リモート LAN

リモート LAN について

リモート LAN（RLAN）は、コントローラを使用する有線クライアントの認証に使用されます。有線クライアントがコントローラに正常に接続すると、LAN ポートは中央スイッチング モードとローカル スイッチング モードの間でトラフィックをスイッチングします。有線クライアントからのトラフィックは、ワイヤレス クライアント トラフィックとして扱われます。

アクセス ポイント（AP）の RLAN は、有線クライアントを認証するための認証要求を送信します。RLAN での有線クライアントの認証は、ワイヤレス クライアントの中央認証に似ています。

（注） RLAN は、複数のイーサネット ポートを備えた AP でサポートされています。

サポートされる AP モデルは次のとおりです。

- Cisco Aironet OEAP 1810 および 1815T シリーズ
- Cisco Aironet 1810w および 1815w シリーズ
- Cisco Aironet 702w シリーズ

（注） Cisco Aironet 702w シリーズ AP に接続されているオープン認証 RLAN クライアントは、有線クライアントとして機能します。したがって、次の show コマンドを実行しても、これらのクライアントの IP アドレスと統計情報は表示されません。

- show wireless client summary
- show wireless client mac *mac_address* detail

イーサネット（AUX）ポートについて

Cisco Aironet 1850、2800、および 3800 シリーズ AP では、2 番目のイーサネット ポートがデフォルトでリンク集約（LAG）ポートとして使用されます。この LAG ポートは LAG が無効になっている場合に RLAN ポートとして使用できます。

次の AP は、LAG ポートを RLAN ポートとして使用します。

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I
- 3802P

Cisco 2700 アクセス ポイントでの AUX ポートの使用に関する制限事項

- RLAN は、このポートの AUX ポートおよび非ネイティブ VLAN をサポートしています。
- ローカル モードでは、中央スイッチの有線クライアント トラフィックがサポートされます。一方、Flexconnect モードでは中央スイッチはサポートされません。
- Flexconnect モードでは、ローカル スイッチの有線クライアント トラフィックはサポートされますが、中央スイッチについてはサポートされません。
- AUX ポートをトランク ポートとして使用することはできません。ポートの背後にスイッチまたはブリッジを追加することもできません。
- AUX ポートは dot1x をサポートしていません。

コントローラの役割

- コントローラはオーセンティケータとして機能し、有線クライアントからの Extensible Authentication Protocol（EAP）over LAN（EAPOL）メッセージは AP 経由でコントローラに到達します。
- コントローラは、設定された認証、認可、およびアカウンティング（AAA）サーバと通信します。
- コントローラは AP 用の LAN ポートを設定し、対応する AP にプッシュします。

リモート LAN（RLAN）の設定

すべての RLAN の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] ap remote-lan shutdown** 例： `Device(config)# [no] ap remote-lan shutdown`	すべての RLAN を有効または無効にします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RLAN プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap remote-lan profile-name** *remote-lan-profile-name rlan-id* 例： `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	リモート LAN プロファイルを設定します。 • *remote-lan-profile*：リモート LAN プロファイル名です。範囲は英数字で 1 ～ 32 文字です。 • *rlan-id*：リモート LAN の識別子です。範囲は 1 ～ 128 です。

	コマンドまたはアクション	目的
		（注） 最大 128 の RLAN を作成できます。既存の RLAN の *rlan id* を別の RLAN の作成時に使用することはできません。 RLAN と WLAN の両方のプロファイルに同じ名前を付けることはできません。同様に、RLAN と WLAN のポリシープロファイルに同じ名前を付けることはできません。

RLAN プロファイル パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Remote LAN]** を選択します。

