 アドバタイズメントと ad 2 アドバタイズメントを交互に送信します。

たとえば、ad1 アドバタイズメント期間が 210 センチ秒、ad2 アドバタイズメント期間が 310 センチ秒、アドバタイズメント間隔がそれぞれ 100 センチ秒の場合、BLE モジュールは、最初に 210 センチ秒の間に 3 つの ad 1 アドバタイズメントを送信し、次に 310 センチ秒の間に 4 つの ad2 アドバタイズメントを送信します。このパターンでは、BLE モジュールは ad1 および ad2 アドバタイズメントを交互に送信します。

アドバタイズメント間隔は、rfid-tracking ble advertisement interval コマンドを使用して設定します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメントを連続モードで送信するように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement mode continuous ad1

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を連続モードで送信するように設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement mode continuous ad1

AP ap 1 上で、BLE モジュール 1 の ad1 および ad2 のアドバタイズメント情報を Periodic モードで送信するように設定します。ad1 のアドバタイズメント期間を 200 センチ秒、ad2 のアドバタイズメント期間を 100 センチ秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement mode periodic ad1 200 ad2 100

AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad1 および ad2 のアドバタイズメント情報を Periodic モードで送信するように設定します。ad1 のアドバタイズメント期間を 200 センチ秒、ad2 のアドバタイズメント期間を 100 センチ秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement mode periodic ad1 200 ad2 100

23.1.14 rfid-tracking ble aging-time

Syntax

rfid-tracking ble aging-time *aging-time*

undo rfid-tracking ble aging-time

デフォルト

AP view: AP group view の設定を使用します。AP group view に設定がない場合、global configuration view の設定を使用します。

AP group view: global configuration view の設定を使用します。

global configuration view: 180 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

aging-time: エージングタイムを 60~3600 秒の範囲で指定します

説明

rfid-tracking ble aging-time コマンドは BLE デバイスのエージングタイムを設定します。

undo rfid-tracking ble aging-time コマンドはデフォルトに戻します。

rfid-tracking ble aging-time コマンドは、BLE デバイスのエージングタイムを設定します。AP view の設定は、AP group view の設定よりも優先されます。AP group view の設定は、グローバル設定 view の設定よりも優先されます

例

AP ap 1 の BLE デバイスのエージングタイムを 60 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ble aging-time 60

AP group 10 の BLE デバイスのエージングタイムを 60 秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] rfid-tracking ble aging-time 60

BLE デバイスのエージングタイムをグローバルで 60 秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] rfid-tracking ble aging-time 60

23.1.15 tx-power

Syntax

tx-power { *power-level* **| value** *power-value* **}**

undo tx-power

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 送信電力レベル 1 です。これは送信電力 4dBm を示します。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

power-level:送信電力レベルを指定します。値は 1、2、3、4 のいずれかで、それぞれ 4 dBm、-1 dBm、-5 dBm、-9 dBm の送信電力を示します。

value *power-value*: 送信電力を指定します。値の範囲は-40 dBm~+8 dBm です。

説明

tx-power コマンドはモジュールの送信電力を設定します。

undo tx-power コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 のモジュール 1 の送信電力レベルを 4 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] tx-power 4

AP group 1 の AP モデル QX-W1110 で、モジュール 1 の送信電力レベルを 4 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] tx-power 4

23.1.16 type ble

Syntax

type ble

undo type

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 設定なし

View

Module view

AP group module view

定義済みユーザロール

network-admin

説明

type ble コマンドは、サポート対象モジュールタイプとして BLE を指定します。

undo type コマンドはデフォルトに戻します。

AP 上のモジュールが正しく動作するには、指定するサポート対象モジュールタイプが物理モジュールタイプと一致している必要があります。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 のモジュール 1 でサポート対象モジュールタイプとして BLE を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] type ble

AP group 1 の AP モデル QX-W1110 で、モジュール 1 のサポート対象モジュールとして BLE を指定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] type ble

23.1.17 wlan execute module reset

Syntax

wlan execute module reset ap *ap-name* **module** *module-id*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module *module-id*: モジュール ID を指定します。module-id 引数の値の範囲は、AP モデルによって異なります。

説明

wlan execute module reset コマンドは AP のモジュールを再起動します。

例

AP ap1 のモジュール 1 を再起動します。

<AC> system-view

[AC] wlan execute module reset ap ap1 module 1

23.2 サーバへのIoTデータのレポート設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

23.2.1 azure-dps group-symmetric-key

Syntax

azure-dps group-symmetric-key { cipher | simple } *string*

undo azure-dps group-symmetric-key

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストで鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、平文形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵の文字列を指定します。暗号テキストの鍵は大文字と小文字を区別する 33～201 の文字列です。プレーンテキストの鍵は大文字と小文字を区別する 1～128 文字の文字列です。

説明

azure-dps group-symmetric-key コマンドは Microsoft Azure IoT Hub DPS のグループ対称キーを設定します。

undo azure-dps group-symmetric-key コマンドはデフォルトに戻します。

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、このコマンドを実行する必要があります。グループ対称キーを編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

例

Microsoft Azure IoT hub DPS のグループ対称キーを、暗号テキストで設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] azure-dps group-symmetric-key cipher OpsBHTTubGabpHTmYbc3w7dKqG9XC6e8OS2apbHRMtVunBkYTY9B/ScyjLeRpf7cjJxXPIsIqna8WV1DePS8uA==

関連コマンド

iot transport-profile

23.2.2 azure-dps id-scope

Syntax

azure-dps id-scope *id-scope*

undo azure-dps *id-scope*

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

id-scope: Microsoft Azure IoT Hub DPS の ID スコープの文字列を指定します。ID スコープは 1～63 文字の文字列です。

説明

azure-dps id-scope コマンドは Microsoft Azure IoT Hub DPS の ID スコープを設定します。

undo azure-dps id-scope コマンドはデフォルトに戻します。

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、このコマンドを実行する必要があります。ID スコープを編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

例

Microsoft Azure IoT hub DPS の ID スコープを 1234567890a として設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] azure-dps id-scope 1234567890a

関連コマンド

iot transport-profile

23.2.3 display iot transport-profile

Syntax

display iot transport-profile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display iot transport-profile コマンドは、IoT トランスポートプロファイルに関する情報を表示します。

IoT トランスポートプロファイルに関する情報を表示するには、まず System view で IoT トランスポートプロファイルを作成する必要があります。

例

作成されたすべての IoT トランスポートプロファイルに関する情報を表示します。

<AC> display iot transport-profile

```
Profile name                Server type          Status
Azureiot1                   Azure                Enabled
Azureiot2                   Azure                Disabled
```

表 23-3

フィールド	説明
Server type	サーバタイプ。サポートされているのはAzureのみ。
Status	IoTトランスポートプロファイルの状態: • Enabled • Disabled

関連コマンド

iot-transport-profile

23.2.4 display iot transport-profile in-use

Syntax

display iot transport-profile in-use

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display iot transport-profile in-use コマンドは、使用中の IoT トランスポートプロファイルに関する情報を表示します。

例

使用中の IoT トランスポートプロファイルに関する情報を表示します。

<AC> display iot transport-profile in-use

```
Connect status: connected
Connected for: 0d 19h 20m 15s
Profile name: aaa
Server URL: global.azure-devices-provisioning.net
Server type: azure iot
Azure DPS information:
  ID scope: 0cn0002B978
  Key type: symmetric
  Group                                                    key(cipher):
$c$3$hQpNztebohdFlXL5p0aVIsA4Hn2QYH5PIWSJDTtZr0mwKW942Erghtscx0aZ3
osazfgmTSZ0PKjz5DavZFpYk6y/ijJqAHC5U+6jIltCjhh2vrRCsh2gNiCnHGpOEr8YH0HJhHOzxE
acd6Q=
  Register ID: sn-210235A3KYC187000028
Report interval: 60 seconds
Keepalive interval: 60 seconds
Total sent messages: 0
Sent BLE data messages: 0
Sent keepalive messages: 0
Total received messages: 0
```