ステップ 2 [RLAN Profile] タブで [Add] をクリックします。

[Add RLAN Profile] ウィンドウが表示されます。

ステップ 3 [General] タブで次の手順を実行します。

a) RLAN プロファイルの [Name] と [RLAN ID] を入力します。

b) [Client Association Limit] フィールドで RLAN ごとのクライアント接続数を設定します。

範囲は 0 ～ 10000 です。0 は無制限のクライアント接続を意味します。

c) プロファイルを有効にするには、ステータスを [Enable] に設定します。

ステップ 4 **[Security]** > **[Layer2]** タブで次の手順を実行します。

a) RLAN の 802.1x を有効にするには、[802.1x] ステータスを [Enabled] に設定します。

（注） Web 認証リストまたは 802.1x 認証リストを同時にアクティブにできます。

b) [MAC Filtering] ドロップダウンリストから、許可リスト名を選択します。

c) [Authentication List] ドロップダウンリストから RLAN 認証リスト名に対して 802.1x を選択します。

ステップ 5 **[Security]** > **[Layer3]** タブで次の手順を実行します。

a) RLAN の Web 認証を有効にするには、[Web Auth] ステータスを [Enabled] に設定します。

（注） Web 認証リストまたは 802.1x 認証リストを同時にアクティブにできます。

b) [Webauth Parameter Map] ドロップダウンリストから、Web 認証パラメータ マップを選択します。

c) [Authentication List] ドロップダウンリストから Web 認証リスト名を選択します。

ステップ 6 **[Security]** > **[AAA]** タブで次の手順を実行します。

a) [Local EAP Authentication] を [enabled] に設定します。また、必要な [EAP Profile Name] をドロップダウンリストから選択します。

ステップ 7 設定を保存します。

RLAN プロファイル パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**client association limit** *client-connections* 例： `Device(config-remote-lan)# client association limit 1`	RLAN ごとのクライアント接続数を設定します。 *client-connections*：RLAN ごとの最大クライアント接続数。範囲は 0 ～ 10000 です。0 は無制限を意味します。
ステップ 2	**ip access-group web** *IPv4-acl-name* 例： `Device(config-remote-lan)# ip access-group web acl_name`	RLAN IP コンフィギュレーション コマンドを設定します。 *IPv4-acl-name*：IPv4 ACL の名前または ID を指します。
ステップ 3	**local-auth** *profile name* 例： `Device(config-remote-lan)# local-auth profile_name`	RLAN で EAP プロファイルを設定します。 *profile name*：RLAN 上の EAP プロファイルです。
ステップ 4	**mac-filtering** *mac-filter-name* 例： `Device(config-remote-lan)# mac-filtering mac_filter`	RLAN で MAC フィルタリング サポートを設定します。 *mac-filter-name*：許可リスト名です。
ステップ 5	**security dot1x authentication-list** *list-name* 例： `Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list`	RLAN の 802.1X を設定します。 *list-name*：認証リスト名です。
ステップ 6	**security web-auth authentication-list** *list-name* 例：	RLAN の Web 認証を設定します。 *list-name*：認証リスト名です。

	コマンドまたはアクション	目的
	`Device(config-remote-lan)# security web-auth authentication-list web_auth_list`	（注） Web 認証リストまたは dot1x 認証リストを同時にアクティブにできます。
ステップ 7	**[no] shutdown** 例： `Device(config-remote-lan)# shutdown`	RLANプロファイルを有効または無効にします。
ステップ 8	**end** 例： `Device(config-remote-lan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 （注） この項の設定は、RLAN プロファイルに必須ではありません。 中央スイッチング モードの場合は、中央スイッチングと中央 DHCP の両方を設定する必要があります。

RLAN ポリシー プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap remote-lan-policy policy-name** *profile name* 例： `Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name`	RLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。

RLAN ポリシー プロファイル パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Remote LAN]** を選択します。

ステップ 2 [Remote LAN] ページで [RLAN Policy] タブをクリックします。

ステップ 3 [RLAN Policy] ページで、[Policy] の名前をクリックするか、[Add] をクリックして新しいポリシーを作成します。

[Add/Edit RLAN Policy] ウィンドウが表示されます。

ステップ 4 [General] タブで次の手順を実行します。

a) ポリシー プロファイルの [Name] と [Description] を入力します。
b) [Central Authentication] を [Enabled] 状態に設定します。
c) [Central DHCP] を [Enabled] 状態に設定します。
d) [PoE] チェック ボックスを有効または無効の状態に設定します。
e) ポリシーを有効にするには、ステータスを [Enable] に設定します。

ステップ 5 [Access Policies] タブで、[VLAN] ドロップダウンリストから VLAN 名または番号を選択します。

ステップ 6 [Host Mode] ドロップダウンリストで、次のオプションからリモート LAN 802.1x の [Host Mode] を選択します。

- [Single-Host Mode]：デフォルトのホスト モードです。このモードでは、スイッチ ポートは 1 つのホストだけを認証し、トラフィックを 1 つずつ通過させます。
- [Multi-Host Mode]：最初に認証するデバイスがスイッチ ポートを開き、他のすべてのデバイスがそのポートを使用できます。他のデバイスを個別に認証する必要はありません。認証されたデバイスが承認済み状態になると、スイッチ ポートは閉じられます。
- [Multi-Domain Mode]：オーセンティケータは、データ ドメインの 1 つのホストと、音声ドメインの別のホストを許可します。これは、IP フォンが接続されているスイッチ ポートの一般的な設定です。

ステップ 7 IPv6 ACL または Flexible Netflow を設定します。

- **[Access Policies]** > **[Remote LAN ACL]** セクションで、ドロップダウンリストから [IPv6 ACL] を選択します。
- **[Access Policies]** > **[AVC]** > **[Flow Monitor IPv6]** セクションで、[Egress Status] と [Ingress Status] のチェック ボックスをオンにしてドロップダウンリストからポリシーを選択します。

ステップ 8 [Advanced] タブをクリックします。

a) [Violation Mode] ドロップダウンリストから、リモート LAN 802.1x の違反モードを設定し、次のオプションから違反モード タイプを選択します。

- [Shutdown]：ポートを無効にします。
- [Replace]：現在のセッションを削除し、新しいホストの認証を開始します。これはデフォルトの動作です。
- [Protect]：システム メッセージを生成せずに、予期しない MAC アドレスを使用するパケットをドロップします。

b) [Session Timeout (sec)] の値を入力して、クライアントのセッション期間を定義します。

範囲は 20 ～ 86400 秒です。

c) [AAA Policy Params] セクションで、[AAA Override] チェック ボックスをオンにして AAA オーバーライドを有効にします。

d) [Exclusionlist Params] セクションで、[Exclusionlist] チェック ボックスをオンにして [Exclusionlist Timeout] の値を入力します。

これにより、クライアントの除外時間が設定されます。範囲は 0 ～ 2147483647 秒です。0 はタイムアウトしないことを意味します。

ステップ 9 設定を保存します。

RLAN ポリシー プロファイル パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**central switching** 例： `Device(config-remote-lan-policy)# central switching`	中央スイッチングを設定します。
ステップ 2	**central dhcp** 例： `Device(config-remote-lan-policy)# central dhcp`	中央 DHCP を設定します。
ステップ 3	**exclusionlist timeout** *timeout* 例： `Device(config-remote-lan-policy)# exclusionlist timeout 200`	RLAN で除外リストを設定します。 *timeout*：クライアントが除外状態になるまでの時間を設定します。範囲は 0 ～ 2147483647 秒です。0 はタイムアウトしないことを意味します。
ステップ 4	**vlan** *vlan* 例：	VLAN 名または ID を設定します。 - *vlan*：VLAN 名です。

	コマンドまたはアクション	目的
	`Device(config-remote-lan-policy)# vlan vlan1`	
ステップ 5	例： `Device(config-remote-lan-policy)# ipv6 acl ipv6_acl`	
ステップ 6	**aaa-override** 例： `Device(config-remote-lan-policy)# aaa-override`	AAA ポリシーのオーバーライドを設定します。
ステップ 7	**session-timeout** *timeout in seconds* 例： `Device(config-remote-lan-policy)# session-timeout 21`	クライアントのセッション タイムアウトを設定します。 *timeout in seconds*：セッション期間を定義します。範囲は 20 ～ 86400 秒です。
ステップ 8	**host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**} 例： `Device(config-remote-lan-policy)# host-mode multidomain`	リモート LAN 802.1x のホスト モードを設定します。 *voice domain*：RLAN 音声ドメインの VLAN ID です。範囲は 0 ～ 65535 です。 次の IEEE 802.1X 認証モードを設定できます。 • [Multi-Domain Mode]：オーセンティケータは、データ ドメインの 1 つのホストと、音声ドメインの別のホストを許可します。これは、IP フォンが接続されているスイッチ ポートの一般的な設定です。 • [Multi-Host Mode]：最初に認証するデバイスがスイッチ ポートを開き、他のすべてのデバイスがそのポートを使用できます。他のデバイスを個別に認証する必要はありません。認証されたデバイスが承認済み状態になると、スイッチ ポートは閉じられます。 • [Single-Host Mode]：デフォルトのホスト モードです。このモードでは、スイッチ ポートは 1 つのホス