表 23-4

フィールド	説明
Connect status	デバイスとサーバ間の接続の状態: ● connecting－接続試行中 ● connected －接続 ● disconnected－切断
Connected for	サーバとの接続時間
Profile name	IoTトランスポートプロファイル名
Server URL	サーバのURL
Server type	サービスタイプ。現在のソフトウェアではMicrosoft Azure IoT Hub DPSのみをサポートしています。
Azure DPS information	Azure DPSの情報
ID scope	Azure DPSのIDスコープ。
Key type	Azure DPSキーの種類。現在のソフトウェアでは対称キーのみをサポートしています。
Group key(cipher)	Azure DPS登録グループの対称キー。キーは暗号テキストで表示されます。
Register ID	Azure DPSのデバイス登録ID
Report interval	APがIoTデータをサーバにレポートする間隔。単位は秒です。
Keepalive interval	サーバにキープアライブパケットを送信する間隔。単位は秒です。
Total sent messages	送信したメッセージの合計数
Sent BLE data messages	送信したBLEデータメッセージの合計数
Sent keepalive messages	送信したキープアライブメッセージの合計数
Total received messages	受信したメッセージの合計数

23.2.5 filter rssi threshold

Syntax

filter rssi threshold *rssi-threshold*

undo filter rssi threshold

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: ロケーションパケットをフィルタリングするための RSSI しきい値を-127~+20 dBm の範囲で指定します。

説明

filter rssi threshold コマンドはロケーションパケットをフィルタリングするための RSSI しきい値を設定します。

undo filter rssi threshold コマンドはデフォルトに戻します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。
- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

指定された RSSI しきい値を超える RSSI を持つロケーションパケットのみが IoT AP によって受け入れられ、IoT サーバに報告されます。

適切な RSSI しきい値を設定します。値が大きすぎると、大量のロケーションパケットが破棄される可能性があります。値が小さすぎると、最適なパケットフィルタリングパフォーマンスを実現できません。

例

ロケーションパケットをフィルタリングするための RSSI しきい値を-70 dBm に設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-transport-profile-azureiothub] filter rssi threshold -70

23.2.6 filter rssi-fluctuation threshold

Syntax

filter rssi-fluctuation threshold *rssi-threshold*

undo filter rssi-fluctuation threshold

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: ロケーションパケットをフィルタリングするための RSSI 変動しきい値を 1～127 dBm の範囲で指定します。

説明

filter rssi-fluctuation threshold コマンドはロケーションパケットをフィルタリングするための RSSI 変動しきい値を設定します。

undo filter rssi-fluctuation threshold コマンドはデフォルトに戻します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。
- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットのレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

指定された RSSI 変動しきい値以上の RSSI 変動値を持つロケーションパケットのみが IoT AP によって受け入れられ、IoT サーバに報告されます。

適切な RSSI 変動しきい値を設定します。値が大きすぎると、大量のロケーションパケットが破棄される可能性があります。値が小さすぎると、最高のパケットフィルタリングパフォーマンスを実現できません。

例

ロケーションパケットをフィルタリングするための RSSI 変動しきい値を 20 dBm に設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC -iot-transport-profile-azureiothub] filter rssi-fluctuation threshold 20

関連コマンド

iot-transport-profile

23.2.7 filter recent-packet duration

Syntax

filter recent-packet duration *duration*

undo filter recent-packet duration

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

duration: 各レポート間隔の対象となる最新のサブ間隔を指定します。これにより、このサブ間隔よりも前に受信されたロケーションパケットを、詳細なパケットフィルタリングで抑制できます。

説明

filter recent-packet duration コマンドは IoT AP が各レポート間隔の指定された最新のサブ間隔で受信したロケーションパケットのみをレポートできるようにします。

undo filter recent-packet duration コマンドは IoT トランスポートプロファイルを削除します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。

- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットのレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

このコマンドを設定すると、IoT AP は、各レポート間隔の指定された最新のサブ間隔で受信したロケーションパケットのみをレポートします。

各レポート間隔の最新のサブ間隔は、**report interval** コマンドで指定したレポート間隔よりも小さい必要があります。

値が大きすぎると、大量のロケーションパケットが破棄される可能性があります。値が小さすぎると、最適なパケットフィルタリングパフォーマンスを実現できません。

例

各 IoT AP がレポート間隔の最新の 50 秒間に受信したロケーションパケットのみをレポートするように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-transport-profile-azureiothub] filter recent-packet duration 50

関連コマンド

- **iot transport-profile**
- **report interval**

23.2.8 filter highest-rssi

Syntax

filter highest-rssi

undo filter highest-rssi

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

説明

filter highest-rssi コマンドはレポート間隔中に各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみを IoT サーバにレポートするように装置を設定します。

undo filter highest-rssi コマンドはデフォルトに戻します。

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI しきい値。
- RSSI 変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットのレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

このコマンドを設定すると、IoT AP はレポート間隔中に、各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみを IoT サーバにレポートします。レポート間隔を設定するには、**report interval** コマンドを使用します。

例

レポート間隔中に、各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみを IoT サーバにレポートするように IoT AP を設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-transport-profile-azureiothub] filter highest-rssi

関連コマンド

- **iot transport-profile**
- **report interval**

23.2.9 iot transport-profile

Syntax

iot transport-profile *transport-profile-name*

undo iot transport-profile *transport-profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

transport-profile-name: IoT トランスポートプロファイル名を指定します。IoT トランスポートプロファイル名は、大文字、小文字を区別しない 1～63 文字の文字列です。

説明

iot transport-profile コマンドは IoT トランスポートプロファイルを作成し、その View に入るか、既存の IoT トランスポートプロファイル View に入ります。

undo iot transport-profile コマンドは IoT トランスポートプロファイルを削除します。

IoT トランスポートプロファイルには、IoT データを送信する宛先のサーバアドレスや、レポート間隔などを設定します。

IoT トランスポートプロファイルは最大 8 個まで作成できます。

IoT トランスポートプロファイルを削除する場合、事前に IoT トランスポートプロファイルのバインド設定を解除する必要があります。

例

IoT トランスポートプロファイル azureiothub を作成し、その view に移行します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub]

関連コマンド

iot-transport-profile

23.2.10 iot-transport-profile

Syntax

iot-transport-profile *transport-profile-name*

undo iot-transport-profile *transport-profile-name*

デフォルト

設定なし

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

transport-profile-name: IoT トランスポートプロファイル名を指定します。IoT トランスポートプロファイル名は、大文字と小文字は区別しない 1～63 文字の文字列です。

説明

iot-transport-profile コマンドは IoT トランスポートプロファイルをバインドします。

undo iot-transport-profile コマンドはデフォルトに戻します。

オンライン AP は、グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドした後にのみ、IoT データをサーバにレポートします。

既存の IoT トランスポートプロファイル名のみを指定できます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

#グローバルコンフィグレーション View で、IoT トランスポートプロファイル azureiothub をバインドします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] iot-transport-profile azureiothub

関連コマンド

iot transport-profile

23.2.11 keepalive interval

Syntax

keepalive interval *interval*

undo keepalive interval

デフォルト

60 秒

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

interval: キープアライブパケットを送信する間隔を 1~600 秒の範囲で指定します。

説明

keepalive interval コマンドは装置がサーバにキープアライブパケットを送信する間隔を設定します。

undo keepalive interval コマンドはデフォルトに戻します。

例

キープアライブパケットを 50 秒毎にサーバに送信するように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] keepalive interval 50

関連コマンド

iot transport-profile

23.2.12 report interval

Syntax

report interval *interval*

undo report interval

デフォルト

60 秒

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

interval: IoT データをサーバにレポートする間隔を 1~600 秒の範囲で指定します。

説明

report interval コマンドは IoT データをサーバにレポートする間隔を設定します。

undo report interval コマンドはデフォルトに戻します。

レポートする間隔が長すぎるとサービスに影響しますが、間隔を短くすると AC の負荷が増加するため、適切な値を設定する必要があります。

例

50 秒毎に IoT データをサーバにレポートするように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] report interval 50

関連コマンド

iot transport-profile

23.2.13 server-url

Syntax

server-url *server-url-string*

undo server-url

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

server-url-string: サーバの URL を指定します。サーバの URL は、大文字と小文字を区別する 1～127 文字の文字列です。

説明

server-url コマンドは IoT データレポート用のサーバの URL を設定します。

undo server-url コマンドはデフォルトに戻します。

IoT トランスポートプロファイルを有効にする前に、このコマンドを設定する必要があります。

サーバの URL を編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

このコマンドを複数回実行した場合は、最新の設定が有効になります。

例

IoT データレポート用のサーバの URL を global.azure-devices-provisioning.net として設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] server-url global.azure-devices-provisioning.net

関連コマンド

iot transport-profile

23.2.14 transport-profile enable

Syntax

transport-profile enable

undo transport-profile enable

デフォルト

無効

View

IoT transport profile view

定義済みユーザロール

network-admin

説明

transport-profile enable コマンドは IoT トランスポートプロファイルを有効にします。

undo transport-profile enable コマンドはデフォルトに戻します。

例

IoT トランスポートプロファイル azureiothub を有効にします。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] transport-profile enable

関連コマンド

iot transport-profile

23.3 ワイヤレスロケーション共通パラメータの設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

23.3.1 display wlan rfid-tracking radio

Syntax

display wlan rfid-tracking radio [ap *ap-name* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan rfid-tracking radio コマンドは、ワイヤレスロケーションの無線情報を表示します。

例

ワイヤレスロケーションの無線情報を表示します。

<AC> display wlan rfid-tracking radio

```
                    Wireless Locating
--------------------------------------------------------------------------
 AP name                       Radio ID   Type
--------------------------------------------------------------------------
 ap1                           1          MU/Tag
 ap2                           1          MU
 ap3                           2          Tag
 ap4                           1          N/A
--------------------------------------------------------------------------
```

表 23-5 コマンド出力

フィールド	説明
Type	検索するデバイスのタイプ : • MU/Tag : MUデバイスとTagデバイスの両方 • MU : MUデバイス • Tag : Tagデバイス • N/A : 検索するデバイスのタイプが指定されていません

23.3.2 rfid-tracking client rate-limit

Syntax

rfid-tracking client rate-limit { disable | enable }

undo rfid-tracking client rate-limit

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking client rate-limit enable コマンドは AP のワイヤレスパケットの受信レート制限を有効にします。

rfid-tracking client rate-limit disable コマンドは AP のワイヤレスパケットの受信レート制限を無効にします。

undo rfid-tracking client rate-limit コマンドはデフォルトに戻します。

この機能を使用すると、AP は CIR と CBS の両方を超過した場合に、過剰なクライアントパケットからのロケーション情報を報告できなくなります。各クライアントのロケーション情報をロケーションサーバに送信できるようになり、クライアントパケットが AP にフラッディングするのを防ぐことができます。

パケットの間引きが有効になっている場合、この機能は間引きされたパケットのレートを制限します。

例

AP ap1 で、ワイヤレスパケットの受信レート制限を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking client rate-limit enable

AP グループ 1 の AP で、ワイヤレスパケットの受信レート制限を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking client rate-limit enable

グローバルで、ワイヤレスパケットの受信レート制限を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking client rate-limit enable

関連コマンド

rfid-tracking client rate-limit cir

23.3.3 rfid-tracking client rate-limit cir

Syntax

rfid-tracking client rate-limit cir *cir* **[cbs** *cbs* **]**

undo rfid-tracking client rate-limit cir

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: CIR は 0、CBS は 0

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

cir *cir*: 受信ワイヤレスパケットの CIR を 1 から 1300000 kbps の範囲で指定します。

cbs *cbs*: 受信ワイヤレスパケットの CBS を 80 から 130000000 バイトの範囲で指定します。デフォルトの CBS は CIR×700 バイトです。

説明

rfid-tracking client rate-limit cir コマンドはワイヤレスパケットの受信レートの制限値を設定します。

undo rfid-tracking client rate-limit cir コマンドはデフォルトに戻します。

CIR および CBS の設定は、ワイヤレスパケットの受信レート制限を有効にした場合にのみ有効になります。

例

AP ap1 で、受信ワイヤレスパケットの CIR と CBS をそれぞれ 200000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking client rate-limit cir 200000 cbs 50000

AP グループ 1 の AP で、受信ワイヤレスパケットの CIR と CBS をそれぞれ 200000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking client rate-limit cir 200000 cbs 50000

#グローバルで、受信ワイヤレスパケットの CIR と CBS をそれぞれ 200000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking client rate-limit cir 200000 cbs 50000

関連コマンド

rfid-tracking client rate-limit

23.3.4 rfid-tracking dilution

Syntax

rfid-tracking dilution { disable | enable }

undo rfid-tracking dilution

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking dilution enable コマンドは AP のパケットの間引きを有効にします。

rfid-tracking dilution disable コマンドは AP のパケットの間引きを無効にします。

undo rfid-tracking dilution コマンドはデフォルトに戻します。

この機能を使用すると、AP は特定の数のワイヤレスパケットを受信したとき、または特定の間隔でロケーションパケットを送信します。これにより、ロケーションサーバと AP の負荷を軽減することができます。

例

AP ap1 で、パケットの間引きを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking dilution enable

AP グループ 1 の AP で、パケットの間引きを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking dilution enable

グローバルで、パケットの間引き有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking dilution enable

関連コマンド

rfid-tracking dilution factor

23.3.5 rfid-tracking dilution factor

Syntax

rfid-tracking dilution factor *factor* **timeout** *timeout*

undo rfid-tracking dilution factor

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

factor *factor*: パケットの間引き係数を 1～10000 の範囲で指定します。

timeout *timeout*:パケットの間引きタイムアウトタイマを 1~60 秒の範囲で指定します。

説明

rfid-tracking dilution factor コマンドはパケットの間引き係数を設定します。

undo rfid-tracking dilution factor コマンドはデフォルトに戻します。

パケットの間引き係数を 10、タイムアウトタイマを 5 秒に設定した場合、パケットの間引きは次のように動作します。

- AeroScout ロケーションまたは RF フィンガープリントが有効の場合、AP は MU クライアントから、10 個のワイヤレスパケット(管理パケット、ブロードキャストパケットを除く)を受信するたびにロケーションパケットを送信します。タイムアウトのタイマ時間が経過する前に AP が MU クライアントから 10 個のワイヤレスパケットを受信できなかった場合、AP は最新のワイヤレスパケットをロケーションサーバに送信します。
- CUPID ロケーションが有効の場合、AP は関連付けられていないクライアントから 10 個のプローブ要求を受信するたびにロケーション測定を実行します。タイムアウトのタイマが経過する前に AP がアソシエートされていないクライアントから 10 個のプローブ要求を受信できなかった場合、タイマが時間切れになると AP はロケーション測定を実行します。

例

AP ap1 で、パケットの間引き係数を 10、パケットの間引きタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking dilution factor 10 timeout 10

#AP グループ 1 の AP で、パケットの間引き係数を 10、パケットの間引きタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking dilution factor 10 timeout 10

グローバルで、パケットの間引き係数を 10、パケットの間引きタイムアウトタイマを 10 秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking dilution factor 10 timeout 10