	コマンドまたはアクション	目的
		トだけを認証し、トラフィックを 1 つずつ通過させます。
ステップ 9	**violation-mode** {**protect** | **replace** | **shutdown**} 例： `Device(config-remote-lan-policy)# violation-mode protect`	リモート LAN 802.1x の違反モードを設定します。 セキュリティ違反が発生すると、ポートは、次のような設定済みの違反アクションに基づいて保護されます。 • [Shutdown]：ポートを無効にします。 • [Replace]：現在のセッションを削除し、新しいホストの認証を開始します。これはデフォルトの動作です。 • [Protect]：システム メッセージを生成せずに、予期しない MAC アドレスを使用するパケットをドロップします。シングルホスト認証モードでは、データ VLAN で複数のデバイスが検出された場合に違反がトリガーされます。マルチホスト認証モードでは、データ VLAN または音声 VLAN で複数のデバイスが検出された場合に違反がトリガーされます。
ステップ 10	[**no**] **poe** 例： `Device(config-remote-lan-policy)# poe`	PoE を有効または無効にします。
ステップ 11	[**no**] **shutdown** 例： `Device(config-remote-lan-policy)# shutdown`	RLAN ポリシー プロファイルを有効または無効にします。
ステップ 12	**end** 例： `Device(config-remote-lan-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー タグの設定と RLAN ポリシー プロファイルの RLAN プロファイルへのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy remote-lan-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id* 例： `Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2`	RLAN ポリシー プロファイルを RLAN プロファイルにマッピングします。 • *remote-lan-profile-name*：RLAN プロファイルの名前です。 • *rlan-policy-profile-name*：ポリシー プロファイルの名前です。 • *port-id*：アクセス ポイントの LAN ポート番号です。指定できる値の範囲は 1 ～ 4 です。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LAN ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap name* **lan port-id** *lan port id* {**disable** | **enable**} 例： `Device# ap name L2_1810w_2 lan port-id 1 enable`	LAN ポートを設定します。 • enable：LAN ポートを有効にします。

	コマンドまたはアクション	目的
		• disable：LAN ポートを無効にします。

アクセス ポイントへのポリシー タグの付加（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] の順に選択します。
ステップ 2 ポリシー タグを付加する AP を選択します。
ステップ 3 [Tags] セクションで、[Policy] ドロップダウンを使用してポリシー タグを選択します。
ステップ 4 [Update & Apply to Device] をクリックします。

アクセス ポイントへのポリシー タグの付加（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ap** *ap-ethernet-mac* 例： `Device(config)# ap 00a2.891c.21e0`	AP のマップ アドレスを設定し、AP コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag remote-lan-policy-tag`	アクセス ポイントにポリシータグを付加します。 *policy-tag-name*：以前に定義したポリシー タグの名前です。
ステップ 4	**end** 例： `Device(config-ap-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RLAN 設定の確認

すべての RLAN の概要を表示するには、次のコマンドを使用します。

```
Device# show remote-lan summary

Number of RLANs: 1

RLAN        Profile Name                      Status
------------------------------------------------------------------
1            rlan_test_1                       Enabled
```

ID 別に RLAN 設定を表示するには、次のコマンドを使用します。

```
Device# show remote-lan id <id>

Remote-LAN Profile Name              : rlan_test_1
=================================================
Identifier                                : 1
Status                                    : Enabled
Mac-filtering                             : Not Configured
Number of Active Clients                  : 1
Security_8021X                            : Disabled
8021.x Authentication list name           : Not Configured
Local Auth eap Profile Name               : Not Configured
Web Auth Security                         : Disabled
Webauth Authentication list name          : Not Configured
Web Auth Parameter Map                    : Not Configured
Client association limit                  : 0
Ipv4 Web Pre Auth Acl                     : Not Configured
Ipv6 Web Pre Auth Acl                     : Not Configured
```

プロファイル名別に RLAN 設定を表示するには、次のコマンドを使用します。

```
Device# show remote-lan name <profile-name>

Remote-LAN Profile Name                   : rlan_test_1
=========================================================
Identifier                                : 1
Status                                    : Enabled
Mac-filtering                             : Not Configured
Number of Active Clients                  : 1
Security_8021X                            : Disabled
8021.x Authentication list name           : Not Configured
Local Auth eap Profile Name               : Not Configured
Web Auth Security                         : Disabled
Webauth Authentication list name          : Not Configured
Web Auth Parameter Map                    : Not Configured
Client association limit                  : 0
Ipv4 Web Pre Auth Acl                     : Not Configured
Ipv6 Web Pre Auth Acl                     : Not Configured
```