関連コマンド

rfid-tracking dilution

23.3.6 rfid-tracking ignore ap-frame

Syntax

rfid-tracking ignore ap-frame { disable | enable }

undo rfid-tracking ignore ap-frame

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking ignore ap-frame enable コマンドは AP フレームの無視を有効にします。

rfid-tracking ignore ap-frame disable コマンドは AP フレームの無視を無効にします。

undo rfid-tracking ignore ap-frame コマンドはデフォルトに戻します。

AP フレームを無視すると、AP は受信した AP フレーム内の情報をロケーションサーバに送信できなくなります。AP フレームは、AP が他の AP から受信したフレームです。この機能は、AP を検索または監視する必要がない場合に設定します。

例

AP ap1 で、AP フレームの無視を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ignore ap-frame enable

AP グループ 1 の AP で、AP フレームの無視を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking ignore ap-frame enable

グローバルで、AP フレームの無視を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking ignore ap-frame enable

23.3.7 rfid-tracking ignore beacon

Syntax

rfid-tracking ignore beacon { disable | enable }

undo rfid-tracking ignore beacon

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking ignore beacon enable コマンドはビーコンフレームの無視を有効にします。

rfid-tracking ignore beacon disable コマンドはビーコンフレームの無視を無効にします。

undo rfid-tracking ignore beacon コマンドはデフォルトに戻します。

ビーコンフレームを無視すると、AP は受信したビーコンフレームをロケーションサーバに送信できなくなります。

ビーコンフレームを無視することで、トラフィックフラッディングを防止します。

例

AP ap1 で、ビーコンフレームの無視を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ignore beacon enable

AP グループ 1 の AP で、ビーコンフレームの無視を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking ignore beacon enable

#グローバルで、ビーコンフレームの無視を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking ignore beacon enable

23.3.8 rfid-tracking keepalive

Syntax

rfid-tracking keepalive { disable | enable }

undo rfid-tracking keepalive

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking keepalive enable コマンドはワイヤレスロケーションのキープアライブを有効にします。

rfid-tracking keepalive disable コマンドはワイヤレスロケーションのキープアライブを無効にします。

undo rfid-tracking keepalive コマンドはデフォルトに戻します。

この機能を有効にすると、AP は 15 秒間隔で Hello パケットをロケーションサーバに送信します。ロケーションサーバが 30 秒以内に AP からパケットを受信しない場合、ロケーションサーバは AP がオフラインであると判断します。

例

AP ap1 で、ワイヤレスロケーションのキープアライブを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking keepalive enable

AP グループ 1 の AP で、ワイヤレスロケーションのキープアライブを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking keepalive enable

グローバルで、ワイヤレスロケーションのキープアライブを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking keepalive enable

23.3.9 rfid-tracking rate-limit

Syntax

rfid-tracking rate-limit { disable | enable }

undo rfid-tracking rate-limit

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking rate-limit enable コマンドは AP のロケーションパケットレート制限を有効にします。

rfid-tracking rate-limit disable コマンドは AP のロケーションパケットレート制限を無効にします。

undo rfid-tracking rate-limit コマンドはデフォルトに戻します。

この機能を使用すると、CIR と CBS の両方が超過した場合に、AP が過剰なロケーションパケットを破棄します。これにより、ロケーションパケットがロケーションサーバにフラッディングするのを防ぐことができます。

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

例

AP ap1 で、ロケーションパケットレート制限を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rate-limit enable

AP グループ 1 の AP で、ロケーションパケットレート制限を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rate-limit enable

グローバルで、ロケーションパケットレート制限を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rate-limit enable

関連コマンド

rfid-tracking client rate-limit cir

23.3.10 rfid-tracking rate-limit cir

Syntax

rfid-tracking rate-limit cir *cir* **[cbs** *cbs* **]**

undo rfid-tracking rate-limit cir

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: CIR は 0、CBS は 0

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

cir *cir*: 受信ワイヤレスパケットの CIR を 8 から 1300000 kbps の範囲で指定します。

cbs *cbs*: 受信ワイヤレスパケットの CBS を 500 から 130000000 バイトの範囲で指定します。デフォルトの CBS は CIR×700 バイトです。

説明

rfid-tracking rate-limit cir コマンドはロケーションパケットの送信レートの制限値を設定します。

undo rfid-tracking rate-limit cir コマンドはデフォルトに戻します。

CIR および CBS の設定は、ロケーションパケットレート制限を有効にした場合にのみ有効になります。

例

AP ap1 で、送信ロケーションパケットの CIR と CBS をそれぞれ 800000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rate-limit cir 800000 cbs 50000

AP グループ 1 の AP で、送信ロケーションパケットの CIR と CBS をそれぞれ 800000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rate-limit cir 800000 cbs 50000

グローバルで、送信ロケーションパケットの CIR と CBS をそれぞれ 800000 kbps と 50000 バイトに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rate-limit cir 800000 cbs 50000

関連コマンド

rfid-tracking client rate-limit

23.3.11 rfid-tracking rssi

Syntax

rfid-tracking rssi { disable | enable }

undo rfid-tracking rssi

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking rssi enable コマンドは RSSI ベースのパケットフィルタリングを有効にします。

rfid-tracking rssi disable コマンドは RSSI ベースのパケットフィルタリングを無効にします。

undo rfid-tracking rssi コマンドはデフォルトに戻します。

RSSI ベースのパケットフィルタリングが有効の場合、AP は RSSI しきい値よりも低い RSSI を持つパケットのロケーション情報を報告しません。この機能により、AP は AP から遠く離れたクライアントを見つけることができなくなります。

例

AP ap1 で、RSSI ベースのパケットフィルタリングを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rssi enable

AP グループ 1 の AP で、RSSI ベースのパケットフィルタリングを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rssi enable

グローバルで、RSSI ベースのパケットフィルタリングを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rssi enable

関連コマンド

rfid-tracking rssi threshold

23.3.12 rfid-tracking rssi threshold

Syntax

rfid-tracking rssi threshold *rssi-threshold*

undo rfid-tracking rssi threshold

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 5 (–123 dBm)

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

threshold *rssi-threshold*: パケットフィルタリングの RSSI しきい値を 5(-123dBm)から 100(-28 dBm) の範囲で指定します。

説明

rfid-tracking rssi threshold コマンドは RSSI ベースのパケットフィルタリングの RSSI しきい値を設定します。

undo rfid-tracking rssi threshold コマンドはデフォルトに戻します。

AP は、指定された RSSI しきい値よりも RSSI が低いパケットの位置情報を報告しません。このコマンドは、RSSI ベースのパケットフィルタリングが有効の場合にのみ有効です。

例

AP ap1 で、RSSI ベースのパケットフィルタリングの RSSI しきい値を 50 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking rssi threshold 50

AP グループ 1 の AP で、RSSI ベースのパケットフィルタリングの RSSI しきい値を 50 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking rssi threshold 50

グローバルで、RSSI ベースのパケットフィルタリングの RSSI しきい値を 50 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking rssi threshold 50

関連コマンド

rfid-tracking rssi

目次

24 章 Hotspot 2.0 の設定 24-1
24.1 Hotspot 2.0 の設定コマンド 24-1
24.1.1 3gpp-info 24-1
24.1.2 authentication-type 24-2
24.1.3 comeback-delay 24-3
24.1.4 description 24-3
24.1.5 dgaf enable 24-4
24.1.6 display wlan hotspot uploaded-osu-icon 24-5
24.1.7 domain-name 24-6
24.1.8 friendly-name 24-7
24.1.9 gas-limit 24-8
24.1.10 hessid 24-8
24.1.11 hotspot-policy 24-9
24.1.12 icon-file 24-10
24.1.13 ip-protocol 24-12
24.1.14 ip-type 24-13
24.1.15 method 24-14
24.1.16 nai 24-15
24.1.17 nai-realm 24-16
24.1.18 nai-realm config-order 24-18
24.1.19 network-type 24-19
24.1.20 operator-name 24-20
24.1.21 osu-provider 24-21
24.1.22 osu-ssid 24-22
24.1.23 policy-name 24-23
24.1.24 roam-oi 24-24
24.1.25 uri 24-25
24.1.26 venue group 24-26
24.1.27 venue name 24-29
24.1.28 wan-metrics 24-30
24.1.29 wlan hotspot-policy 24-31
24.1.30 wlan hotspot osu-icon unload 24-32
24.1.31 wlan hotspot osu-icon upload 24-32
24.1.32 wlan osu-provider 24-33
24.1.33 wlan venue url-unescape-chars 24-34

24章 Hotspot 2.0 の設定

🕮 **メモ：**

Hotspot 2.0 の設定は、QX-W1000 シリーズではソフトウェアバージョン 7.2.74、QX-W1100 シリーズではソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

24.1 Hotspot 2.0の設定コマンド

24.1.1 3gpp-info

Syntax

3gpp-info country-code *mobile-country-code* **network-code** *mobile-network-code*

undo 3gpp-info country-code *mobile-country-code* **network-code**

mobile-network-code

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

mobile-country-code: モバイル国コード(MCC)を指定します。MCC は、クライアントが属する国を一意に識別する 3 桁の数値コードです。

mobile-network-code: モバイルネットワークコード(MNC)を指定します。モバイルネットワークコードは、クライアントが属するモバイルネットワークを一意に識別する 2 桁または 3 桁の数値コードです。

説明

3gpp-info コマンドは 3GPP 情報を設定します。

undo 3gpp-info コマンドは 3GPP 情報を削除します。

Hotspot 2.0 ポリシーでは、最大 32 個の国コードとモバイルネットワークコードの組み合わせを指定できます。

一つの国コードを複数のモバイルネットワークコードと組み合わせることができます。

例

3GPP 情報を設定するため、国コードを 460 に、ネットワークコードを 01 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] 3gpp-info country-code 460 network-code 01

24.1.2 authentication-type

Syntax

authentication-type { **0** [**redirect-url** *url*] | **1** | **2 redirect-url** *url* | **3** }

undo authentication-type { **0** | **1** | **2** | **3** }

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

0: 使用条件への同意を指定します。

1: オンライン登録を指定します。

2: HTTP/HTTPS リダイレクトを指定します。

3: DNS リダイレクトを指定します。

redirect-url *url*: リダイレクトされた URL アドレスを指定します。

説明

authentication-type コマンドはネットワーク認証の種類を指定します。

undo authentication-type コマンドはネットワーク認証の種類を削除します。

Hotspot 2.0 ポリシーには、最大 4 つのネットワーク認証タイプを指定できます。

例

ネットワーク認証タイプを指定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] authentication-type 1

24.1.3 comeback-delay

Syntax

comeback-delay *value*

undo comeback-delay

デフォルト

1 TU

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

value: カムバック遅延を 1 から 1024 TU の範囲で指定します。1TU は 1024 μs に相当します。

説明

comeback-delay コマンドはクライアントが GAS カムバック要求を送信するためのカムバック遅延を設定します。

undo comeback-delay コマンドはデフォルトを復元します。

クライアントが多くの GAS カムバック要求を送信するのを防ぐことができます。

例

カムバック遅延を 10 TU に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] comeback-delay 10

24.1.4 description

Syntax

description *description* **lang-code** *lang-code*

undo description *description* **lang-code** *lang-code*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

description: 説明を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、一般的な国際標準をサポートします。

説明

description コマンドは OSU サーバの説明を設定します。

undo description コマンドは OSU サーバの説明を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

OSU サーバには、最大 32 個の説明を設定できます。クライアントには、クライアントシステムと同じ言語の説明が 1 つ表示されます。

例

OSU サーバ 1 の説明を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] description "Free service for test purpose" lang-code eng

24.1.5 dgaf enable

Syntax

dgaf enable

undo dgaf enable

デフォルト

有効

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

説明

dgaf enable コマンドは Downstream Group-Addressed Forwarding(DGAF)を有効にします。

undo dgaf enable コマンドは DGAF を無効にします。

DGAF を使用すると、AP はすべてのダウンストリームワイヤレスブロードキャスト ARP パケットおよびワイヤレスマルチキャストパケットを転送できます。ダウンストリームマルチキャストを使用したスプーフィング攻撃を防止するには、AP の DGAF を無効にします。

DGAF を無効にする前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認します。

パケット損失を回避するには、DGAF を無効にする前にプロキシ ARP とマルチキャスト最適化を有効にします。プロキシ ARP の詳細については、オペレーションマニュアルのセクション 5 *IP サービス*“*Proxy ARP*”を参照してください。

例

DGAF を無効にします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] undo dgaf enable

24.1.6 display wlan hotspot uploaded-osu-icon

Syntax

display wlan hotspot uploaded-osu-icon

View

Any view

定義済みユーザロール

network-admin

network-operator

説明

display wlan hotspot uploaded-osu-icon コマンドはアップロードされた OSU サーバアイコンのリストを表示します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

例

アップロードされた OSU サーバアイコンのリストを表示します。

<AC> display wlan hotspot uploaded-osu-icon

```
Total uploaded osu icon count: 1
Icon name                       Icon type
--------------------------------------------------------------------------------
college.png                     png
```

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon upload**

24.1.7 domain-name

Syntax

domain-name *domain-name*

undo domain-name *domain-name*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。大文字と小文字が区別される 1 から 255 文字の文字列です。

説明

domain-name コマンドはドメイン名を設定します。

undo domain-name コマンドはドメイン名を削除します。

1 つの Hotspot 2.0 ポリシーでは、最大 32 個のドメイン名を設定できます。

例

Hotspot 2.0 ポリシー1 でドメイン名を college に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] domain-name college

24.1.8 friendly-name

Syntax

friendly-name *friendly-name* **lang-code** *lang-code*

undo friendly-name *friendly-name* **lang-code** *lang-code*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

description: 説明を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、一般的な国際標準をサポートします。

説明

friendly-name コマンドは OSU サーバの名前を設定します。

undo friendly-name コマンドは指定した OSU サーバ名を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。OSU サーバには最大 32 個の名前を設定できます。クライアントには、クライアントシステムと同じ言語の名前が表示されます。

OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、サーバに指定された最新の名前を削除することはできません。

例

OSU サーバ 1 の名前を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] friendly-name osu1 lang-code en

24.1.9 gas-limit

Syntax

gas-limit number *number* **interval** *interval*

undo gas-limit

デフォルト

AC が受信できる GAS 初期要求の数に制限はありません。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

number *number*: AC が受信できる GAS 初期要求の最大数を 10 から 60 の範囲で指定します。

Interval *interval*: AC が GAS 初期要求を受信する間隔を 10 から 60 秒の範囲で指定します。

説明

gas-limit コマンドは AC が指定された間隔内に受信できる GAS 初期要求の最大数を設定します。

undo gas-limit コマンドはデフォルトを復元します。

AC が受信した GAS 初期要求の数が制限を超えた場合、超過したフレームは廃棄されます。

例

AC が 15 秒以内に受信できる GAS 初期要求の最大数を 50 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] gas-limit number 50 interval 15

24.1.10 hessid

Syntax

hessid *hessid*

undo hessid

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

hessid: 同一 ESS を一意に識別する HESSID を H-H-H 形式で指定します。値をすべてゼロにすることはできません。

説明

hessid コマンドは同一 ESS 識別子(HESSID)を設定します。

undo hessid コマンドはデフォルトを復元します。

HESSID を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認してください。

例

Hotspot 2.0 ポリシー1 で HESSID を 0000-5e00-5310 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] hessid 0000-5e00-5310