すべての RLAN の詳細な出力を表示するには、次のコマンドを使用します。

```
Device# show remote-lan all

Remote-LAN Profile Name            : rlan_test_1
=================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
```

```
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name            : rlan_test_2
================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                      Description                              Status

-------------------------------------------------------------------------------------------
rlan_named_pp1                Testing RLAN policy profile              Enabled
```

Cisco AP の LAN ポート設定を表示するには、次のコマンドを使用します。

```
Device# show ap name <ap_name> lan port summary
LAN Port status for AP L2_1815w_1
Port ID      status       vlanId      poe
---------------------------------------------
LAN1         Enabled       20          Disabled
LAN2         Enabled       20          NA
LAN3         Disabled      0           NA
```

すべてのクライアントの概要を表示するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1

MAC Address       AP Name         WLAN         State    Protocol    Method     Role
-------------------------------------------------------------------------------------------
d8eb.97b6.fcc6    L2_1815w_1      1            * Run     Ethernet    None      Local
```

ユーザ名を指定してクライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless client username cisco
MAC Address        AP Name          Status      WLAN      Auth Protocol
-------------------------------------------------------------------------------------------
0014.d1da.a977    L2_1815w_1        Run 1 *      Yes        Ethernet
d8eb.97b6.fcc6    L2_1815w_1        Run 1 *      Yes        Ethernet
```

MAC アドレス別にクライアントの詳細情報を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address <mac_address> detail
Client MAC Address : d8eb.97b6.fcc6
Client IPv4 Address : 9.2.20.78
Client IPv6 Addresses : fe80::1863:292f:feaa:2cf
```

```
Client Username: N/A
AP MAC Address : 707d.b99e.c2e0
AP Name: L2_1815w_1
AP slot : 2
Client State : Associated
Policy Profile : rlan_named_pp1
Flex Profile : rlan-flex-profile
Remote LAN Id : 1
Remote LAN Name: rlan_test_1
BSSID : 707d.b99e.c2e1
Connected For : 1159 seconds
Protocol : Ethernet
Channel : 0
Port ID: 2
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 1800 sec (Remaining time: 641 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
Current Rate : 0.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 07/06/2018 11:25:26 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 1159 seconds
Policy Type : N/A
Encryption Cipher : None
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 20
Access VLAN : 20
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000008
  IIF ID           : 0x90000008
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 32130209000000136C48A29D
  Acct Session ID  : 0x00000000
  Aaa Server Details
  Server IP        :
  Auth Method Status List
   Method : None
  Local Policies:
   Service Template : wlan_svc_rlan_named_pp1_local (priority 254)
```

```
    Absolute-Timer   : 1800
    VLAN             : 20
  Server Policies:
  Resultant Policies:
    VLAN             : 20
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 6855
  Number of Bytes Sent : 1640
  Number of Packets Received : 105
  Number of Packets Sent : 27
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```

すべての AP タグの概要を表示するには、次のコマンドを使用します。

```
Device# show ap tag summary
Number of APs: 2

AP Name             AP Mac               Site Tag Name         Policy Tag Name
RF Tag Name              Misconfigured     Tag Source
------------------------------------------------------------------------------------------
L2_1810d_1        0008.3296.24c0       default-site-tag        default-policy-tag
  default-rf-tag             No               Default
L2_1810w_2        00b0.e18c.5880       rlan-site-tag              rlan_pt_1
  default-rf-tag             No               Static
```

すべてのポリシー タグの概要を表示するには、次のコマンドを使用します。

```
Device# show wireless tag policy summary
Number of Policy Tags: 2

Policy Tag Name                  Description
------------------------------------------------------------------------
rlan_pt_1
default-policy-tag               default policy-tag
```

特定のポリシー タグの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>
Policy Tag Name : rlan_pt_1
Description     :

Number of WLAN-POLICY maps: 0
```

```
Number of RLAN-POLICY maps: 2
REMOTE-LAN Profile Name           Policy Name                              Port Id

-------------------------------------------------------------------------------------
rlan_test_1                       rlan_named_pp1                              1

rlan_test_1                       rlan_named_pp1                              2
```