24.1.11 hotspot-policy

Syntax

hotspot-policy *policy-number*

undo hotspot-policy

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

policy-number: Hotspot 2.0 ポリシーの番号を 1 から 32 の範囲で指定します。

説明

hotspot-policy コマンドは Hotspot 2.0 ポリシーをサービステンプレートにバインドします。

undo hotspot-policy コマンドはデフォルトに戻します。

Hotspot 2.0 ポリシーをサービステンプレートにバインドする場合は、次のガイドラインに従ってください。

- Hotspot 2.0 ポリシーが存在し、サービステンプレートが無効になっていることを確認してください。
- サービステンプレートが次のように設定されていることを確認してください。
  - 802.1X 認証および鍵管理モード
  - RSN IE
  - AES-CCMP 暗号スイート

例

Hotspot 2.0 ポリシー1 をサービステンプレート 1 にバインドします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] hotspot-policy 1

24.1.12 icon-file

Syntax

icon-file *filename* **lang-code** *lang-code* **icon-type** *icon-type*

undo icon-file *filename*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

filename: アイコンファイルを名前で指定します。1 から 63 文字の文字列で、大文字と小文字が区別されます。

lang-code *lang-code*: 言語コードを指定します。デバイスは、一般的な国際標準をサポートしています。

icon-type *icon-type*: アイコンファイルの種類を指定します。1 から 15 文字の文字列で、大文字と小文字が区別されます。

説明

icon-file コマンドは OSU サーバのアイコンを指定します。

undo icon-file コマンドは OSU サーバの指定したアイコンを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

コマンドが実行されると、デバイスは指定されたアイコンを読み込みます。OSU サーバには最大 6 つのアイコンを指定できます。クライアントには、クライアントシステムと同じ言語のアイコンが表示されます。

OSU サーバのアイコンを指定する場合は、次の制限とガイドラインに従ってください。

- バージョンファイルが保存されているルートディレクトリに icon という名前のディレクトリを作成し、FTP または TFTP を使用してアイコンファイルをフォルダにダウンロードしてからコマンドを実行します。
- 指定したアイコンファイルがアイコンディレクトリにない場合、アイコンファイルを読み込めません。アイコンファイルを読み込むには、アイコンディレクトリにアイコンファイルを保存してから、**wlan hotspot osu-icon upload** コマンドを実行してください。
- ファイルサイズは 64 KB を超えることはできません。
- コマンドで指定されたファイルの種類が実際のファイルの種類と同じであることを確認してください。
- OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、最後に指定した OSU サーバのアイコンを削除することはできません。

例

OSU サーバ 1 のアイコンを指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] icon-file test_icon lang-code eng icon-type png

24.1.13 ip-protocol

Syntax

ip-protocol { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number* { **closed** | **open** | **unknown** }

undo ip-protocol { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

esp: ESP プロトコルを指定します。

icmp: ICMP プロトコルを指定します。

tcp: TCP プロトコルを指定します。

udp: UDP プロトコルを指定します。

port-number: ポート番号を指定します。

表 24-1 ポート番号とプロトコル種別

プロトコル種別	ポート番号	説明
ICMP	0	診断で使用されます。
TCP	20	FTPで使用されます。
TCP	22	SSHで使用されます。
TCP	80	HTTPで使用されます。
TCP	443	TLS VPNで使用されます。
TCP	1723	Point to Point Tunneling Protocol VPNで使用されます。
TCP	5060	VoIPで使用されます。
UDP	500	IKEv2(IPSec VPN)で使用されます。
UDP	5060	VoIPで使用されます。
UDP	4500	IKEv2(IPSec VPN)で使用されます。
ESP	0	IPSec VPNで使用されます。

closed: ポートステータスをクローズとして指定します。

open: ポートステータスをオープンとして指定します。

unknown: ポートステータスを不明として指定します。

説明

ip-protocol コマンドは IP プロトコルのポートステータスを設定します。

undo ip-protocol コマンドは設定を削除します。

例

ポート番号を 20 に設定し、TCP のポートステータスをオープンに設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] ip-protocol tcp port-number 20 open

24.1.14 ip-type

🕮 **メモ**:

IPv6 は未サポートです。

Syntax

ip-type ipv4 *ipv4-type* **ipv6** *ipv6-type*

undo ip-type

デフォルト

可用性は、IPv4 アドレスの場合は 1、IPv6 アドレスの場合は 2 です。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

ipv4-type: IPv4 アドレスの可用性を 0～7 の範囲で指定します。

表 24-2 IPv4 アドレスの可用性

アドレス値	説明
0	アドレスの種類は使用できません。
1	使用可能なパブリックIPv4アドレスです。

アドレス値	説明
2	使用可能なポート制限IPv4アドレスです。
3	使用可能な単一NATプライベートIPv4アドレスです。
4	使用可能なダブルNATプライベートIPv4アドレスです。
5	使用可能なポート制限付きIPv4アドレスおよび単一NAT IPv4アドレスです。
6	使用可能なポート制限付きIPv4アドレスおよびダブルNAT IPv4アドレスです。
7	アドレスタイプの可用性が不明です。

ipv6-type: IPv6 アドレスの可用性を 0～2 の範囲で指定します。

表 24-3 IPv6 アドレスの可用性

アドレス値	説明
0	アドレスの種類は使用できません。
1	使用可能なアドレスタイプです。
2	アドレスタイプの可用性が不明です。

説明

ip-type コマンドは IP アドレスの可用性を設定します。

undo ip-type コマンドはデフォルトに戻します。

例

可用性を IPv4 アドレスの場合は 2、IPv6 アドレスの場合は 1 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] ip-type ipv4 2 ipv6 1

24.1.15 method

Syntax

method *method-id*

undo method *method-id*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

method-id: プロトコル ID を指定します。

- 0: OMA-DM を指定します。
- 1: SOAP-XML SPP を指定します。

説明

method コマンドはクライアントが OSU サーバと通信するためのプロトコルを指定します。

undo method コマンドはクライアントが OSU サーバと通信するための指定されたプロトコルを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

両方のプロトコルを指定できます。クライアントは、OSU サーバと通信するためのプロトコルを選択します。

OSU サーバが既に Hotspot 2.0 ポリシーにバインドされている場合は、クライアントが OSU サーバと通信するために指定された最新のプロトコルを削除することはできません。

例

クライアントが OSU サーバと通信するためのプロトコルを指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] method 0

24.1.16 nai

Syntax

nai *nai*

undo nai

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

nai: NAI を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

説明

nai コマンドは OSU サーバのネットワークアクセス識別子(NAI)を設定します。

undo nai コマンドは OSU サーバに設定した NAI を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

OSU サーバに対して NAI が設定されている場合、クライアントは OSEN OSU を介して OSU AP に接続します。OSU サーバに対して NAI が設定されていない場合、クライアントは Open OSU を介して OSU AP に接続します。

例

OSU サーバ 1 の NAI を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] nai abc@example.com

24.1.17 nai-realm

Syntax

nai-realm name *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication*

undo nai-realm name *realm-name* [**eap-method** *eap-method-id* [**auth-method** *auth-method-id* [**authentication** *authentication*]]]

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

name *realm-name*: NAI レルム名を指定します。1 から 255 文字の文字列で、大文字と小文字が区別されます。

eap-method *eap-method-id*: EAP 認証方式を ID で指定します。

表 24-4 EAP 認証方式

eap-method-id	説明
1	EAP-Transport Layer Security (EAP-TLS)
2	Lightweight Extensible Authentication Protocol (LEAP)
3	EAP for GSM Subscriber Identity Module (EAP-SIM)
4	EAP-Tunneled Transport Layer Security (EAP-TTLS)
5	EAP-Authentication and Key Agreement (EAP-AKA)
6	Protected EAP (PEAP)

auth-method *auth-method-id*: 認証方式を ID で指定します。

authentication *authentication*: 認証パラメータを ID で指定します。

表 24-5 認証方式および認証パラメータ

auth-method-id	auth-method-type	authentication
2	Non-EAP Inner Authentication Type	• 1: PAP • 2: CHAP • 3: MSCHAP • 4: MSCHAPV2
5	Credential Type	• 1: SIM • 2: USIM • 3: NFC Secure Element • 4: Hardware Token • 5: Soft Token • 6: Certificate • 7: username/password • 8: none

auth-method-id	auth-method-type	authentication
6	Tunneled EAP Method Credential Type	• 1: SIM • 2: USIM • 3: NFC Secure Element • 4: Hardware Token • 5: Soft Token • 6: Certificate • 7: username/password • 8: Reserved • 9: Anonymous

説明

nai-realm コマンドは NAI レルムを作成し、NAI レルムの認証タイプを指定します。

undo nai-realm コマンドは NAI レルムを削除します。

undo nai-realm コマンドを使用する場合は、次のガイドラインに従ってください。

- **undo nai-realm name** *realm-name* コマンドは、同じ名前を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* コマンドは、同じ名前と EAP 認証方式を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* コマンドは、同じ名前、EAP 認証方式、および認証方式を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication* コマンドは、同じ名前、EAP 認証方式、認証方式、および認証パラメータを使用するすべての NAI レルムを削除します。

Hotspot 2.0 ポリシーには、最大 32 の NAI レルム名を設定できます。

例

Hotspot 2.0 ポリシー1 で NAI レルム test の認証タイプを指定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] nai-realm name test eap-method 2 auth-method 5 authentication 1

24.1.18 nai-realm config-order

Syntax

nai-realm config-order

undo nai-realm config-order

デフォルト

NAI レルムは辞書順に保存されます。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

説明

nai-realm config-order コマンドは NAI レルムが設定された順序で保存されるように設定します。

undo nai-realm config-order コマンドはデフォルトに戻します。

例

設定された順序で NAI レルムを保存するように設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] nai-realm config-order

24.1.19 network-type

Syntax

network-type *network-type* [**access-internet**]

undo network-type

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

network-type: ネットワークタイプを 0 から 5、14、および 15 の範囲で指定します。

表 24-6 アクセスネットワークタイプ

値	説明
0	プライベートネットワーク
1	ゲストアクセスのプライベートネットワーク
2	有料のパブリックネットワーク
3	無料のパブリックネットワーク
4	パーソナルデバイスネットワーク
5	緊急サービス専用ネットワーク
14	テストまたは実験用
15	ワイルドカード

access-internet: インターネットへのアクセスを有効にします。このキーワードを指定しない場合、インターネットにはアクセスできません。

説明

network-type コマンドはアクセスネットワークタイプを設定します。

undo network-type コマンドはデフォルトに戻します。

アクセスネットワークの種類を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認してください。

例

アクセスネットワークの種類を 1 に設定し、インターネットへのアクセスを有効にします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] network-type 1 access-internet

24.1.20 operator-name

Syntax

operator-name *operator-name* **lang-code** *lang-code*

undo operator-name *operator-name* **lang-code** *lang-code*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

operator-name: サービスプロバイダ名を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、ISO 639-1 と ISO 639-2 の両方の規格をサポートしています。

説明

operator-name コマンドはサービスプロバイダ情報を設定します。

undo operator-name コマンドはサービスプロバイダ情報を削除します。

Hotspot 2.0 ポリシーでは、最大 32 個のサービスプロバイダと言語コードの組み合わせを構成できます。

例

サービスプロバイダ example の言語コードを en に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] operator-name example lang-code en

24.1.21 osu-provider

Syntax

osu-provider *osu-provider-number*

undo osu-provider *osu-provider-number*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

osu-provider-number: OSU サーバを 1 から 32 の範囲の番号で指定します。指定された OSU サーバが存在している必要があります。

説明

osu-provider コマンドは OSU サーバを Hotspot 2.0 ポリシーにバインドします。

undo osu-provider コマンドは OSU サーバを Hotspot 2.0 ポリシーからバインド解除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

最大 32 台の OSU サーバを Hotspot 2.0 ポリシーにバインドできます。

OSU サーバを Hotspot 2.0 ポリシーにバインドする前に、次の設定が完了していることを確認してください。

- OSU サーバの名前を設定します。
- OSU サーバの URI を指定します。
- クライアントが OSU サーバと通信するためのプロトコルを指定します。
- OSU サーバのアイコンを指定します。

例

OSU サーバ 1 を Hotspot 2.0 ポリシー1 にバインドします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] osu-provider 1

関連コマンド

- **friendly-name**
- **icon-file**
- **method**
- **uri**
- **wlan osu-provider**

24.1.22 osu-ssid

Syntax

osu-ssid *ssid-name*

undo osu-ssid

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を指定します。1 から 32 文字の文字列で、大文字と小文字が区別されます。

説明

osu-ssid コマンドはオンラインサインアップサービスの SSID を設定します。

undo osu-ssid コマンドはオンラインサインアップサービス用に設定した SSID を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

オンラインサインアップサービス用に構成された SSID が、オンラインサインアップサービステンプレートの SSID と同じであることを確認します。

例

オンラインサインアップサービスの SSID を osu に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] osu-ssid osu

24.1.23 policy-name

Syntax

policy-name *name*

undo policy-name

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

name: Hotspot 2.0 ポリシー名を 1 から 32 文字の大文字と小文字を区別しない文字列で指定します。

説明

policy-name コマンドは Hotspot 2.0 ポリシーの名前を設定します。

undo policy-name コマンドはデフォルトを復元します。

例

Hotspot 2.0 ポリシー1 の名前を market に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] policy-name market

24.1.24 roam-oi

Syntax

roam-oi *oi* [**in-beacon**]

undo roam-oi *oi*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

oi: ローミングコンソーシアムを一意に識別できる OI を、6 桁または 10 桁の 16 進数で指定します。

in-beacon: ビーコンに OI を追加します。ベストプラクティスとして、クライアントが OI を取得するには、このキーワードを指定します。

説明

roam-oi コマンドは組織識別子(OI)を設定します。

undo roam-oi コマンドは OI を削除します。

OI を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認します。Hotspot 2.0 ポリシーでは最大 32 の OI を構成でき、ビーコンには最大 3 つの OI を追加できます。

例

OI を 004096 に設定し、ビーコンに OI を追加します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] roam-oi 004096 in-beacon

24.1.25 uri

Syntax

uri *uri*

undo uri

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

uri: OSU サーバの URI を指定します。1 から 255 文字の文字列で、大文字と小文字が区別されます。

説明

uri コマンドは OSU サーバの URI を指定します。

undo uri コマンドは OSU サーバの構成済み URI を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。クライアントは、構成された URI を使用して OSU サーバにアクセスし、オンラインサインアップを実行します。

OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、サーバの構成された URI を削除することはできません。

例

OSU サーバ 1 の URI を指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] uri https://osu-server.example.org/

24.1.26 venue group

Syntax

venue group *venue-group-number* **type** *venue-type-number*

undo venue group

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

venue-group-number: 場所グループを番号で指定します。範囲は 1 から 11 です。

表 24-7 場所グループの番号と説明

番号	説明
1	アセンブリ
2	ビジネス
3	教育
4	工場
5	施設
6	商業施設
7	住宅
8	倉庫
9	公共施設
10	車両
11	屋外

venue-type-number: 番号で場所タイプを指定します。値は場所グループ番号によって異なります。詳細については、表 22-8 を参照してください。

表 24-8 場所タイプ番号と説明

場所グループ番号	場所タイプ番号	場所説明
1	0	未指定
1	1	アリーナ
1	2	スタジアム
1	3	旅客ターミナル
1	4	円形劇場
1	5	遊園地
1	6	礼拝所
1	7	会議場
1	8	図書館
1	9	博物館
1	10	レストラン
1	11	劇場
1	12	バー
1	13	喫茶店
1	14	動物園または水族館
1	15	緊急対応センター
2	0	未指定
2	1	医師又は歯科医師の診療所
2	2	銀行
2	3	消防署
2	4	警察署
2	6	郵便局
2	7	専門オフィス
2	8	研究開発施設
2	9	弁護士事務所
3	0	未指定
3	1	小学校
3	2	中学校
3	3	大学
4	0	未指定
4	1	工場
5	0	未指定
5	1	病院
5	2	介護老人保健施設

場所グループ番号	場所タイプ番号	場所説明
5	3	アルコール・薬物リハビリテーションセンター
5	4	グループホーム
5	5	刑務所または拘置所
6	0	未指定
6	1	小売店
6	2	食料品市場
6	3	自動車サービスステーション
6	4	ショッピングモール
6	5	ガソリンスタンド
7	0	未指定
7	1	個人住宅
7	2	ホテルまたはモーテル
7	3	宿舎
7	4	下宿
8	0	未指定
9	0	未指定
10	0	未指定
10	1	自動車またはトラック
10	2	飛行機
10	3	バス
10	4	フェリー
10	5	船またはボート
10	6	電車
10	7	モーターバイク
11	0	未指定
11	1	自治体メッシュネットワーク
11	2	市立公園
11	3	休憩施設
11	4	交通管制施設
11	5	バス停
11	6	売店

説明

venue group コマンドは AP の場所グループ情報を設定します。

undo venue group コマンドはデフォルトに戻します。

例

AP ap3 の場所グループ 1 および場所タイプ 2 を指定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] venue group 1 type 2

24.1.27 venue name

Syntax

venue name *venue-name* **lang-code** *lang-code* [**url** *url*]

undo venue name *venue-name* **lang-code** *lang-code* [**url** *url*]

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

venue-name: 場所名を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 場所の言語コードを指定します。デバイスは、ISO 639-1 と ISO 639-2 の両方の標準をサポートしています。

url: AP が属する場所の URL を指定します。1 から 63 文字の文字列で、大文字と小文字は区別されません。URL アドレスには疑問符 (?) を含めることができます。

説明

venue name コマンドは AP の場所名を設定します。

undo venue name コマンドは場所名を削除します。

一つの場所に複数の言語コードを設定できます。

AP には、最大 32 個の場所名と言語コードの組み合わせを設定できます。

このコマンドで指定する URL は、標準の HTTP または HTTPS プロトコルを介してアクセスでき、http://または https://で始まる必要があります。

例

AP ap3 の場所名を office に、言語コードを en に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] venue name office lang-code en

AP ap1 の場所名を v1 に、言語コードを en に、場所 URL を http://www.example.com に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1120

[AC-wlan-ap-ap1] venue name v1 lang-code en url http://www.example.com

24.1.28 wan-metrics

Syntax

wan-metrics { **link-down** | **link-test** | **link-up** } [**asymmetric downlink-speed** *downlink-speed* **uplink-speed** *uplink-speed* | **symmetric link-speed** *link-speed*]

undo wan-metrics

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

link-down: WAN のリンクステータスを down に設定します。

link-test: WAN のリンクステータスを testing に設定します。

link-up: WAN のリンクステータスを up に設定します。

asymmetric: 非対称リンクを指定します。

downlink-speed *downlink-speed*: ダウンリンクの速度を 1 から 4194304 Kbps の範囲で指定します。

uplink-speed *uplink-speed*: アップリンクの速度を 1 から 4194304 Kbps の範囲で指定します。

symmetric: 対称リンクを指定します。

link-speed *link-speed*: 対称リンクの速度を 1 から 4194304 Kbps の範囲で指定します。

説明

wan-metrics コマンドは WAN リンクステータスパラメータを設定します。

undo wan-metrics コマンドはデフォルトに戻します。

例

WAN のリンクステータスをアップに、対称リンクレートを 67 Kbps に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] wan-metrics link-up symmetric link-speed 67

24.1.29 wlan hotspot-policy

Syntax

wlan hotspot-policy *policy-number*

undo wlan hotspot-policy *policy-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-number: Hotspot 2.0 ポリシーの番号を 1 から 32 の範囲で指定します。

説明

wlan hotspot-policy コマンドは Hotspot 2.0 ポリシーを作成してそのビューを開始するか、既存の Hotspot 2.0 ポリシーのビューを開始します。

undo wlan hotspot-policy コマンドは Hotspot 2.0 ポリシーを削除します。

サービステンプレートにバインドされている Hotspot 2.0 ポリシーは削除できません。

例

Hotspot 2.0 ポリシー1 を作成し、そのビューに入ります。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1]

24.1.30 wlan hotspot osu-icon unload

Syntax

wlan hotspot osu-icon unload

View

System view

定義済みユーザロール

network-admin

説明

wlan hotspot osu-icon unload コマンドはすべての OSU サーバアイコンファイルをアンロードします。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

このコマンドは、OSU サーバアイコンファイルをアンロードするだけで、アイコンファイルは削除されません。

例

すべての OSU サーバアイコンファイルをアンロードします。

<AC> system-view

[AC] wlan hotspot osu-icon unload

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon upload**

24.1.31 wlan hotspot osu-icon upload

Syntax

wlan hotspot osu-icon upload

View

System view

定義済みユーザロール

network-admin

説明

wlan hotspot osu-icon upload コマンドは指定したすべての OSU サーバアイコンファイルをロードします。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

このコマンドを使用して、OSU サーバに指定されたすべてのアイコンファイルを読み込み、アイコンファイルの変更が発生したときに変更を検証します。

例

指定した OSU サーバのアイコンファイルをすべて読み込みます。

<AC> system-view

[AC] wlan hotspot osu-icon upload

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon unload**

24.1.32 wlan osu-provider

Syntax

wlan osu-provider *osu-provider-number*

undo wlan osu-provider *osu-provider-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

osu-provider-number: OSU サーバを 1 から 32 の範囲の番号で指定します。

説明

wlan osu-provider コマンドは OSU サーバを作成してそのビューを開始するか、既存の OSU サーバのビューを開始します。

undo wlan osu-provider コマンドは指定した OSU サーバを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

Hotspot 2.0 ポリシーにバインドされている OSU サーバを削除することはできません。

例

OSU サーバ 1 を作成し、そのビューを入力します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1]

24.1.33 wlan venue url-unescape-chars

Syntax

wlan venue url-unescape-chars { **composition1** | **composition2** | **custom** *character-string* }

undo wlan venue url-unescape-chars [**custom** *character-string*]

デフォルト

composition1

View

System view

定義済みユーザロール

network-admin

説明

wlan venue url-unescape-chars コマンドは場所 URL のエスケープから特定の特殊文字を除外できます。

undo wlan venue url-unescape-chars コマンドは場所 URL のエスケープから除外された特殊文字を削除できます。

クライアントが特殊文字を構文またはコマンドとして解釈し、意図した意味を変更しないようにするには、これらの文字を安全な形式 (エスケープ文字) に変換する必要があります。

実際には、サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、エラーが発生することがあります。このような場合は、このタスクを実行して、特定の特殊文字をエスケープから除外できます。

場所 URL では、大文字と小文字および数字以外の文字はエスケープする必要がなく、このコマンドを使用して残りの特殊文字を構成できます。

デフォルトでは、デバイスは composition1 の特殊文字をエスケープしません。

サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、例外が発生する場合があります。これに対処するには、これらの特定の文字がエスケープされないように機能を構成します。

例

場所 URL でのエスケープから composition2 の特殊文字を除外します。

<AC> system-view

[AC] wlan venue url-unescape-chars composition2

特殊文字を除く;() が場所 URL でエスケープされないようにします。

<AC> system-view

[AC] wlan venue url-unescape-chars custom ;()